

What the Processing Industry Must Learn from the Boeing 737 MAX Crashes

Richard Carter, P. Eng., F.S. Eng. (TÜV Rheinland), ACM Facility Safety Inc., 926 5th Ave SW, Calgary, rcarter@acm.ca

Introduction: Two Surprisingly Similar Industries

At first glance, it would appear that there is not much a processing facility can learn from an aviation disaster. In reality, however, there are many similarities between aviation safety and process safety, and therefore lessons learned in one of these industries are valuable to the other.

Both a commercial aircraft and an operating plant involve continuous, or extended, operation of sophisticated pieces of equipment with complex physical parts, control systems, programming, and human factors. Both are operated by trained and experienced personnel who are required to monitor a system for many hours at a time, yet are still required to respond within a manner of seconds to an abnormal situation. Both have the potential for highly hazardous scenarios to occur, and both rely on a variety of automatic and manual controls to prevent severe outcomes if something goes wrong. So, when a failure of any kind is identified in either industry, it is important to ask what the other industry can also learn from these incidents.

Catastrophic scenarios in the aviation and process industries almost always happen because of multiple failures in different stages of a project, and at many levels within each organization. The two Boeing 737 MAX crashes, which killed 346 people and caused all aircraft of this type worldwide to be grounded, were no different and involved failures at many levels within the process safety management system. After these incidents have happened, all we can do is search for and apply as many lessons as we can to prevent similar scenarios from occurring in the future.

It is not within the scope of this paper to cover every one of the myriad items that led to these events. Instead, it will focus on some key lessons to be learned from the set of circumstances which created the conditions that allowed these crashes to occur. In particular, it will discuss the following learnings:

- Pushing to meet financially-driven deadlines can jeopardize safety
- Undue focus on financial considerations can cause companies to hide or ignore important warning signs
- Critical instrumentation and equipment may need redundancy to meet required reliability
- It is dangerous to assume that someone who is familiar with a “similar” system will take the correct action every time in a high-pressure and high-stress situation
- If the design is significantly changed, the risk assessment must be revalidated
- Not fully understanding how a control system works can lead to unidentified risks
- If any safeguards are removed from the design, or discovered to be inoperable, the risk assessment is no longer valid and needs to be revalidated
- Every so-called “near-miss” is an opportunity to stop the full scenario from occurring in the future

Each one of these lessons is an activity or priority that, if heeded, can prevent future disastrous accidents from occurring. To that end, this paper will also discuss how process safety management approaches could have prevented these vulnerabilities, based on the Center for Chemical Process Safety’s risk based process safety management (RBPSM) system.

The Cause of the Crashes: the Maneuvering Characteristics Augmentation System (MCAS)

The key system that led to these incidents is called the Maneuvering Characteristics Augmentation System (MCAS). The MCAS is designed to automatically stabilize the plane if it is close to a stall, a condition in which there is not enough airflow over the wings to cause lift, and which can cause the plane to fall. The plane has an angle-of-attack (AoA) sensor that detects the direction of airflow compared with the orientation of the aircraft (see Figure 1). When the angle of attack is too great, the MCAS activates and moves the horizontal stabilizer, which pushes the nose of the aircraft down to reduce the angle of attack (HTCI, 2020).

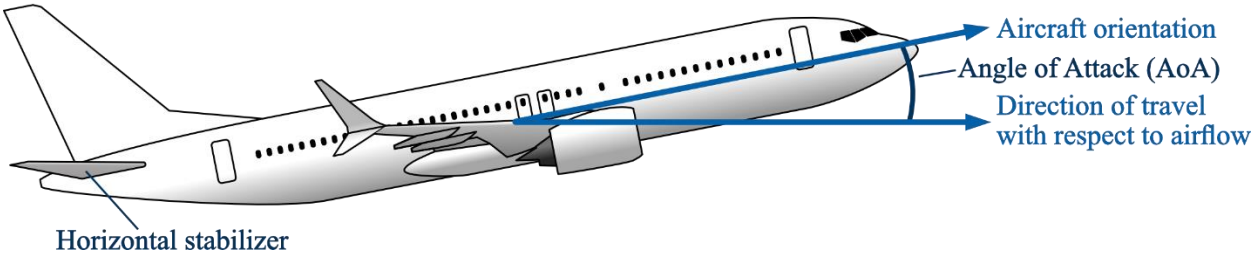

Figure 1. Explanation of Angle of Attack and Location of Horizontal Stabilizer

The 737 MAX has larger engines than its predecessors which required being placed farther forward on the wing to avoid dragging on the ground, thus changing the flight dynamics of the plane. The MCAS was implemented in order to provide additional stability. This also made the plane feel more like its predecessors for the pilots and so theoretically reduced the training required to operate.

