Lessons from the Boeing 737 Max 8

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

David Normansell
Spring, 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

Introduction

On October 29, 2018, a brand new Boeing 737 Max 8 airplane carrying 189 passengers and crew from Jakarta to the Bangka islands crashed shortly after takeoff, killing everyone on board (NTSB, 2019). On March 10, 2019, another new Boeing 737 Max 8 airplane en route from Addis Ababa to Nairobi crashed shortly after takeoff, killing all 157 people on board (NTSB, 2019). Over the last few decades, society has developed an increasing trust in the aviation industry as the industry focuses more on safety and yearly accident rates dwindle, and those that do occur are only freak accidents easily written off as terrible luck (Smith-Spark, 2019). But the Boeing 737 Max 8 disasters have struck at that trust; both were easily preventable accidents caused by human error, not a bird or storm. This paper studies these accidents and their consequences in order to assign responsibility and draw knowledge that can be used to prevent similar disasters from happening in the future. Ultimately, the author hopes to gather knowledge that he can use in his own career as an aerospace engineer to earn back the public trust again. This paper analyzes these disasters, and the role of the engineer in the disasters, and in public safety in general, through the STS Framework of Co-Production. In doing so, this paper answers the question: What went wrong that led to the Boeing 737 Max 8 crashes and groundings, and how do those disasters inform the role of the engineer in ensuring public safety?

Research Methods

This paper uses three different research methods to answer the proposed question. First and foremost, this paper uses documentary research methods for analysis of the responsibility for the crashes. Many articles and analyses have been written about the incidents and continue to be written to this day, assigning blame to everyone from Boeing engineers, the Federal Aviation

Administration (FAA), Lion Air, and Ethiopian Airlines. This paper uses documentary research methods to create a larger narrative from a multitude of documents surrounding an issue or event. Here, the documents were news searches for the Boeing 737 Max 8 following the accidents, with articles from the New York Times, the Washington Post, Bloomberg, and more. In addition, historical analysis will also be used in this paper to answer the question of what went wrong and led to the crashes. For the purposes of this paper, 'historical' refers to anything that happened prior to the investigation of the second crash. Much of the evidence used in this paper is compiled from historical documentation from the official NTSB investigation report on the accidents and government oversight documentation. Additionally, some information is pulled from the Challenger disaster as a point of comparison. Finally, this paper features discourse analysis, because there are so many differing views on the disasters and the results. Discourse analysis, broadly speaking, seeks to analyze textual evidence and varying positions on relevant issues (Ruiz, 2019). Documentary research and historical research provide many differing viewpoints, so discourse analysis will be used to string everything together and construct a position of academic value.

Background

The Boeing 737 Max 8 was a modified version of the tried and tested Boeing 737 equipped with more powerful engines. The new engines, CFM-LEAP models, were larger and more powerful than the previous engines, and as a result, Boeing made some structural changes to the wings and undercarriage to make room (Kitroeff, 2019). A side effect of this change was that the stall characteristics, the performance of the airplane at high angles of attack, were not up to federal standards. The angle of attack is the angle that the moving air hits the wing at, and for

most wings, the maximum safe angle of attack is around 20 degrees. Stall is the condition where a wing no longer generates lift, and a plane starts to fall out of the sky; this happens at around 20 degrees angle of attack, and is avoided at all times. To reach federal standards, Boeing implemented the Maneuvering Characteristics Augmentation System (MCAS), a piece of software designed to maintain control of the aircraft as it approached stall (Boeing, 2020). The MCAS system takes input from the angle of attack sensor on the aircraft, which detects the angle of attack, and determines if the aircraft is about to stall. If the system detects an imminent stall, it uses the elevator of the tail wing to pitch the nose down, which would recover a stall. According to the National Transportation Safety Board (NTSB) accident report, the direct cause of the two accidents was that the MCAS system malfunctioned and sent the plane into a nosedive in response to faulty angle of attack readings (NTSB, 2019). The angle of attack sensor was broken, and the MCAS system believed that the plane was dangerously close to stall, and used the elevator to force the plane to pitch down. The pilots in both cases tried to fight the system, but were overpowered by the hydraulic controls, and the planes crashed.

