A Virtue Ethics Analysis of the Boeing 737 MAX Design

STS Research Paper
Presented to the Faculty of the
School of Engineering and Applied Science
University of Virginia

By

Katherine Taylor

May 4, 2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: ____

Approved: _______________________________________ Date ________________________
Benjamin J. Laugelli, Assistant Professor, Department of Engineering and Society

Introduction

In both November of 2018, and March of 2019, a Boeing 737 MAX airliner crashed, killing all passengers and crew on board. Preliminary reporting showed that a device called the MCAS (maneuvering characteristics augmentation system) caused the planes to enter uncontrollable dives, ultimately causing the crashes (National Transportation Safety Board [NTSB], 2019). Scholars currently place blame for the crashes on Boeing, but also on the FAA for failing to appropriately regulate Boeing's use of the MCAS on the 737 MAX. Some scholars even suggest that the design of the 737 MAX represented a failure of Systems Engineering.

However, there is little discussion of the moral or ethical implications of including a MCAS on a passenger airliner. There is the possibility that the designers in creating the 737 MAX including the MCAS behaved unethically. Without examining the ethical implications of the design choices, Systems Engineers would not understand how designs can be unethical or systems of ethical elements can become unethical.

Examining the design of the Boeing 737 MAX with the inclusion of the MCAS through the lens of virtue ethics allows for a structured analysis of how Systems Engineers designed an inherently unethical system. Specifically, I argue that the designers of the Boeing 737 MAX airliner behaved unethically as they violated two ethical virtues: foresight, and holistic thinking.

Background

The Boeing 737 aircraft has been in service for over 52 years. There have been several iterations of the design, with the plane remaining the most popular aircraft in the world. With the latest iteration, Boeing wanted to improve the fuel efficiency of the plane to compete with Airbus, which necessitated the use of larger engines (Travis, 2019). Using larger engines meant the plane had an increased risk of stalling at higher angles of attack (AOA), which occur during takeoff or landing. However, Boeing wanted the new model to handle exactly like the previous model, the 737 NG, and added the MCAS to compensate for the different aerodynamics caused by the engines. When an AOA above the optimal range is detected, the MCAS trims the stabilizer down, forcing the nose of the plane towards the ground. Boeing has traditionally used the MCAS only on military planes with ejection seats, and this was the first time the technology was used on a commercial aircraft. In retrofitting the MCAS for use on the 737 MAX, Boeing only used data from one AOA sensor rather than both sensors on the plane. If pilots feel that the MCAS is coming on erroneously, there is the ability to manually deactivate it, but information on how to turn off the system did not originally appear in flight manuals (Johnston & Harris, 2019).

Literature Review

Although the crashes involving a 737 MAX occurred recently in November of 2018 and March of 2019, there already exists a plethora of literature on the technical failures that caused the crash and lessons for those designing safety-critical systems. Some articles do focus on how the design was a failure of Systems Engineering, but they do not discuss whether the system was designed according to ethical standards.

In *The Boeing 737 Max Saga: Lessons for Software Organizations*, P. Johnson and R. Harris discuss several complex factors that led to the crashes and groundings of the 737 MAX aircraft. These factors include poor documentation, rushed release, delayed software updates, and humans out of the loop. The authors go on to discuss the broader system’s context of the failure and advice for other software organizations designing similar systems. They even go as far as to declare the crashes as a failure of Systems Engineering. However, the authors fail to connect issues such as poor documentation directly to their ethical consequences.

T. Sgobba in *B-737 MAX and the crash of the regulatory system* argues that Boeing 737 MAX accidents represent a major failure of the airline industry to properly regulate the airworthiness of aircraft. He argues that as the technology evolved, the industry did not properly cope with safety issues and instead created substantial backup systems that only need to pass a hardware capability check. While regulations should not have allowed the Boeing 737 MAX to be flown with the MCAS in place, Sgobba does not make claim to any ethical problems with the inclusion of the MCAS. Just because these accidents represent a failure of the aviation regulatory system does not preclude the design of the plane from being an ethical failure.