In both 737 MAX crashes, the MCAS system activated when it should not have due to incorrect information from the AoA sensor (HCTI, 2020). The system thought the plane was stalling, so it moved the horizontal stabilizer to push the nose down, which in both cases caused the plane to enter a dive from which the flight crew could not recover.

Lessons to Learn

Pushing to meet financially-driven deadlines can jeopardize safety

It is well-known that tight budgets and short schedules can negatively impact safety, but it requires constant vigilance to prevent economic or schedule pressures from degrading the safety management systems in place within any organization. Boeing had originally been considering developing a brand-new aircraft since 2005. However, after learning in 2011 that American Airlines was going to purchase hundreds of Airbus airplanes it shifted focus to “re-engining” the 737 NG into the 737 MAX to stay competitive. The 737 MAX development program was under intense pressure to compete with the rival Airbus A320neo. Senior Boeing management installed “Countdown Clocks” in their conference room to remind employees of the importance of keeping to the program schedule (HTCI, 2020). This resulted in decreased project supervision and more-rushed certification.

The Federal Aviation Administration (FAA) had increasingly delegated risk assessments to the plane manufacturers, citing lack of funding and resources as the reason. The FAA decided which parts of the safety certification process to keep in-house, and which to delegate to Boeing. Some personnel at Boeing were “Authorized Representatives” (AR), who had authority to approve items on the FAA’s behalf. Since the ARs were employed by Boeing, there was an incentive for the ARs to support Boeing’s financial interests. While the ARs are intended to be impartial, it can be very difficult to remain that way if your paycheques are written by the company that you are overseeing. Indeed, a November 2016 internal Boeing survey found that 39% of Boeing ARs said they had experienced “undue pressure” and that 29% said they were concerned about “consequences” if they reported these incidents (HCTI, 2019).

One of the four foundational blocks of the CCPS’s RBPSM system is **Commit to Process Safety**. It is clear that this was defeated in this instance. A key element within this foundation block is **Process Safety Culture**. The culture of any company influences, and is influenced by, “how we behave when no one is watching” (CCPS, 2007). In this case, without the FAA watching closely, the financially-focused attitudes of the organization were allowed to come to the forefront and create an environment that focused on finances at the expense of safety. This undermined the other pillars within the remaining three foundational blocks of **Understand Hazards and Risk, Manage Risk**, and **Learn from Experience**, as we will see in the upcoming sections.

Undue focus on financial considerations can cause companies to hide or ignore important warning signs

Boeing had significant financial incentive to avoid the requirement for simulator training for pilots transitioning to the 737 MAX from its predecessor. For example, in a 2011 contract with Southwest Airlines, Boeing would have had to lower each plane's price by $1 million if simulator training were required – a total potential loss of $200 to $400 million (HCTI, 2020). This created pressure to minimize or hide any information that could indicate that simulator training would be required due to installation of the MCAS system.

In November 2012, during a flight simulator test session, a Boeing test pilot required more than ten seconds to respond to a scenario of an uncommanded activation of the MCAS. This was deemed as "catastrophic" by the test pilot (HTCI, 2020). As per the FAA's guidelines, pilots should be able to respond to this situation within four seconds. This information was communicated several times between 2015 and 2018, but was never communicated outside of Boeing, despite at least four Boeing ARs being aware of this issue.

Furthermore, a Boeing internal meeting in 2013 concluded not to mention MCAS outside the company, and it was also removed from the pilot training manuals with FAA approval in 2016 (HCTI, 2020).