As a result of the accidents, the 737 Max 8 was grounded indefinitely. To date, the aircraft has been grounded for 12 months. Boeing lost 5.6 billion dollars in the second quarter of fiscal year 2019, with little improvement in the rest of the year, and a large proportion of Boeing's revenue stream grounded indefinitely (MacMillan, 2019). Major airlines flying the 737 Max also sustained heavy losses. American Airlines, for example, was projected to lose almost 350 million dollars in 2019 over the groundings, assuming the aircraft was back in service by August of 2019. The plane was not in service then, and is still not in service, and American

Airlines executives estimated they could lose as much as 180 million dollars per quarter until the plane is recertified by the FAA and put back into service (MacMillan, 2019).

Boeing, as a manufacturer of airplanes, is entrusted with providing safe, reliable airplanes to the public. Engineers at Boeing, like all professional engineers, are held by a code of ethics to "hold paramount the safety, health, and welfare of the public" (NSPE). The FAA was established by an act of Congress in 1958 to "provide for the safe and efficient use of national airspace" (FAA, 2017). Part of this responsibility is to ensure that all aircraft meet a standard of construction and safety to fly. The Airline Pilots Association establishes a code of ethics for pilots to uphold, which begins with "A pilot will keep uppermost in his mind that the safety, comfort, and well-being of the passengers who entrust their lives to him are his first and greatest responsibility" (ALPA, 2020).

Each of these parties had an opportunity to prevent the crashes of the Boeing 737 Max 8s. Boeing had years of development during which they could have made aerodynamic design changes. Instead, Boeing chose the cheaper route of adding a software patch to address the flaws of the system. The FAA could have required more testing on the airplane before certifying it, or by taking a more direct role in the safety evaluations. The pilots could have prevented the accidents by turning the system off; the Lion Air plane that crashed experienced the exact same problem on takeoff the night before the fatal accident, but a more experienced pilot was present, and turned off the autopilot system responsible for the erratic behavior (Langewiesche, 2019). The next morning, no such experienced pilot was there, and the plane crashed from the malfunction.

STS Framework

This STS research analyzes these questions, the role of the engineer in the disasters, and in public safety in general, through the framework of Co-Production. Co-production attempts to overcome the simplifications of technical determinism and social constructivism, focusing on how society and technology develop simultaneously and interact through mutual development (Jasanoff, 2004). This framework is useful in analyzing the socio-technical relationships at play with the disasters: the public puts its trust in those with technical knowledge, allowing the technology to develop society as long as the public feels comfortable. But in cases such as this, it becomes evident that society has a strong effect on the technology, as the backlash from the crashes immediately impacted the technical development of the 737 max and other planes.

Co-production has been used repeatedly to examine the interplay between science and governments, particularly as many nations were reconstructing after WWII. Michael Aaron Dennis used it to uncover the early development of science policy in the United States during the Truman administration. Vannevar Bush is commonly cited as the father of the National Science Foundation, and thus as the father of science policy in America, but Dennis used co-production to show how Bush's ideas became reality by intertwining political development and scientific development (Dennis, 2004). A common theme in co-production analyses is the motivation of a desired change by establishing a critical need in another field and linking the two. In this way a linked system is formed. Both Clark Miller and Claire Waterton and Brian Wynne describe the push for global climate awareness in this way. Miller argues that the Intergovernmental Panel on Climate Change (IPCC) was able to create a new global political order by simultaneously developing itself as an expert knowledge base, and focusing on the global effects of climate

change instead of the local ones (Miller, 2004). Waterton and Wynne make a similar case about the European Environment Agency's rise to political power (Waterton & Wynne, 2004).