While both articles offer guidelines for the design and regulation of safety-critical systems, there is little insight into the ethical implications of the Boeing 737 MAX design and inclusion of the MCAS. Current research focuses more on the best practices of designing and certifying similar systems in the future but not on how the designers violated engineering virtues. This paper will use a virtue ethics framework to develop a judgment on the morality of the designers of the 737 MAX.

Conceptual Framework

My analysis of the design of the Boeing 737 MAX and inclusion of the MCAS draws on virtue ethics. Virtue ethics was originally developed by Aristotle and focuses on the nature of the acting individual. Virtues are good or desirable characteristics that a person should have to be moral and are learned over time. These moral virtues are defined as a place of equilibrium; for example, courage can be defined as the balance of cowardice and recklessness (van de Poel & Royakkers, 2011). Virtue ethics can be seen as a mixture of ethics and psychology with an emphasis on developing good character traits.

When applying virtue ethics, the virtues relevant to the situation depend on the context and the nature of the acting individual. In the case of the design of the 737 MAX and inclusion of the MCAS, I define the relevant rules to be the INCOSE (International Council on Systems Engineering) code of ethics. The rules most relevant to the issues at hand are under the "Fundamental Duties to Society and Public Infrastructure" heading and are listed in *Figure 1* below. These rules are deemed necessary for the proper practice of Systems Engineering and are promoted by INCOSE, the international organization certifying all Systems Engineers.

1. Guard the public interest and protect the environment, safety, and welfare of those affected by engineering activities and technological artifacts
2. Accept responsibility for your actions and engineering results, including being open to ethical scrutiny and assessment
3. Proactively mitigate unsafe practice
4. Manage risk using knowledge granted by a whole system viewpoint and understanding of systemic interfaces
5. Promote the understanding, implementation, and acceptance of prudent Systems Engineering measures

Figure 1: INCOSE Code of Ethics, "Fundamental Duties to Society and Public Infrastructure" (Code, n.d.)

Specifically, I will focus on how the rules "proactively mitigate unsafe practice" and "manage risk using knowledge granted by a whole system viewpoint and understanding of systemic interfaces" are violated by the design of the Boeing 737 MAX. I define risk in this context per I. van de Poel and L. Royakkers, meaning the "product of the probability of an undesirable event and the effect of that event" (van de Poel & Royakkers, 2011). To discuss the design of the Boeing 737 MAX through the lens of virtue ethics, I derived the two virtues of foresight and holistic oversight from the above rules. Foresight in this instance means the ability to predict issues that may arise in the future, in order to create a safer system. Holistic thinking refers to evaluating the system from broader scope in order to manage risk. To judge the ethicality of the designers of the Boeing 737 MAX and their choice to include an MCAS, I will examine whether or not these virtues appear to be observed in the design of the system. While the designers may only violate these two virtues, Pritchard argues in the context of general engineering virtues, lacking at least one is enough to deem an engineer immoral (Pritchard, 2011). Therefore, I will focus on these two virtues, as they are enough to deem the designers unethical.

Analysis

The designers of the Boeing 737 MAX airliner behaved immorally, which can be shown through the violation of two ethical virtues: foresight, which correlates to the rule "failure to proactively mitigate unsafe practice" and holistic thinking, derived from the rule to "manage risk using knowledge granted by a whole system viewpoint and understanding of systemic interfaces". As the designers are lacking these two virtues and, according to Pritchard, lacking at least one engineering virtue can deem an engineer immoral, the designers can be considered immoral (Pritchard, 2001). This stance is evidenced by testimony from airline industry experts, pilots, the NTSB (National Transportation Safety Board), and Boeing itself. The following paragraphs examine each virtue in detail and highlight how the designers are immoral.

<u>Foresight (Proactively Mitigate Unsafe Practice)</u>

The designers of the Boeing 737 MAX failed to have foresight as the aerodynamics of the aircraft were unsound, AOA discrepancy sensors were not included on all models, and there were blatant issues with the information given to pilots. These three issues contributed to the instability of the design and the two fatal crashes that occurred. First, I will examine the aerodynamics of the plane itself.