The key RBPSM elements that failed here are **Stakeholder Outreach** and **Training and Performance Assurance**. Important information was hidden from the pilots, with Boeing even going so far as to remove references to the MCAS from the pilot training manuals. An airline that reached out to ask for additional training was mocked internally. The pilots on these aircraft didn't know that this system was in place, and therefore could not fix it when it acted incorrectly. If the pilots had been more involved, or if they had been at the least made aware of this system's existence and what it could do, they may have been able to identify and the cause of the malfunction and avert these disasters.

Critical instrumentation and equipment may need redundancy to meet required reliability

The aircraft was fitted with two angle-of-attack (AoA) sensors, however the MCAS only took information from one of them. Concerns regarding the potential for a faulty AoA sensor to incorrectly activate the MCAS were raised multiple times during the course of development of the aircraft (HCTI, 2020). Furthermore, AoA sensors are known to be susceptible to damage from ground crews or bird strikes.

The design included an "AoA disagree" alarm to alert the flight crew if the two AoA sensors reported significantly different values, and trusted in the flight crew's ability to manually correct for the malfunction. This alarm, however, was not present on the majority of the 737 MAX aircraft, as discussed later in this paper.

The key element of RBPSM that failed in this area was **Asset Integrity and Reliability**. Each component and system must have a reliability appropriate to its situation. By increasing the reliability of the angle of attack measurement system, the MCAS would have been less likely to have activated in this catastrophic fashion.

It is dangerous to assume that someone who is familiar with a "similar" system will take the correct action every time in a high-pressure and high-stress situation

The risk assessment conducted for the aircraft assumed that pilots would identify an unnecessary activation of the MCAS and override it accordingly (HCTI, 2020). However, pilots were not even made aware of this system and so did not know what the problem was. The MCAS was not mentioned in the flight manuals and as no simulator training was required, pilots did not have the opportunity to practice responding to such a malfunction. Because of the way the MCAS would repeatedly activate, instead of continuously moving the horizontal stabilizer, it was not clear to the pilots what was wrong and so they didn't know what action to take.

When discussing a potential hazardous scenario of a risk assessment, the cause is usually known and clear to the risk assessment team. In an emergency situation, however, it is often not clear what the cause of the scenario is. Therefore, there is a danger of overestimating how quickly and easily personnel will be able to identify and correct the cause of the failure. The risk assessment assumed that if the horizontal stabilizer moved suddenly, the pilot would realize what was wrong, override the MCAS, and continue flying normally. The assumption in this risk assessment was that, because the aircraft was similar to its predecessor, the pilot's training in emergency situations would be adequate. We know now that the pilots were not aware of the MCAS system and therefore could not have identified the true cause of the malfunction. Even if they had known of this system, however, it is dangerous to assume that they would correctly identify the malfunction every time.

The RBPSM elements to study here are **Hazard Identification and Risk Analysis** and **Emergency Management**. If the hazard analysis study had conducted a more thorough review of the pilot's likely response to this scenario occurring during a routine flight, it may have concluded that the pilot identifying the failure and responding correctly could not be fully relied upon and further protection was required. Furthermore, emergency management plans need to take into account that in high-stress situations humans cannot be relied upon to do the right thing unless the required response is trained and practiced extensively and often. As one witness to a workplace explosion said, "you think come an emergency you're just going to jump on top of things and be just like the TV and, you know, Superman and save everybody. It's funny, it gets surreal. And I couldn't even remember how to dial 911" (CSB, 2011). While aircraft flight crew have a high level of training and competency requirement in emergency response, they are still susceptible to human error in high-pressure situations.

If the design is significantly changed, the risk assessment must be revalidated

Even seemingly minor changes to design limits can have large, unforeseen impacts, which is why Management of Change (MOC) is so important. At the time of the risk assessment, the MCAS was only designed to be able to move the horizontal stabilizer up to 0.6 degrees (out of a maximum range of about 5 degrees). During later test flights, it was determined that this number needed to be higher to be able to respond adequately under low airspeed conditions, so it was increased to a maximum of 2.5 degrees – more than four times the original design (HCTI, 2020). The design change was not adequately communicated, and not all documentation was updated appropriately, and therefore this modification was not adequately analyzed for its potential to cause a hazardous event.

