Flawed analysis, failed oversight: How Boeing, FAA certified the suspect 737 MAX flight control system

Dominic Gates

March 17, 2019 at 6:00 am Updated March 21, 2019 at 9:46 am

By

Seattle Times aerospace reporter

As Boeing hustled in 2015 to catch up to Airbus and certify its new 737

MAX, Federal Aviation Administration (FAA) managers pushed the agency's safety engineers to delegate safety assessments to Boeing itself, and to speedily approve the resulting analysis.

But the original safety analysis that Boeing delivered to the FAA for a new flight control system on the MAX — a report used to certify the plane as safe to fly — had several crucial flaws.

That flight control system, called MCAS (Maneuvering Characteristics Augmentation System), is now under scrutiny after two crashes of the jet in less than five months resulted in the FAA's March 13 order to ground the plane.

Current and former engineers directly involved with the evaluations or familiar with the document shared details of Boeing's "System Safety Analysis" of MCAS, which The Seattle Times confirmed.

The safety analysis:

- Understated the power of the new flight control system, which was designed to swivel the horizontal tail to push the nose of the plane down to avert a stall. When the planes later entered service, MCAS was capable of moving the tail more than four times farther than was stated in the initial safety analysis document.
- Failed to account for how the system could reset itself each time a pilot responded, thereby missing the potential impact of the system repeatedly pushing the airplane's nose downward.
- Assessed a failure of the system as one level below "catastrophic." But even that "hazardous" danger level should have precluded activation of the system based on input from a single sensor — and yet that's how it was designed.

The people who spoke to The Seattle Times and shared details of the safety analysis all spoke on condition of anonymity to protect their jobs at the FAA

and other aviation organizations.

Both Boeing and the FAA were informed of the specifics of this story and were asked for responses 11 days ago, before the second crash of a 737 MAX on March 10.

Late on the 15th, the FAA said it followed its standard certification process on the MAX. Citing a busy week, a spokesman said the agency was "unable to delve into any detailed inquiries."

Boeing responded March 16 with a statement that "the FAA considered the final configuration and operating parameters of MCAS during MAX certification, and concluded that it met all certification and regulatory requirements."

Adding that it is "unable to comment ... because of the ongoing investigation" into the crashes, Boeing did not respond directly to the detailed description of the flaws in MCAS certification, beyond saying that "there are some significant mischaracterizations."

Several technical experts inside the FAA said October's Lion Air crash, where the MCAS has been clearly implicated by investigators in Indonesia, is only the latest indicator that the agency's delegation of airplane certification has gone too far, and that it's inappropriate for Boeing employees to have so much authority over safety analyses of Boeing jets.

"We need to make sure the FAA is much more engaged in failure assessments and the assumptions that go into them," said one FAA safety engineer.

Certifying a new flight control system

Going against a long Boeing tradition of giving the pilot complete control of the aircraft, the MAX's new MCAS automatic flight control system was

designed to act in the background, without pilot input.

It was needed because the MAX's much larger engines had to be placed farther forward on the wing, changing the airframe's aerodynamic lift.

Designed to activate automatically only in the extreme flight situation of a high-speed stall, this extra kick downward of the nose would make the plane feel the same to a pilot as the older-model 737s.

Boeing engineers authorized to work on behalf of the FAA developed the System Safety Analysis for MCAS, a document which in turn was shared with foreign air-safety regulators in Europe, Canada and elsewhere in the world.

The document, "developed to ensure the safe operation of the 737 MAX," concluded that the system complied with all applicable FAA regulations.

