Introduction

In the course of my previous work I was involved in discussions related to MCAS, angle of attack indicators, and reliable air data. I was involved in these discussions as my role in Flight Deck Crew Operations Integration was in the Flight Control Systems group. I was responsible for reviewing flight control system design and designing appropriate crew alerting and crew procedures based on expected failures, necessary flight crew action, and overall Boeing flight deck philosophy. Early in my time with Crew Operations Integration I was assigned to work the Air Data SRP that was created as a result of Air France 447, analyzing the response of Boeing models to a similar situation. My work statement also included preparing the 737 MAX Flight Control Crew Systems Interface Document and providing inputs to the Flight Technical pilot group on system design to determine the impact to pilot training. Additionally, I worked with representatives from Aviation Safety [redacted] to analyze loss of control inflight accidents and design flight deck features that would work to break the accident chain of various events. Examples of this work include the Enhanced Bank Angle Warning, added to the 737 NG and MAX after analyzing a series of six 737 accidents where the airplane crashed at a bank angle greater than 45 degrees, and the BCA Strategy for Reducing the Risk of Loss of Control Events[redacted] That strategy was presented to several in executive management, including [redacted], who refused to sign the document, and [redacted], who ultimately did.

Before I get into the details of that document, I would like to note the following. It is understood that the preference for ethics complaints is that they be made close to the time of occurrence. Given the nature of this report, this was difficult for two reasons. The first of these is that the general picture described by these individual events can only be seen when several events are examined together after their occurrence. The second is that, given the nature of this complaint, the fear of retaliation is high despite all official assurances that this should not be the case. In the course of discussing these individual events with coworkers, several mentioned that while they see the problems, they fear for their jobs should they speak up about it. They do not know how to give appropriate feedback to improve the company. There is a suppressive cultural attitude towards criticism of corporate policy – especially if that criticism comes as a result of analysis of fatal accidents. Briefings by lawyers during my time in Crew Operations Integration directed us to not write down any assessments about what could have led to an accident – a policy which inhibits learning and transmission of knowledge gained from data analysis to decision makers. This policy also creates a fear of doing something wrong; the fear is itself a serious safety issue. Despite the introduction of the Boeing Behaviors and the assertion that we should Collaborate with Candor and Honesty, at least some of the workforce does not think the company has the culture that allows them to do this. This perception has a negative effect on the safety culture at Boeing.

I have chosen to write this report not only because the Boeing Behaviors campaign says I should be able to, but because the nature of the industry we work in requires information exchange, clarity, and accountability in order to fulfill the primary ethical imperative of an engineer - to protect the safety of the public. The fact that the line "We will protect the safety, health, and well-being of the workforce, public, and customer" was removed from the 2019 version of Boeing's Engineering Code is another ethical concern. In many codes of engineering ethics adopted by professional engineering societies, a line similar to that is the top priority. In Boeing's new Engineering Code, the most similar line is, "I play an integral role in ensuring the integrity and safety of our products," buried as the second sentence of the third paragraph of the code. De-emphasizing the primary ethical imperative of professional engineers in this manner is not ethical, and has a negative effect on the safety culture at Boeing.

737 MAX Working Environment

Ethical concerns with the design and production of the 737 MAX go back several years. Many of these are small events - at the time in my personal career I did not recognize their significance. For example, during early 737 MAX discussions with the FAA, my manager in Flight Deck Crew Operations Integration [redacted]), asked me to assemble a chart showing the predicted fleet mix of 737 NG and MAX in the future, as part of an argument that the two models had to have similar training. He asked me to use the simple prediction formula that an airframe will go out of service 30 years from its production date. I desired to check the validity of this formula, so in addition to making the requested chart I investigated out of service dates of the -100/-200 and -300/-400/-500 upon the introduction of the next series. In the course of this investigation I also was given a presentation by an airline (KLM, in this case) on how they incorporate new models into their existing fleet mix. The results of this investigation did not support the use of the simple prediction formula I was asked to use; airplanes went out of service faster upon introduction of a new model than the formula predicted, and the impact of a fleet mix on airlines like KLM was limited when populations of different models were of a similar size. I informed my manager of these conclusions, and he asked me what he should do. I told him to not make his original argument as there was not data to support it. I later heard him in a phone meeting making the argument anyway. Perhaps this should have been reported to Ethics when it happened; but it is really only an aspect of a much larger corporate culture. This manager also undermined my concerns about the 737 by stating Boeing only makes changes as a result of fatal accidents – if I couldn't point to an event that happened on a 737 previously, there would be no support for a change. A long list of 737 unreliable air data incidents – as long as they were just incidents and not accidents – was simply not convincing.