It is clear that the key element of RBPSM here is **Management of Change**. Whenever something changes, either in the design phase or in an operating facility, that change needs to be reviewed to determine if it introduces any new hazards or increases the risk of any existing hazards. This increase in power of the system by a factor of four had a significant impact on the real-world result of an incorrectly-activated MCAS. During the risk assessment, it was assumed that the impact to the aircraft's flight would be relatively minor, and easily corrected. In reality, the MCAS activating could move the horizontal stabilizer by half of its operating range, which put the plane in a catastrophic dive unless corrected immediately. This is a significant design change that should have been subject to an MOC process to identify any new or increased risks, however it was not studied and the hidden risk remained.

Not fully understanding how a control system works can lead to unidentified risks

Even accounting for the modification described above, the MCAS was only supposed to be able to move the horizontal stabilizer by a maximum of 2.5 degrees. But in reality, this limit was 2.5 degrees per *activation*, and it could activate multiple times. So what happened was:

1. The AoA sensor erroneously reported a high angle of attack;
2. The MCAS activated and moved the horizontal stabilizer by 2.5 degrees, unnecessarily;
3. The pilots used a switch on their control column to move the stabilizer in a corrective action;
4. The MCAS, still thinking the plane is about to stall, re-activated and moved the stabilizer by another 2.5 degrees – now 5 degrees total, the full limit of movement of the stabilizer;
5. Each time the pilot tried to correct, the MCAS would push the stabilizer back to maximum angle.

Without knowing that the MCAS existed, the pilots could not successfully troubleshoot the problem. Therefore, there are two disconnects here: the lack of training provided to the pilots on the MCAS, and the difference between how the MCAS was intended to work and how it actually worked.

These two failures could have been corrected with the RBPSM elements **Training and Performance Assurance**, which has been discussed above, and **Hazard Identification and Risk Analysis**. When conducting the risk analysis for the system, it should have been identified that the MCAS could activate repeatedly and that it might not be clear to the pilots what was causing the horizontal stabilizer to move. If this had been identified, the system could have been restricted so that it could only activate once in a certain time frame, or a certain number of times before the pilot was required to confirm that its influence was desired. Alternatively, it could have highlighted the need for the pilots to know about the MCAS system and how to bypass it in the event of a malfunction.

If any safeguards are removed from the design, or discovered to be inoperable, the risk assessment is no longer valid and needs to be revalidated

The MCAS system was designed with an AoA sensor disagree alarm, which would alert the pilots in the event that the AoA sensors were reading different values. This would indicate that one of the sensors had malfunctioned, and help the pilots troubleshoot the scenario. However, the software for this alarm was routed through an optional angle-of-attack indicator instrument, which was not installed on most 737 MAX aircraft produced (HCTI, 2020). Therefore, most of the aircraft did not have working AoA sensor malfunction alarms, even though it was required as part of the design. This defeated a critical safeguarding strategy that had been relied upon when developing the design and hazard analysis.

It was discovered that Boeing knew about this deficiency, but did not inform the FAA or client airlines until after the first crash in October 2018. Even with that new information, however, the airlines could not identify the key hazard and consequence of MCAS activation, because airlines and pilots were unaware that the MCAS system existed.

The pertinent RBPSM element here is **Management of Change**. In this case, the lack of an AoA sensor disagree alarm is a change in the safeguarding philosophy of the system, and should have been subject to an MOC process as soon as it was discovered, as it was the only thing that could reliably tell the pilot what the malfunction was.

Every so-called "near-miss" is an opportunity to stop the full scenario from occurring in the future

As Dr. Trevor Kletz, one of the founders of modern process safety management, has said, "…it's also in human nature, there's a tendency to say, 'oh gosh, that was a near one…let's forget about it and get on with the job'" (CSB, 2013). It is important to think of these events not as "near-misses" but rather "near-hits", and investigate and follow up on them as such. Each time a scenario almost occurs but is avoided, it is an opportunity to find out what could have happened and why, and apply those learnings to prevent the worst case from happening in the future.

On the day before the first fatal 737 MAX crash, the same aircraft was flying from Denpasar to Jakarta and experienced an incorrect reading from the left AoA sensor that caused incorrect activation of the MCAS system. One of the pilots on the flight deck identified the cause of the unexpected movement of the horizontal stabilizer and correctly identified how to deactivate the faulty system. Upon arriving safely at Jakarta the cautions and warnings that appeared during the flight were logged, but an explain of how the crew were able to deactivate the faulty system was not included (HCTI, 2020). This was a "near-hit" that could have saved many lives had it been communicated to the crew that flew the same aircraft the next day, and shared with other pilots and airlines operating 737 MAX aircraft.