Without the MCAS installed on the 737 MAX, the aircraft was not aerodynamically stable. According to G. Travis, "In the 737 Max, the engine nacelles themselves can, at high angles of attack, work as a wing and produce lift. And the lift they produce is well ahead of the wing's center of lift, meaning the nacelles will cause the 737 Max at a high angle of attack to go to a *higher* angle of attack. This is aerodynamic malpractice of the worst kind." (Travis, 2019). As Travis states, the engines can generate lift in specific phases of flight, which forces the plane to increase its angle of attack, leading to an increased chance of a stall, a dangerous state that can crash the plane. It goes against generally accepted aircraft design to have the engines generate lift like this. This aircraft would not be aerodynamically stable without compensation from a system such as the MCAS. Since the aircraft without the MCAS could stall at lower AOAs than previous iterations of the design or other aircraft, this is a violation of the virtue of foresight. To compensate for this aerodynamic instability, Boeing included a system called the MCAS on the aircraft. However, the implementation of an MCAS on the 737 MAX has its host of ethical issues, which are discussed below.

While the MCAS worked to counteract the increased ability of the aircraft to stall, it relied on measurements from only one AOA sensor. This goes against accepted design practice for safety-critical systems; as D. Griffin and C. Devine conclude, "from the beginning, it should have been a fail-safe design, which would have relied on two inputs to make sure that you weren't sensitive to one failure" (Griffin & Devine, 2019). As Griffin and Devine state, relying on one AOA sensor meant that if the one sensor is malfunctioning, then the MCAS could turn on and push the nose of the plane down when there is little risk on the plane stalling. In the November 2018 crash, the angle measured by the AOA sensor that activated the MCAS differed from the other sensor by 20 degrees (NTSB, 2019). If data from both AOA sensors were used in the initial design, then at least one of the fatal crashes could have been prevented. As only using one sensor is unsafe and was proven to be unsafe in that it caused a fatal crash, the designers of the system failed to utilize foresight.

Even though the MCAS only used measurements from one AOA sensor, Boeing created an AOA sensor disagree alert that should have been installed on every plane (Griffin & Devine, 2019). The AOA sensor disagree alert indicates whether the measurements from the two AOA sensors differ by more than an acceptable amount. This warning was not included with the standard version of the aircraft because of "Boeing's fundamental design philosophy of retaining commonality with the 737NG" (Boeing, 2019). As discussed in the background section, Boeing's design philosophy for the 737 MAX was to maintain as much continuity with the previous generation of 737, the 737 NG, which did not contain an AOA disagree sensor (Travis, 2019). Neither of the 737 MAX models that crashed had the optional AOA sensor disagree alert. According to van de Poel and Royakkers, ethically the "system should thus provide [pilots] the right information on time," especially as pilots cannot judge the angle of attack without the aid of sensors, and cannot discern issues with AOA disagreement (van de Poel & Royakkers, 2011). If this alert was included on the planes, the pilots might have had increased information as to what was going wrong with their planes and could have prevented the crashes.

It has also come to light that Boeing was aware of the absence of the alert in as early as 2017 and decided to not to inform the FAA or the plane operators (Zazulia, 2019). Boeing only opened up about the mistake in April 2018 after both crashes had occurred, stating that "in 2017, within several months after beginning 737 MAX deliveries, engineers at Boeing identified that the 737 MAX display system software did not correctly meet the AOA Disagree alert requirements" (Boeing, 2018). The lack of an AOA sensor disagree alert on all models of the 737

MAX and failure of Boeing to correct the problem violates the virtue of foresight, as lacking the disagree alert is unsafe and Boeing failed to proactively correct the problem.

Finally, Boeing acted immorally by failing to provide adequate information to pilots on the MCAS, such that pilots were not aware of how the new system worked. In an anonymous ASRS (Aviation Safety Reporting System) report, one 737 MAX pilot stated that "I think that it is unconscionable that a manufacturer, the FAA, and the airlines would have pilots flying an airplane without adequately training, or even providing available resources and sufficient documentation to understand the highly complex systems that differentiate this aircraft from prior models" (Johnston & Harris, 2019). As stated above, pilots had noticed that there was something different about the handling on the 737 MAX, while uninformed as to what exactly was different. The pilot also alludes to the various organizations responsible for ensuring the safety of the design, and how they failed to stop this plane from flying before multiple accidents occurred. It was not until after the November 2018 crash that Boeing finally put out a bulletin to "call attention to an AOA failure condition that can occur during manual flight only" (Boeing, 2018). There is a failure here on Boeing's part to proactively provide information on a system that completely changes the handling of an aircraft, thus leading to the unsafe practice of pilots flying a passenger airplane without being completely informed as to how the plane worked.