Another similar event happened later. We received a request from EASA in [redacted] stating that they were aware of 5 events where a 737 experienced an autothrottle disconnect on approach and the flight crew did not respond appropriately (these events were the subject of several COSP items - [redacted] and others. The COSP items were determined to involve airplanes that had a speed deviation alert installed - which uses the same caution/warning light as the autothrottle disconnect and leads to crew confusion). In their letter, EASA asked if Boeing was aware of any further events; EASA was interested in the measures taken to prevent recurrence in the MAX design. No changes were planned for this issue on the MAX; a design where the autothrottle disconnect alert is already non-compliant with regulations (FAR 25.1329(k) requires a Caution - an amber light and an aural - the 737 just has a red flashing light). No events had been reported through COSP, but my manager asked me to look at databases of in-service events to determine if there were any potentially relevant events. I looked through these databases with the assistance of our human factors ATF [redacted]. We identified a further 5 events that may have had the same root cause as the COSP items. Following a discussion with my manager and second-level manager [redacted] the decision was made to not tell EASA about these events, as they had not come through the COSP process, and that we would fix the issue ourselves. The ultimate response to EASA can be seen in coordination sheet [redacted]. While this may not be completely unethical, it is presented here to build the picture of Boeing management's attitude towards regulatory bodies - even if the company is internally aware of an issue, this is not information it will share with the regulator, especially if it is dancing around a system that is already not in compliance and does not want to bring that to their attention. This dance has a negative effect on the safety culture at Boeing.

There are many instances such as these in the history of the 737 MAX design process; from the FAA being concerned about an engine rotorburst cutting the non-redundant rudder control cables, exclaiming, "we told you to fix this 20 years ago," to a meeting about available hydraulic power during an engine failure answering the question 'what would happen in a US Airways 1549-type event?' with uncomfortable silence (the unspoken conclusion being that the flight crew would have to run the stabilizer manually to retain control…shortly after takeoff and close to the ground). On the whole, the 737 MAX was designed via piecemeal updates to prevent triggering expensive certification and training, and Flight Crew Operations Integration got a unique look at the integrated effects of that approach. In fact, the resulting view from this group was such that I left the company voluntarily in 2015. In emails to colleagues at the time, I stated that I did not feel I could have a net positive impact on aviation at a company that was squeezing the engineering budget for new programs while spending $6 Billion a year buying its own stock. With so much on the line when an airplane takes to the air, I did not and do not regard the company's business practices as ethical. I was willing to stand up for safety and quality, but was unable to actually have an effect in those areas; Boeing management was more concerned with cost and schedule than safety or quality. As the company still struggles with these items today, in a more severe fashion, I will now go into some of the details of what I observed in my time on the 737 MAX program.

Issues with Alerting and Regulations

Early in the development of the 737 MAX there was a push to equip the flight deck with the modern crew alerting system EICAS (in fact[redacted], exhorted Crew Ops to make this effort as it was necessary for the 737 to be a modern airplane). Enough effort was put into this task to determine the detailed changes that would be necessary and understand the impact to crew procedures – indeed it was a change to have the crew respond to EICAS alert messages rather than the 737's current alerting system of "lights all over the flight deck." Ultimately, due to this impact and the overall cost of changing 737 systems to conform to a new alerting paradigm, the push to change the 737's alerting system to EICAS was abandoned. As an alerting system, EICAS is designed to be compliant with FAA regulations. The crew alerting regulation, 25.1322, is one of these. Of course, the original 737 was not certified to 25.1322, so when Boeing determined the cert basis for the 737 MAX it essentially got to pick what parts of 25.1322 it complied to. For example, 25.1322(b) describes the alerting categories Warning, Caution, and Advisory. The 737 MAX only has Warnings and Advisories, as unlike Boeing EICAS models it does not have a Caution aural and thus cannot have anything that qualifies as a caution. This has an interesting interaction with autoflight systems, not just for the autothrottle disconnect alert reason mentioned earlier. Documents relating to the certification of the Cat IIIB autoland system on the 737 NG are particularly interesting. There were discussions as to whether the annunciation for autoland engagement should be LAND 3, like the other Boeing airplanes, or something else, as the system on the 737 is not triple-redundant like other models (the end result is that the annunciation is LAND 3, for commonality across uncommon designs). Additionally there were discussions about how to do alerting for levels of autoland capability. On models like the 777 and 747, this is handled by Caution and Advisory messages in the EICAS message stack. The result of the design process on the 737 NG was to create an EICAS message stack, just for autoland capability messages. In the 737 NG round of certification these were called Caution messages. For the 737 MAX, they are not – its certification basis does not include Cautions. This dance around alert messages is an ethical concern.