The use of Co-production theory in this paper was carefully constructed, as Co-production has been critiqued as reducing power relationships between actors in a system (Boyle & Harris, 2009), which play a key role in the analysis of the interplay between regulators and engineers. Co-production has also been critiqued as being defined so broadly as to lose practical value, and a lack of fundamental understanding of the theory would lead to invalid analysis (Boyle & Harris, 2009). To ensure a valid conclusion was drawn, this paper is careful to limit its considerations of co-production so as to avoid the issue of breadth, and to consider the power dynamics at play, for example the FAA-Boeing relationship.

Results and Discussion

The ultimate failure that led to the deaths of 364 people was not a single technical one, rather, it was a failure where technical elements interacted. The fact that the pilots were not flying aces should not have been a fatal error, nor should a sensor malfunction. The fact that Boeing had a questionable software patch on the aircraft should not have been a fatal error, but the fact that the pilots were not informed of the patch was deadly. To avoid similar accidents in the future, engineers must understand that a safety culture is the co-production of engineering judgement and modeling and test data, and always act according to the engineering ethical code. Engineers must ensure that they are always aware of documented hazards, and complete analysis in a timely manner so such issues are not lost.

The Pilots

Legal culpability for an automobile accident typically falls on the driver who had the last chance to avert the accident and did not. In this case, such logic would place the blame and responsibility for the 737 Max crashes on the pilots. Indeed, airline pilots are held to a standard of ethics by the Airline Pilots Association that, first and foremost, the pilot is responsible for the wellbeing of the passengers (ALPA, 2020). The pilots could have averted disaster in this case, but does that mean the accidents were their fault? Boeing was aware that the MCAS system could be a major hazard; it could lead to runaway trim--the condition where the tail of the aircraft consistently forces the nose of the aircraft downward--and Boeing accounted for this in their safety analysis of the aircraft (NTSB, 2019). If a runaway trim condition were to occur, the pilot was supposed to disable the autopilot and fly the plane manually (NTSB, 2019). Boeing assumed that any pilot familiar with the 737 family would be able to recognize such a failure and know the corrective action from the flight manual. This assumption appeared to be validated when, on the night before the doomed Lion Air flight, that airplane experienced the exact same problem that would crash the plane the next day, when the MCAS system triggered runaway trim shortly after takeoff. But that night, there was a more experienced pilot in the cockpit, who recognized the runaway trim condition and performed the mitigation procedure: he turned off the autopilot (Langewiesche, 2019). It would appear that Boeing's assumption was correct, however, even the more experienced pilot took five minutes to solve the problem. Regardless, the pilots on both of the flights that crashed should have turned off the autopilot.

The natural question, though, is whose fault is it that the pilots did not pull the switches to disable the faulty system? A better question, is *why* did the pilots not pull the switches? The obvious answer is that they did not know to pull the switches. Langwiesche argues that this was

because the pilots were subpar, graduating from defunct pilot schools and lacking in 'airmanship,' the natural understanding of an airplane that fighter pilots have (Langewiesche, 2019). While there is certainly validity in claiming that a better pilot would have handled the situation better, the question is really whether the pilots can be expected to perform at that level. According to the NTSB, the answer is no. In the investigation report for the accidents, the NTSB noted that the pilots were subjected to a cacophony of errors and alarms while the MCAS system was activated, from a loud stall alarm to a shaker stick warning, not to mention the aerodynamic stresses and readings going haywire (NTSB, 2019). Under such conditions, the pilots were unable to identify the root cause of the problem, and the planes crashed. Indeed, even the pilot that saved the Lion Air flight the night before took almost five minutes to turn off the autopilot (Langewiesche, 2019). In Boeing's analysis, the pilots would be able to control the situation in a matter of seconds, not minutes (NTSB, 2019). Therefore, Boeing's analysis was flawed, and blaming the pilots for the accidents is altogether too harsh a statement.