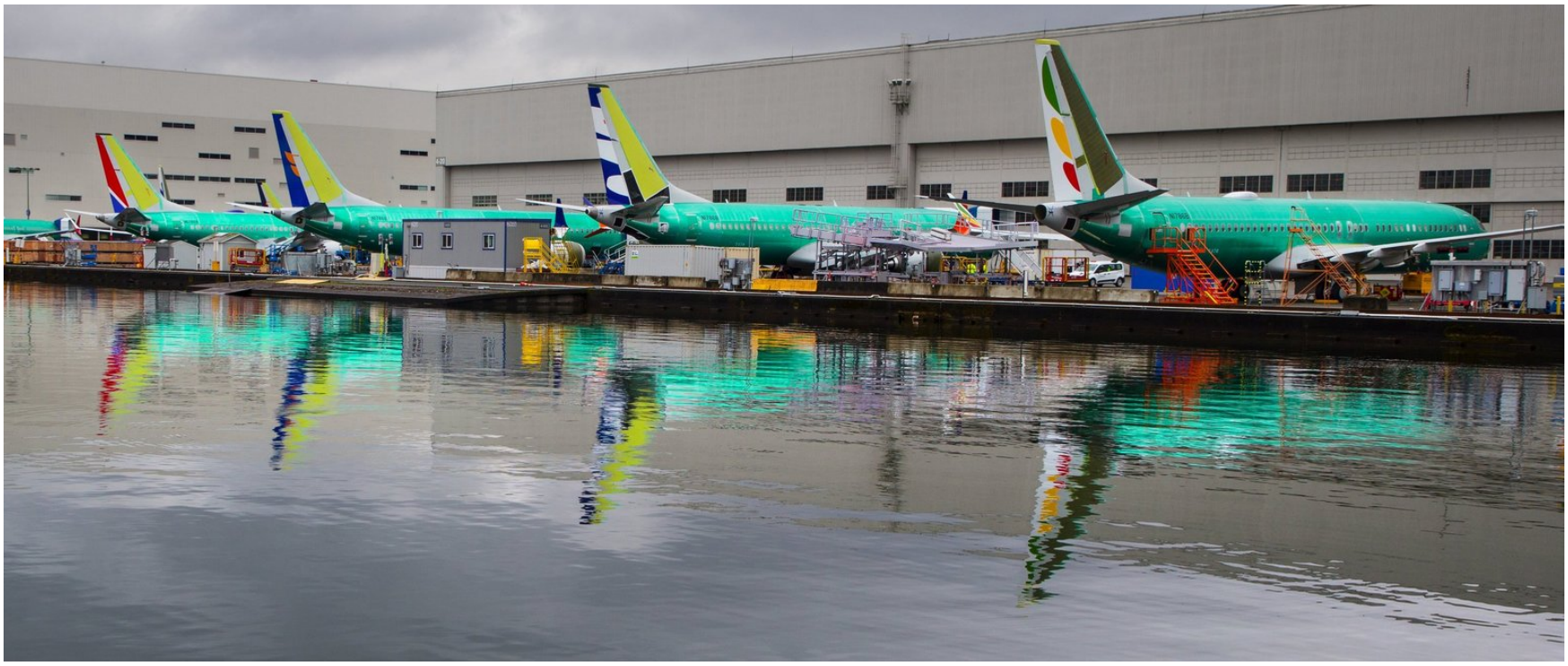
Yet black box data retrieved after the Lion Air crash indicates that a single

faulty sensor — a vane on the outside of the fuselage that measures the plane's "angle of attack," the angle between the airflow and the wing — triggered MCAS multiple times during the deadly flight, initiating a tug of war as the system repeatedly pushed the nose of the plane down and the pilots wrestled with the controls to pull it back up, before the final crash.

When announcing the grounding of the 737 MAX, the FAA cited similarities in the flight trajectory of the Lion Air flight and the crash of Ethiopian Airlines Flight 302.

Investigators also found the Ethiopian plane's jackscrew, a part that moves the horizontal tail of the aircraft, and it indicated that the jet's horizontal tail was in an unusual position — with MCAS as one possible reason for that.

Investigators are working to determine if MCAS could be the cause of both crashes.



Boeing 737 MAX planes sit in a row last week behind the Renton plant on the south shore of Lake Washington. (Mike Siegel / The Seattle Times)

Delegated to Boeing

The FAA, citing lack of funding and resources, has over the years delegated increasing authority to Boeing to take on more of the work of certifying the

safety of its own airplanes.