In the design of the 737 MAX and inclusion of the MCAS, the designers at Boeing failed to utilize foresight, which is exemplified by the initial aerodynamic instability of the aircraft, use of one AOA sensor, lack of an AOA sensor disagree alert and insufficient information for pilots. Without proper foresight, the designers did not build a safe aircraft, and failed to proactively correct issues. Next, I will examine how the design of the aircraft also violates the virtue of holistic thinking.

Holistic Thinking (Manage Risk Using Knowledge Granted by a Whole System Viewpoint and Understanding of Systemic Interfaces)

The designers of the Boeing 737 MAX also failed to employ holistic thinking because the overall design with the MCAS did not meet safety-critical system standards and made improper assumptions about pilot response as a part of accident prevention. First, I will focus on how the MCAS does not meet safety-critical system standards.

The design of the 737 MAX did not meet the accepted standards for the entire airline industry as M. McClellan states that "what's critical to the current, mostly uninformed discussion is that the 737 MAX system is not triply redundant. In other words, it can be expected to fail more frequently than one in a billion flights, which is the certification standard for flight critical systems and structures" (McClellan, 2020). One idea to note from this quote is that the system is not triply redundant, which means there is no backup if the MCAS fails. Having at least three backups is considered standard in airplane design practice, and thus as McClellan goes on to state, the system would be expected to fail more often than what is acceptable. Prior to the second crash, internal FAA estimates pegged that without modification of the 737 MAX, it "'could result in as many as 15 future fatal crashes over the life of the fleet.' This translates into one crash every three years during the 45 years of the estimated life of the program, potentially leading to the death of 2,900 people" (Brady, n.d.). This was the reasoning behind letting airlines continue to fly the plane after the first accident while Boeing worked on a software patch for the MCAS, as the FAA did not expect another accident for three years. This presents a failure of holistic thinking on the part of Boeing and the FAA, as the lack of triple redundancy in the airliner design is a large risk, and so is assuming that the plane would not crash for another three years.

Boeing's assumptions about pilot behavior in accident prevention were improper as they show little understanding of the complicated nature of pilot interfaces. According to the NTSB, "neither Boeing's system safety assessment nor its simulator tests evaluated how the combined effect of alerts and indications might impact pilots' recognition of which procedure(s) to prioritize in responding to an unintended MCAS operation caused by an erroneous AOA input" (NTSB, 2019). Based on the above assessment, Boeing failed to study how all the alerts and indicators mounted in the cockpit could affect the pilot's response to an erroneous activation of the MCAS. This presents a problem with holistic thinking, as Boeing did not appropriately test the MCAS in the context of the whole system.

I have just argued that Boeing made improper assumptions about pilot behavior in the case of the MCAS turning on erroneously. Now, some argue that pilots should have been able to recover from the MCAS turning on erroneously. McClellan, an airline pilot, concludes that "though the pitch system in the MAX is somewhat new, the pilot actions after a failure are the same as would be for a runaway trim in any 737 built since the 1960s. As pilots, we really don't need to know why the trim is running away, but we must know, and practice, how to disable it" (McClellan, 2020). As McClellan states, the pilots should have known what to do if the MCAS turned on in error. While I agree with McClellan that a pilot should be able to respond to the MCAS turning on, it does not appear that Boeing designed the system with a reasonable response time in mind.

From a hearing conducted by the House Committee on Transportation, it was stated Boeing expected that a pilot could respond to the MCAS activating erroneously within four seconds; but an internal memo from 2018 stated that a "slow reaction time scenario (>10 seconds) found the failure to be catastrophic" (Bogaisky, 2019). In the March 2019 accidents, it was determined that the pilots initially responded within eight seconds, but the plane still went down (Bogaisky, 2019). Designing the system with the assumption a pilot could respond in four seconds seems unreasonable, especially when a response time of over ten seconds could cause a catastrophic failure. This connects back to holistic thinking, as Boeing made assumptions about pilot response time that did not take into account the whole system and thus failed to appropriately manage risk.