Boeing

The next natural question is what went wrong in the Boeing analysis? When Boeing submitted the 737 Max to the FAA for approval, the MCAS system was included in the risks, and testing had been conducted that concluded the pilots could appropriately respond to the MCAS failure. It has already been demonstrated here that this was not the case. In their analysis, Boeing had used a simulator to test the pilot response to the same serious MCAS failure that led to the disasters; the pilots all responded appropriately: they recognized the issue from the autopilot and disabled the system (NTSB, 2019). The issue was with the experimental setup: Boeing did not simulate any effects other than the runaway trim--no alarms, no

warnings--because they only wanted to test the response to the runaway trim (NTSB, 2019). By eliminating the confounding variables from the experiment, they hoped to get a clearer response of the dependent variable, but actually deviated too far from reality to obtain a relevant response. The first major failure that led to the accidents was Boeing's flawed analysis assuming that the pilots would be able to respond to a runaway trim caused by MCAS easily.

Regulatory Failure

The next important question to answer is: why did the FAA accept the safety tests conducted by Boeing? In short, the FAA had delegated responsibility for certifying Boeing's aircraft to Boeing, through a branch called the Boeing Aviation Safety Oversight Office (BASOO), responsible for checking Boeing's compliance with FAA procedures in all submitted safety documents (Joint Technical Authorities Review, 2019). Due to budget cuts, the BASOO had less manpower to check Boeing's work, and was under informed about the MCAS system, so the system was approved despite the experimental flaws detailed previously (Joint Technical Authorities Review, 2019).

A better question then is: why was the FAA budget cut for oversight of Boeing? The FAA is a public institution, tasked with ensuring that air travel is safe for the people of the United States. Under this directive the FAA regulates all the major manufacturers looking to sell their planes to US airlines. The FAA is only as strong as it needs to be to ensure the public that flying is safe. But over the last few decades, the public has gradually developed more trust in the aviation industry as more and more focus is put on safety and yearly accident rates dwindle (Smith-Spark, 2019). As a result, the public cares less and less about the FAA, and its budget changes to suit. In 2017, the year of the 737 Max's certification, the arm of the FAA tasked with

oversight had the same budget it had for the previous seven years, and it was shifting resources to unmanned aerial systems (FAA budget, 2017)(FAA, 2009). It is easy to see how the public opinion is intertwined with aircraft technology-as the manufacturers get better at making airplanes, the public puts less regulatory pressure on them. What went wrong here that led to the accidents happen is that Boeing has steadily improved at making airplanes. The root issue here is that the safety culture responsible for public safety is co-produced by public opinion and airplane manufacturers. The co-produced idiom is like a leaky valve: it gradually gets more and more open until disaster strikes, at which point it is tightened again and the system 'resets.'

What can be Done

Having established what went wrong in the accidents: that Boeing did not properly account for the full conditions of MCAS failure and that the FAA, and society had become complacent in regulating Boeing, it is now time to address what engineers should have done differently. For the first issue, there were a multitude of engineering decisions that should have been made differently. By statistics, 50% of all pilots have below average skills, yet the public demands a failure rate of as close to zero as is possible. Therefore, even the bottom 1% of pilots need to be able to safely fly airplanes in all but catastrophic situations. Engineers designing airplanes must always remember this fact. Indeed, the airplane manufacturer Airbus was founded on this philosophy (Langewiesche, 2019). Specifically, Boeing engineers should have carefully assessed the MCAS failure test that was evidence for the safety of the aircraft and determined that it was not realistic. At this point they could have set up a better test and performed it to see that the problem really was worse. Instead, the engineers accepted the results without much thought and submitted them to the FAA. The best solution would not have

required more testing, or even realizing that a pilot would not handle a runaway trim very well. All Boeing needed to do was tell people that the system existed, and under rare circumstances could cause a runaway trim. Such a statement would go in the checklists in the cockpit that pilots study in depth before flying an aircraft. In most cases, when an anomaly occurs in flight, as in the disastrous flights, the pilots go to their checklists immediately (Langewiesche, 2019). If the issue had been documented there, then the pilots would have easily solved the problem. There is a central ethical pillar in engineering: never make false or misleading statements (NSPE, 2019), and in essence Boeing's engineers made misleading statements by omitting details on the aircraft from the manual. An engineer studying this case should simply follow the tenets of engineering ethics to avoid a similar situation in the future.