MCAS

In regards to MCAS, it is only briefly mentioned in the 737 MAX Flight Controls CSID I wrote. Discussions with the Flight Controls group did not go into details of the MCAS design; we were much more focused on the new fly-by-wire spoilers and the Elevator Jam Alleviation System implemented to avoid focused FAA scrutiny on the 737's lack of elevator control in the case of an elevator jam. Flight Controls stated that MCAS would have the same failures as the existing speed trim system, and thus did not require separate annunciation or additional training. In association with the Flight Technical Pilots, Flight Deck Crew Operations Integration scored all new features on the 737 MAX in terms of potential training impact, and managed discussions in an effort to keep the training to level B differences.

Design to Training Differences

One area where training differences significantly affected the design was the flap indicator. The 737 NG has a round dial flap indicator with two needles, just like all 737s before it. The 737 MAX did not have room on the forward panel for this indicator with the new large displays, so it was decided to put flap indication on the displays. The ultimate result of this was to emulate the round dial flap indicator exactly on the new displays, including its method of annunciating a flap asymmetry or skew by splitting the needles and the leading edge flaps transit and extended lights (EASA actually drove a logic change to the LE FLAPS TRANSIT light – on the 737 NG it turns on amber for normal operations, which is not a regulation-compliant [25.1322(f)] design. The 737 MAX suppresses this behavior). The trade study to put the flap indicator included examining a flap tape – the modern method of indicating flap position – which has certain benefits, including making it easier to visually identify issues with flap deployment and the ability to potentially remove the overhead Leading Edge Flap Slat Annunciator. However, the concern of driving training differences, with crews having to look at a new indication to refer to an existing checklist, prevented this change from being made.

Design Efforts to Prevent Loss of Control Accidents

In particular reference to air data reliability and angle of attack, the BCA Strategy for Reducing the Risk of Loss of Control Events identifies airspeed awareness as a dominant theme in loss of control accidents. Two aspects of this theme were analyzed - Stall/Low Airspeed Awareness and Air Data Sensor Failures (as reliable data in the flight deck is an important energy state awareness parameter for the flight crew). Boeing was not the only organization identifying these themes as part of this analysis; our work in Crew Operations Integration and Aviation Safety built off of discussions of the Commercial Aviation Safety Team industry panel. Six of the 18 incidents and accidents analyzed by CAST were Boeing 737 aircraft, five of those were fatal accidents. One of those was Turkish 1951, which crashed on approach to Amsterdam as the result of erroneous radio altimeter information being fed to the autothrottle without a comparison check to the other radio altimeter. The sixth, non-fatal incident was a Thomsonfly 737-300 experiencing pitch instability on approach to Bournemouth, an early incident demonstrating how the 737's stabilizer is inadequate to effectively counter the pitch-up moment from increased engine thrust in certain conditions. This theme continues in the Tatarstan Airlines flight 363 and Flydubai flight 981 fatal accidents. An additional six 737 accidents (2) and incidents (4) were analyzed by Boeing in the course of preparing this strategy.

Notably, the Commercial Aviation Safety Team Airplane State Awareness Joint Safety Analysis team identified "Invalid Source Data" as a theme in 5 of the 18 events the team analyzed. This was defined as, "invalid source data from the air data system sensors or probes, inertial or rate gyro systems, angle-of-attack (AOA) vanes or sensors, or other signals were used as input to primary flight displays, the autoflight system, or the navigation systems with little or no indication the data were invalid." The primary intervention strategy for accident theme is in Aircraft Design. The Invalid Source Data theme was a factor in the Turkish Airlines 1951 accident, where a 737-800 crashed with 8 fatalities while on approach to Amsterdam due to the autothrottle responding to input from a single radio altimeter, which was reporting erroneous information and led to the autothrottle retarding while the airplane was still in the air. The FAA subsequently issued AD 2012-21-08 to detect and correct this unsafe condition associated with erroneous output from a radio altimeter channel. When CEO [redacted] states that there was no "technical slip or gap" in Boeing's design of the 737 MAX, where a single AOA sensor drove MCAS, he makes a false statement; Boeing, the FAA, and a broad industry team were aware of the necessity of detecting invalid source data and preventing its use by downstream systems. The failure to do that in MCAS is unconscionable, and presenting this situation as anything other than a failure is unethical.