In the design of the 737 MAX and inclusion of the MCAS, the designers at Boeing failed observe the virtue of holistic thinking, as the overall design with the MCAS did not meet safety-critical system standards and made improper assumptions about pilot response as a part of accident prevention. In failing to observe this virtue, the designers of the aircraft are immoral because the probability of catastrophic failure for the system was too high. It is important for Systems Engineers to understand how to manage risk in the context of safety-critical systems in order to prevent casualties of this magnitude.

Conclusion

In this paper, I argue that the designers of the Boeing 737 MAX aircraft were immoral due to the failure to follow the virtues of foresight and holistic thinking. Using the framework of virtue ethics, I found that the designers behaved unethically, via examination of the aerodynamics, sensor use, information for pilots, design standards, and assumptions about the pilot response. Because the designers fail to meet two of the virtues, they can be deemed immoral, as according to Pritchard, the lack of any general engineering virtue is enough to deem an actor immoral (Pritchard, 2001). While Boeing plans to make several corrections to pilot training and the MCAS design, it is important for engineers to understand how a system should be designed ethically in the first place (Brady, n.d.). Designing a system while utilizing foresight and holistic oversight in the first place will ultimately reduce costs and improve safety outcomes.

Word count: 3,467

References

Bogaisky, J. (2019, October 31). Here's the new evidence on 737 MAX development released at the House Boeing hearing. Retrieved February 22, 2020, from https://www.forbes.com/sites/jeremybogaisky/2019/10/30/heres-the-new-evidence-on-boeing-737-max-development-released-at-house-hearing/#6dabb0674153

Brady, C. (n.d.). 737 MAX - MCAS. Retrieved from http://www.b737.org.uk/mcas.htm

Code of ethics. (n.d.). Retrieved February 12, 2020, from https://www.incose.org/about-incose/Leadership-Organization/code-of-ethics

Griffin, D., & Devine, C. (2019, May 1). Boeing relied on single sensor for 737 Max that had been flagged 216 times to FAA. Retrieved February 18, 2020, from https://www.cnn.com/2019/04/30/politics/boeing-sensor-737-max-faa/index.html

Johnston, P., & Harris, R. (2019). The Boeing 737 MAX saga: Lessons for software organizations. *Software Quality Professional*, *21*(3), 4 - 12.

McClellan, M. (2020, January 23). Can Boeing trust pilots? Retrieved February 22, 2020, from https://airfactsjournal.com/2019/03/can-boeing-trust-pilots/

Pritchard, M. (2001). Responsible engineering: The importance of character and imagination. *Science and Engineering Ethics, 7*(3), 391–402.

National Transportation Safety Board. (2019). *Assumptions used in the safety assessment process and the effects of multiple alerts and indications on pilot performance*. (Report No. 59582) Retrieved from https://www.ntsb.gov/investigations/AccidentReports/Reports/ASR1901.pdf

Sgobba, T. (2019). B-737 MAX and the crash of the regulatory system. *Journal of Space Safety Engineering, 6*(4),299-303.

The Boeing Company (2018). *Uncommanded nose down stabilizer trim due to erroneous angle of attack (AOA) during manual flight only* [Bulletin] Seattle: The Boeing Company.

The Boeing Company (2018, April 29). *Boeing statement on AOA disagree alert* [Press release]. Retrieved from https://boeing.mediaroom.com/news-releases-statements?item=130431

Travis, G. (2019, April 18). How the Boeing 737 Max disaster looks to a software developer. Retrieved February 11, 2020, from https://spectrum.ieee.org/aerospace/aviation/how-the-boeing-737-max-disaster-looks-to-a-software-developer

van de Poel, I., & Royakkers, L. (2011). *Ethics, technology, and engineering: An introduction*. Hoboken, NJ: Blackwell Publishing Ltd.

Zazulia, N. (2019, May 7). Boeing knew the AOA disagree alert on the 737 MAX didn't work - and said nothing. Retrieved February 18, 2020, from https://www.aviationtoday.com/2019/05/06/boeing-angle-of-attack-disagree-alert/