The socio-technical relationship that led to the failure of the FAA-Boeing system is a much harder problem to solve. The same kind of co-produced system is often seen in engineering safety analyses, particularly when engineers get complacent in light of past successes. A good example of this was the Challenger disaster. In the years prior to the space shuttle deployment, NASA managers and engineers had expressed concern over the inadequacy of the solid rocket motor joints--the components that failed on Challenger (Rogers et. al, 1986). But in 1985--the year before Challenger, NASA officially accepted the risk of the joints, citing past flights without failure (Rogers et. al, 1986). The safety requirements in that case, just as with the Boeing 737 Max 8, were the result of a co-production of engineering expertise and past experience. As the past experience builds, the successful missions, the years of safe flying, the engineering expertise is overpowered, and safety requirements become relaxed. Just as NASA

did in 1985, the FAA did in 2017, choosing to trust previous safe flights in the absence of compelling engineering insight.

To solve such a problem requires understanding the co-production of safety culture. In the early stages of engineering design, safety takes a dominant position in the culture, and all estimates of safety come from engineering judgement. At an early stage, this judgement is usually quite conservative, to account for uncertainty while preserving safety. After tens or hundreds of tests, safety is primarily defined by test data, unless the engineers have compelling evidence that the data is incomplete or erroneous. Safety standards in engineering are co-produced by these two forces, and develop as the two influences change. Therefore, to eliminate the problems arising from such a system there are then two options. First, the system for deriving safety standards can be restructured: establishing a minimum level of scrutiny that must always be used, essentially minimizing the effects of co-production. However, this option is problematic. Initial estimates usually overestimate risks to ensure safety, so initial scrutiny standards would be too strict. As test data comes in, risk levels are more accurately known, and scrutiny levels can fall to a more reasonable level. Also, higher safety standards lead to slower production and higher cost, time and money that are wasted when the standards are unreasonably high.

The second option is to maintain the influence of engineering at a constant level. In the 737 Max and Challenger cases, the MCAS system and solid rocket motor joints were initially labeled as a "major hazard" and a "critical design risk," respectively (NTSB, 2019) (Rogers et. al, 1986). However, in both cases, these characterizations were set early on and then left there with little follow up, and safety standards became dominated by previous test experience. If

engineers had continually assessed the risks associated with the major hazards, and emphasized their existence, then the safety culture would have remained more cautious. In general, it is the responsibility of the safety engineer to continually revise the safety models and assessments to ensure that nothing is overlooked, and that proper caution is maintained when using or implementing risky systems.

This paper has multiple limitations that must be acknowledged before going forward. First and foremost, this research has been compiled from others' research and opinion writings. Not all of the pieces used were written by experts or engineers with direct knowledge or involvement with the accidents. The author performed no investigations, and used only documentary research. Along the same lines, the opinions represented in this paper come predominantly from western authors, because they are the pieces written in English. As a result, some key perspectives have not been fully represented, most notably that of Lion Air and Ethiopia Airlines, and any of the pilots from those airlines. It is easy to judge the airlines from the western perspectives available to English speakers, but both airlines operate in sovereign nations with different laws from the United States, and that must be taken-into-account when judging their actions. Finally, this paper was constrained by time, in two ways. First, it was written over the course of two semesters, while taking other classes and participating in other activities. To do this topic justice would require more time writing. Also, the accidents that are the subject of this paper occurred recently, and not enough time has passed for a complete analysis. New updates are still coming out to this day.