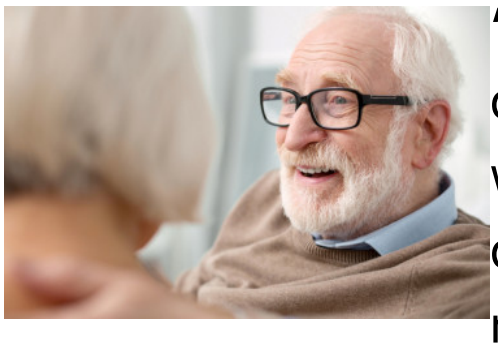
Early on in certification of the 737 MAX, the FAA safety engineering team divided up the technical assessments that would be delegated to Boeing versus those they considered more critical and would be retained within the FAA.

"

There wasn't a complete and proper review of the documents," the former engineer added. "Review was rushed to reach certain certification dates."

But several FAA technical experts said in interviews that as certification proceeded, managers prodded them to speed the process. Development of the MAX was lagging nine months behind the rival Airbus A320neo. Time was of the essence for Boeing.

A former FAA safety engineer who was directly involved in certifying the MAX said that halfway through the certification process, "we were asked by management to re-evaluate what would be delegated. Management thought we had retained too much at the FAA."



"There was constant pressure to re-evaluate our initial decisions," the former engineer said. "And even after we had reassessed it ... there was continued discussion by management about delegating even more items down to the Boeing Company."

Even the work that was retained, such as reviewing technical documents provided by Boeing, was sometimes curtailed.

“There wasn’t a complete and proper review of the documents,” the former engineer added. “Review was rushed to reach certain certification dates.”

When time was too short for FAA technical staff to complete a review, sometimes managers either signed off on the documents themselves or delegated their review back to Boeing.

“The FAA managers, not the agency technical experts, have final authority on delegation,” the engineer said.

Inaccurate limit

In this atmosphere, the System Safety Analysis on MCAS, just one piece of the mountain of documents needed for certification, was delegated to Boeing.

The original Boeing document provided to the FAA included a description specifying a limit to how much the system could move the horizontal tail — a limit of 0.6 degrees, out of a physical maximum of just less than 5 degrees of nose-down movement.

That limit was later increased after flight tests showed that a more powerful movement of the tail was required to avert a high-speed stall, when the plane is in danger of losing lift and spiraling down.

The behavior of a plane in a high angle-of-attack stall is difficult to model in advance purely by analysis and so, as test pilots work through stall-recovery routines during flight tests on a new airplane, it’s not uncommon to tweak the control software to refine the jet’s performance.

After the Lion Air Flight 610 crash, Boeing for the first time provided to airlines details about MCAS. Boeing’s bulletin to the airlines stated that the limit of MCAS’s command was 2.5 degrees.

That number was new to FAA engineers who had seen 0.6 degrees in the

safety assessment.

“The FAA believed the airplane was designed to the 0.6 limit, and that’s what the foreign regulatory authorities thought, too,” said an FAA engineer. “It makes a difference in your assessment of the hazard involved.”

The higher limit meant that each time MCAS was triggered, it caused a much greater movement of the tail than was specified in that original safety analysis document.

The former FAA safety engineer who worked on the MAX certification, and a former Boeing flight controls engineer who worked on the MAX as an authorized representative of the FAA, both said that such safety analyses are required to be updated to reflect the most accurate aircraft information following flight tests.

“The numbers should match whatever design was tested and fielded,” said the former FAA engineer.

But both said that sometimes agreements were made to update documents only at some later date.

“It’s possible the latest numbers wouldn’t be in there, as long as it was reviewed and they concluded the differences wouldn’t change the conclusions or the severity of the hazard assessment,” said the former Boeing flight controls engineer.

If the final safety analysis document was updated in parts, it certainly still contained the 0.6 limit in some places and the update was not widely communicated within the FAA technical evaluation team.

“None of the engineers were aware of a higher limit,” said a second current FAA engineer.

The discrepancy over this number is magnified by another element in the

System Safety Analysis: The limit of the system's authority to move the tail applies each time MCAS is triggered. And it can be triggered multiple times, as it was on the Lion Air flight.