One of the recommendations in the BCA Strategy for Reducing the Risk of Loss of Control Events is to implement the Enhanced Bank Angle Warning on the 737 NG and 737 MAX. The need for this feature, which triggers at a bank angle of 45 degrees and puts a large red arrow on the PFD to indicate the direction to roll back to wings level as well as a voice aural "ROLL LEFT/RIGHT," was developed and evaluated upon noticing a trend of 737 accidents with a loss of spatial awareness in the roll axis. Notably it is not required on more modern Boeing designs; fly-by-wire makes Bank Angle Protection through wheel forces possible. Deploying the alert to in-production 737 NG and getting approval to put it on the 737 MAX were difficult – there is no budget line-item for safety enhancements for development, it is not a feature that can be sold for additional profit, and it affected upset recovery training at a time when every training impact could affect the profitability of a major program. However, a study of 30 line pilots in the Boeing engineering simulator indicated it would have a positive effect on spatial awareness for the pilot flying and a reinforcing effect for the pilot not flying to take over if the other pilot was not recovering appropriately. It is noteworthy that the Enhanced Bank Angle Warning was designed contemporaneously with MCAS and includes a validity check on its inputs – if the two IRUs on the 737 do not agree, the alert will not annunciate as it cannot determine a valid bank angle. The hazard associated with a false time-critical warning flight path annunciation is higher than not annunciating at all.

Another of the recommendations in the BCA Strategy for Reducing the Risk of Loss of Control Events is to implement Synthetic Airspeed on all airplane models that do not have it at the next appropriate software update. The full coordination sheet has an overview of the reasons this was recommended. With regard to the 737, there were several specific reasons relating to the ways systems that use air data respond to erroneous data. For example, on the 737 there is no way to silence an erroneous overspeed aural [Relevant regulation the 737 doesn't meet: 25.1322(d)(2)]. Notably, this was identified as a contributing factor in the Birgenair flight 301 accident, with the result that the FAA issued AD 2004-10-05 requiring a resettable overspeed warning on all Boeing models - except the 737. That is a particularly interesting omission, as Boeing itself thought the 737 should also get a resettable overspeed warning (reference [redacted] and meeting minutes for November 11, 1996 AMPAT), and such a system was even designed (reference [redacted]). It was, according to the designer [redacted] not implemented on the 737 due to cost. The fact that the overspeed aural was continuously annunciating during the final minutes of Ethiopian 302 calls to question whether not implementing an NTSB/FAA recommendation for cost reasons (decades ago) was appropriate. Additionally, synthetic airspeed was recommended on the 737 to prevent erroneous air data information getting to the stall warning speed floor mode; a feature only the 737 has that will annunciate the stall warning for low airspeed and not just angle of attack. A further reason to recommend synthetic airspeed on the 737 MAX was to ensure the display of reliable air data. Unlike other Boeing models that incorporate instrument source select switches in the flight deck, if the display of air data on one side of the 737 flight deck is found to be erroneous, that information cannot be replaced with information from the other side. That pilot is simply stuck with looking at bad information until the problem clears. This situation is four generations of design behind the modern flight deck - the 747/767 have source select switches that allow bad air data to be removed from display and some using systems if the crew can determine the erroneous source, the 777 automatically votes air data to remove erroneous information, and the 787 has additional monitors and synthetic airspeed as a backup to further ensure the flight crew does not have to respond to displayed erroneous data.

The implementation of synthetic airspeed on the 737 MAX was recommended as a trade study several times. The initial trade study for the upgraded ADIRU - the IADIRU - included a statement that implementing synthetic airspeed would be explored as the new system had the ability to do the calculation. This line item was rejected, though the IADIRU trade study was approved overall. Following this, another attempt was made to add synthetic airspeed as its own trade study, with the support of Crew Operations Integration and the 737 [redacted], based on the known history of air data incidents on the 737. This trade study was rejected as it cost too much for the systems IPT leader [redacted] to approve; it was given another chance in a meeting with 737 MAX CPE [redacted], who also rejected the study based on cost and potential training impact. Moving from a system where the flight crew can do nothing about erroneous data to one where the AIRSPEED UNRELIABLE checklist might include a step to flip a switch was certainly a training impact. Notably, my current manager stated to me that synthetic airspeed wasn't on the MAX because it "doesn't give the flight crew what they need." That statement is a serious misunderstanding of the work that went into the development of synthetic airspeed and the collaboration of pilots, Crew Operations Engineers, Systems Engineers, and Aviation Safety analysts that supported such action. This misunderstanding and the processes that led up to its dissemination to the management team are a serious ethical and safety issue.