Therefore, this paper is inherently incomplete. The topic of the Boeing 737 Max 8 should be revisited in a few years when the airplane is back in service and updates have stopped

emerging. Ideally, researchers in a few years time will be able to produce a report on the accidents in the form of the Rogers Commision Report after Challenger, with detailed interviews and first-hand investigations. Such a report would be far more effective at bringing to light the failures described here.

Conclusion

When 346 people died aboard two brand new airplanes, a compendium of engineering failures came to a head. Boeing engineers did not act in accordance with ethical tenets, at a point when the co-produced safety culture was weak. An engineer reading this paper should recognize their responsibility is just like that of the Boeing or NASA engineers. First and foremost, an engineer must act in accordance with the code of ethics, and be careful in performing their analyses. Engineers must also recognize that many safety cultures are co-produced, and that any co-produced safety culture can decay in the same way that the ones documented here did. An understanding of this mechanism allows the engineer to be more vigilant, and ensure that standards do not drop to unsafe levels. Finally, the engineer should ensure that there is minimal delay in handling critical safety components so that the importance of said components is not diminished over time. Had Boeing's engineers not made these errors, the 737 Max 8 disasters would never have happened.

Works Cited

ALPA. (2020). Advancing Aviation Safety and Security Since 1931. Retrieved from https://www.alpa.org/en/about-alpa/what-we-do/code-of-ethics

Boeing. (2020). 737 Max Software Updates. Retrieved from https://www.boeing.com/commercial/737max/737-max-software-updates.page

Dennis, M. A. (2004). Reconstruction sociotechnical order: Vannevar Bush and US Science Policy. In *States of Knowledge : The Co-Production of Science and the Social Order* (pp. 225–253). New York, NY: Routledge.

FAA. (2009). *Budget Highlights: Fiscal Year 2010*.

FAA. (2016). *Budget Estimates: Fiscal Year 2017* (pp. Operations-AVS-1-Operations-AVS-35).

FAA. (2017, January 4). A Brief History of the FAA. Retrieved from https://www.faa.gov/about/history/brief_history/

Joint Authorities Technical Review. (2019). *Boeing 737 Max Flight Control System Observations, Findings, and Recommendations*.

Kitroeff, N. (2019, September 26). Boeing Underestimated Cockpit Chaos on 737 Max, N.T.S.B. Says. Retrieved September 25, 2019, from https://www.nytimes.com/2019/09/26/business/boeing-737-max-ntsb-mcas.html.

Langewiesche, W. (2019, September 18). What Really Brought Down the Boeing 737 Max? Retrieved from https://www.nytimes.com/2019/09/18/magazine/boeing-737-max-crashes.html?smid=nytcore-ios-share.

Miller, C. A. (2004). Climate Science and the Making of a Global Political Order. In *States of Knowledge : The Co-Production of Science and the Social Order* (pp. 46–66). New York, NY: Routledge.

NTSB. Assumptions Used in the Safety Assessment Process and the Effects of Multiple Alerts and Indications on Pilot Performance, Assumptions Used in the Safety Assessment Process and the Effects of Multiple Alerts and Indications on Pilot Performance (2019). Retrieved from https://www.ntsb.gov/investigations/AccidentReports/Reports/ASR1901.pdf

NSPE. (n.d.). Code of Ethics. Retrieved from https://www.nspe.org/resources/ethics/code-ethics.

Rogers, W. P., Armstrong, N. A., Acheson, D. C., Covert, E. E., Feynman, R. P., Hotz, R. B., … Yeager, C. E. (1986). *Report to the President By the Presidential Commission On the Space Shuttle Challenger Accident*.

Smith-Spark, L. (2019, January 3). Plane crash deaths rise in 2018 but accidents are still rare. Retrieved December 8, 2019, from https://www.cnn.com/2019/01/02/health/plane-crash-deaths-intl/index.html.

Waterton, C., & Wynne, B. (2004). Knowledge and Political Order in the European Environmental Agency. In *States of Knowledge : The Co-Production of Science and the Social Order* (pp. 67–86). New York, NY: Routledge.