One current FAA safety engineer said that every time the pilots on the Lion Air flight reset the switches on their control columns to pull the nose back up, MCAS would have kicked in again and "allowed new increments of 2.5 degrees."

"So once they pushed a couple of times, they were at full stop," meaning at the full extent of the tail swivel, he said.

Peter Lemme, a former Boeing flight controls engineer who is now an avionics and satellite-communications consultant, said that because MCAS reset each time it was used, "it effectively has unlimited authority."

Swiveling the horizontal tail, which is technically called the stabilizer, to the end stop gives the airplane's nose the maximum possible push downward.

"It had full authority to move the stabilizer the full amount," Lemme said. "There was no need for that. Nobody should have agreed to giving it unlimited authority."

On the Lion Air flight, when the MCAS pushed the jet's nose down, the captain pulled it back up, using thumb switches on the control column. Still operating under the false angle-of-attack reading, MCAS kicked in each time to swivel the horizontal tail and push the nose down again.

The black box data released in the preliminary investigation report shows that after this cycle repeated 21 times, the plane's captain ceded control to the first officer. As MCAS pushed the nose down two or three times more, the first officer responded with only two short flicks of the thumb switches.

At a limit of 2.5 degrees, two cycles of MCAS without correction would have been enough to reach the maximum nose-down effect.

In the final seconds, the black box data shows the captain resumed control and pulled back up with high force. But it was too late. The plane dived into the sea at more than 500 miles per hour.

Recovery work continues around the crater where the Ethiopian Airlines plane crashed shortly after takeoff last week near Bishoftu, southeast of Addis Ababa. Flight data analysis is yielding clues about the cause of the crash. (Yidnek Kirubel / The Associated Press)

System failed on a single sensor

The bottom line of Boeing's System Safety Analysis with regard to MCAS was that, in normal flight, an activation of MCAS to the maximum assumed authority of 0.6 degrees was classified as only a "major failure," meaning that it could cause physical distress to people on the plane, but not death.

In the case of an extreme maneuver, specifically when the plane is in a banked descending spiral, an activation of MCAS was classified as a "hazardous failure," meaning that it could cause serious or fatal injuries to a

small number of passengers. That's still one level below a "catastrophic failure," which represents the loss of the plane with multiple fatalities.

The former Boeing flight controls engineer who worked on the MAX's certification on behalf of the FAA said that whether a system on a jet can rely on one sensor input, or must have two, is driven by the failure classification in the system safety analysis.

He said virtually all equipment on any commercial airplane, including the various sensors, is reliable enough to meet the "major failure" requirement, which is that the probability of a failure must be less than one in 100,000. Such systems are therefore typically allowed to rely on a single input sensor.

But when the consequences are assessed to be more severe, with a "hazardous failure" requirement demanding a more stringent probability of one in 10 million, then a system typically must have at least two separate input channels in case one goes wrong.

Boeing's System Safety Analysis assessment that the MCAS failure would be "hazardous" troubles former flight controls engineer Lemme because the system is triggered by the reading from a single angle-of-attack sensor.

"A hazardous failure mode depending on a single sensor, I don't think passes muster," said Lemme.

Like all 737s, the MAX actually has two of the sensors, one on each side of the fuselage near the cockpit. But the MCAS was designed to take a reading from only one of them.

Lemme said Boeing could have designed the system to compare the readings from the two vanes, which would have indicated if one of them was way off.

Alternatively, the system could have been designed to check that the angle-of-attack reading was accurate while the plane was taxiing on the ground

before takeoff, when the angle of attack should read zero.

“They could have designed a two-channel system. Or they could have tested the value of angle of attack on the ground,” said Lemme. “I don’t know why they didn’t.”

The black box data provided in the preliminary investigation report shows that readings from the two sensors differed by some 20 degrees not only throughout the flight but also while the airplane taxied on the ground before takeoff.

No training, no information

After the Lion Air crash, 737 MAX pilots around the world were notified about the existence of MCAS and what to do if the system is triggered inappropriately.