Conclusion

Given the complex nature of the Lion Air and Ethiopian accidents it is not possible to say for certain that any actual implementation of synthetic airspeed on the 737 MAX would have prevented the accidents. This report is not written with the intent to argue that a single change should have been made to the 737 MAX design process to prevent the accidents that have occurred. However, it should be noted that synthetic airspeed was implemented on the 787 as a byproduct of the need for flight controls to have highly reliable angle of attack data - the monitors that make synthetic airspeed possible monitor and detect erroneous angle of attack data, and then work to prevent the use of erroneous data by downstream systems. This basic design philosophy established by flight controls makes it clear that piping a single sensor output to a control law without a data check is simply not an acceptable design - even without synthetic airspeed. When CEO Dennis Muilenburg and others state that the 737 MAX was a safe airplane as designed, they seriously misrepresent what Boeing Engineering has learned about how data and flight control functions should be treated through previous fatal accidents and exhaustive industry studies, to the degree that the CEO and others are wholly incorrect in making this statement. They also seriously misrepresent engineering efforts based on thorough analysis to introduce safety into the design that were rejected by management for programmatic reasons.

The failure of the management structure to understand this misrepresentation, and the failure to produce a design that reflects a modern understanding of aviation operations, safety, and the lessons learned from previous fatal accidents, is very serious. This is not merely a design error on a single airplane design; this is a corporate culture issue that affects Boeing's ability to produce all of its products. This thread of corporate culture problems can be traced back decades and is still present in ongoing development programs. It will require a large, exhaustive, and thoroughly honest investigation to completely remedy. And it must be remedied – Boeing is not in a business where safety can be treated as a secondary concern, but the current culture of expediency of design-to-market and cost cutting does not permit any other treatment by the workforce tasked with making executive management's fever dreams a reality.

Safety can and should be an enduring value at Boeing. Safety must be integrated into the Boeing culture from the first design studies to the final delivery preparations of every airplane. This safety culture must take into account previous accidents, failures of Boeing design, failures of airline operations and design and build every product with the lessons learned from those events. To be effective in operation, this safety culture must have a highly integrated view of Boeing products – from design details to high-level system effects – to ensure that all lessons learned have been effectively incorporated. In the case of the 737 MAX, this sadly did not happen. Management focused on cost and training impact, shutting down trade studies that attempted to modernize the airplane and avoiding awareness of known issues encountered in historical 737 operation. The drive by management to update the 737 MAX in a piecemeal fashion, keeping certification and training costs low, was at odds with the engineering workforce's ethical imperative to protect the safety of the public. Safety is not a piecemeal process – it can only be ensured through a detailed process that integrates past experience and high-level system behavior. Ensuring safety in the 737 MAX requires more than just fixing the design error uncovered by the Lion Air and Ethiopian accidents – it requires an exhaustive review of the entire airplane to ensure no other such errors have been made. If Boeing truly wishes to display safety as an enduring value, this review must be performed before returning the 737 MAX to service, and it must make a commitment to make all changes identified by such a review.

Addendum: The 777X

Development of the 777X is currently benefiting from the use of the Airplane Zero integration lab, which is my current assignment at Boeing. This lab is effectively discovering and helping to resolve many integration issues – an improvement over the 737 MAX, where such a lab did not exist. This is a positive step in the creation of a safety culture here at Boeing. However, there are some findings that show there is still work to be done to create an integrated safety culture at Boeing. For example, the Flight Controls/autoflight group, swamped with work, frequently rejects problem reports from Airplane Zero, and has on at least one occasion done so with a false rationale. That behavior is not ethical. It is of particular concern as several problem reports relating to flight controls have been generated because the initial requirements from the group did not meet operational needs; a surprising finding for a group that must have a detailed understanding of how an airplane is flown and should have mature requirements from the 787 to build on. I am not fully aware of all of the reasons for these requirements misses from flight controls, but those misses are a safety concern, and the group's response to generated problem reports shows that the Boeing culture is still having a negative impact on current development programs.

There is a way out of this cultural morass. Part of it is implementing some of the new digital tools (like model-based-engineering, digital twins, and the digital thread) that are being discussed; early model development would help groups like flight controls ensure operational requirements are met well before hardware and customer software is built. However, the larger part is serious, honest introspection on the part of every level of Boeing management and engineering to ensure that cost and schedule are never a secondary priority to safety and quality. Today, management frequently talks about wanting to make safety and quality a priority, but few substantive changes occur. When executives insist that designs which are unacceptable in terms of safety are in fact safe, it does not seem that there is an actual desire to make those substantive changes. That – in the face of deaths of the users of company products – is unethical, and will make it difficult to reestablish trust in the Boeing brand. Radical changes are needed, and possible, if an honest review of this company's business practices is conducted and sweeping changes to place safety and quality at the top of all decision making trees are made.