This was a failure of the **Incident Investigation** element of RBPSM. A strong PSM program includes the investigation of all process incidents with the potential for harm, whether they cause harm or not on that occasion. Any time a severe outcome is narrowly avoided, it needs to be analyzed to determine what went wrong and how it can be prevented in the future. Every operating facility needs to have a robust system for identifying and investigating "near-hit" incidents, and communicating and taking actions on the findings of the investigation.

Conclusion

An old saying relayed by Dr. Trevor Kletz is "if you think safety is expensive, try an accident" (CSB, 2013). It has been shown in this paper that the failures that led to these crashes were allowed to happen due to economic pressures caused by competition from Airbus, as well as from the revenue that would be lost if pilots required simulator training on the 737 MAX. This led to a series of decisions that set the pilots up for failure on the day of the accidents, by providing them with a system that worked differently than was intended and communicated, did not have critical redundancy in place, and about which the operators were missing critical information. These decisions were made with the intent to save Boeing a few hundred million dollars; however, these incidents have cost Boeing nearly USD$19 *billion* (HTCI, 2020), with some estimating the total cost will be USD$23 billion or more (CNN, 2020).

To provide the best process safety management programs, it is important to incorporate as many learnings as possible. The aviation industry is an excellent source of information on potential hazardous scenarios, as well as methods of preventing and mitigating these disasters. The Boeing 737 MAX crashes can teach us many lessons about process safety, spanning management of projects, risk assessment requirements, regulatory oversight, and expectations of the operations group.

These disasters could have been prevented at any of the points discussed in this paper. These incidents reveal the need for continuous focus and effort on safety, and to avoid letting schedule and financial concerns jeopardize safe design and adequate training.

Follow these steps to improve process safety at your facility:

- Understand what is keeping your people, assets and the environment safe, and ensure that it is as reliable as it needs to be.
- Conduct risk assessments to uncover potentially hazardous scenarios, and update them whenever the design changes, or deviations from the design intent are discovered.
- Seek out potential safety issues, and take steps to mitigate them.
- Maintain transparency with your personnel, peers and regulators to allow for continuous improvement in process safety. Concealing information now may cause a much larger issue later.
- Ensure all risks, deficiencies and concerns are tracked, studied, and any required actions are followed through to conclusion.
- Investigate all incidents that had the potential to cause harm and take appropriate actions to prevent the harm from occurring in the future.
- Remember: “If you think safety is expensive, try an accident.”

References

1. Center for Chemical Process Safety (CCPS), 2007, Guidelines for Risk Based Process Safety, John Wiley & Sons
2. Center for Chemical Process Safety (CCPS), Guidelines for Risk Based Process Safety: A summary of risk based process safety (RBPS) management approach as detailed in Guidelines for Risk Based Process Safety, https://www.aiche.org/sites/default/files/docs/summaries/rbps.pdf
3. CNN, 2020, The cost of the Boeing 737 Max crisis: $18.7 billion and counting, https://www.cnn.com/2020/03/10/business/boeing-737-max-cost/index.html
4. The House Committee on Transportation & Infrastructure (HCTI), 2019, The Boeing 737 MAX: Examining the Design, Development, and Marketing of the Aircraft: Hearing Before the Committee on Transportation and Infrastructure House of Representatives, https://www.govinfo.gov/content/pkg/CHRG-116hhrg38282/pdf/CHRG-116hhrg38282.pdf
5. The House Committee on Transportation & Infrastructure (HCTI), 2020, Full Committee Report on The Design, Development & Certification of the Boeing 737 MAX, https://transportation.house.gov/committee-activity/boeing-737-max-investigation
6. US Chemical Safety Board (CSB), 2011, Deadly Practices, https://www.youtube.com/watch?v=rjxBtwl8-Tc
7. US Chemical Safety Board (CSB), 2013, Remembering Trevor Kletz, https://www.youtube.com/watch?v=XQn5fL62KL8