Boeing insists that the pilots on the Lion Air flight should have recognized that the horizontal stabilizer was moving uncommanded, and should have responded with a standard pilot checklist procedure to handle what’s called “stabilizer runaway.”

If they’d done so, the pilots would have hit cutoff switches and deactivated the automatic stabilizer movement.

Boeing has pointed out that the pilots flying the same plane on the day before the crash experienced similar behavior to Flight 610 and did exactly that: They threw the stabilizer cutoff switches, regained control and continued with the rest of the flight.

However, pilots and aviation experts say that what happened on the Lion Air flight doesn’t look like a standard stabilizer runaway, because that is defined as continuous uncommanded movement of the tail.

On the accident flight, the tail movement wasn’t continuous; the pilots were

able to counter the nose-down movement multiple times.

In addition, the MCAS altered the control column response to the stabilizer movement. Pulling back on the column normally interrupts any stabilizer nose-down movement, but with MCAS operating that control column function was disabled.

These differences certainly could have confused the Lion Air pilots as to what was going on.

Since MCAS was supposed to activate only in extreme circumstances far outside the normal flight envelope, Boeing decided that 737 pilots needed no extra training on the system — and indeed that they didn't even need to know about it. It was not mentioned in their flight manuals.

That stance allowed the new jet to earn a common "type rating" with existing 737 models, allowing airlines to minimize training of pilots moving to the MAX.

Dennis Tajer, a spokesman for the Allied Pilots Association at American Airlines, said his training on moving from the old 737 NG model cockpit to the new 737 MAX consisted of little more than a one-hour session on an iPad, with no simulator training.

Minimizing MAX pilot transition training was an important cost saving for Boeing's airline customers, a key selling point for the jet, which has racked up more than 5,000 orders.

The company's website pitched the jet to airlines with a promise that "as you build your 737 MAX fleet, millions of dollars will be saved because of its commonality with the Next-Generation 737."

In the aftermath of the crash, officials at the unions for both American and Southwest Airlines pilots criticized Boeing for providing no information about MCAS, or its possible malfunction, in the 737 MAX pilot manuals.

An FAA safety engineer said the lack of prior information could have been crucial in the Lion Air crash.

Since MCAS was supposed to activate only in extreme circumstances far outside the normal flight envelope, Boeing decided that 737 pilots needed no extra training on the system.

Boeing's safety analysis of the system assumed that "the pilots would recognize what was happening as a runaway and cut off the switches," said the engineer. "The assumptions in here are incorrect. The human factors were not properly evaluated."

The cockpit of a grounded Lion Air 737 MAX 8 jet is seen at Soekarno-Hatta International Airport in Cengkareng, Indonesia, last week. The crash of an Ethiopian Airlines plane bore similarities to the Oct. 29... (Dimas Ardian / Bloomberg) ***More***

On March 11, before the grounding of the 737 MAX, Boeing outlined "a flight control software enhancement for the 737 MAX," that it's been developing

since soon after the Lion Air crash.

According to a detailed FAA briefing to legislators, Boeing will change the MCAS software to give the system input from both angle-of-attack sensors.

It will also limit how much MCAS can move the horizontal tail in response to an erroneous signal. And when activated, the system will kick in only for one cycle, rather than multiple times.

Boeing also plans to update pilot training requirements and flight crew manuals to include MCAS.

These proposed changes mirror the critique made by the safety engineers in this story. They had spoken to The Seattle Times before the Ethiopian crash.

The FAA said it will mandate Boeing's software fix in an airworthiness directive no later than April.

Facing legal actions brought by the families of those killed, Boeing will have to explain why those fixes were not part of the original system design. And the FAA will have to defend its certification of the system as safe.

This story has been updated to put dates on references to days of the week following the second crash.

Seven weeks after it rolled out of the paint hangar, Boeing's first 737 MAX, the Spirit of Renton, flies for the first time Jan. 29, 2016, from Renton Municipal Airport. (Mike Siegel / The Seattle Times)

Dominic Gates: *206-464-2963 or dgates@seattletimes.com; on Twitter: @dominicgates.*