Science You Can Use

Jack K. Horner

Dear Science: Is Boeing responsible for the recent 737 Max 8 airplane crashes? -- Buck R.

Dear Buck: Your question is not easy to answer. As of mid-April 2019, there were still open questions about what happened in those crashes and who, if anyone, could reasonably have done anything to avoid those tragedies.

The Boeing 737 family of aircraft is a major part of Boeing's business portfolio. That family of aircraft is widely used by airlines through the world, and at least until the Max 8 crashes, was considered to be one of the safest aircraft product-families in history.

On March 10, 2019, Ethiopian Airlines Flight 302, a Boeing 737 Max 8, crashed shortly after takeoff from the Ethiopian capital Addis Ababa, killing all 157 passengers and crew. Based on the data recorders recovered from the crash, it appears that the aircraft's flight control software repeatedly tried to force the nose of the plane down. That same data shows the pilots tried to wrest control of the craft from the flight software but were ultimately unsuccessful.

In addition, the Flight 302 data recorder showed that:

1. An "angle-of-attack" sensor fed bad data to a part of the flight-control software called "MCAS". This data falsely implied that the aircraft was in danger of stalling.
2. MCAS assumed the data from the angle-of-attack sensor was correct and forced the nose of the aircraft downward in order to increase the lift forces on the wings.
3. The pilots, despite attempting to shut MCAS off, never recovered control of the aircraft.

On 29 October 2018, Indonesia's Lion Air Flight 610, also a Boeing 737 Max 8, departed Jakarta. About 20 miles into the flight, the crew reported flight control problems and requested clearance to return to the Jakarta airport. The plane crashed offshore northeast of Jakarta, killing all 181 passengers and the crew.

On the night before the Flight 610 crash, the plane used in Flight 610 had experienced "similar" flight control problems.

The Boeing 737 Max 8 and Max 9 are modifications of an existing version of the Boeing 737. Boeing management launched the Max 8/9 development, because it believed that Airbus, a European aerospace corporation, was likely to beat Boeing to market with a competitor of the Max 8/9. If that happened, Boeing management believed, Boeing would lose a large fraction of its commercial aircraft market share.

Among other things, the Max 8/9 modifications replaced the engines of existing version of the 737 with newer, more efficient engines. This modification changed the aircraft's center of gravity and the air flow forces acting on the aircraft, compared to earlier 737 configurations. The

Max 8/9 modifications included software that was intended to help make the handling characteristics of the plane that arose from these changes appear to pilots to be much like that of older 737 configurations.

When modifications are made to the design or implementation of an existing aircraft, the US Federal Aviation Administration (FAA) determines how extensive the certification process for the modified aircraft has to be. At some level, that determination has to rely on information and recommendations the aircraft manufacturer provides to the FAA. The process can range from "short and sweet" to "new aircraft"-level of testing and scrutiny. The "new-aircraft" level of certification can take years and cost hundreds of millions of dollars. It also typically imposes extensive training requirements on aircraft purchasers.

Boeing management hoped, for obvious reasons, that the FAA put the Max 8/9 certification in the "short-and-sweet" category. The FAA agreed. In addition, the FAA agreed that pilot training for Max 8/9 model could be less extensive than the training required for a completely new aircraft design.

That's the history in a nutshell. Who, if anyone, is responsible for the crashes, given that history? Various jurisdictions will try to tackle this question and presumably try to answer many related questions in the process. Some of those questions are really about the safety of most large complex systems on which we have come to rely.

For example, the 737 Max 8 in Ethiopian Airlines Flight 302 crash, an angle-of-attack sensor (there are two on a standard 737 MAX 8 configuration) failed and contributed to the crash. Would additional angle-of-attack sensors have changed the outcome? The answer might be "yes", but how could anyone really know without extensive – possibly years -- of testing? There are hundreds, if not thousands, of components in large modern aircraft that are not, and even in some cases cannot be made, redundant – e.g., each wing, the fuselage, some power and data cables, and some of the cockpit displays.

Not least, it has been known for at least 50 years that it is impossible to test more than a tiny fraction of the control and monitoring software in many systems we rely on every day for our health and safety (e.g., the software in utilities, medical devices, automobiles, and airplanes).

In short, at least some these uncertainties cannot be made to go away, regardless of what the courts decide.

For further information, see John F. Symons and Jack K. Horner, "Software Intensive Science", *Philosophy and Technology* 27 (3): 461-477.

Jack Horner is a systems engineer. Thanks to Ed Goff for suggesting the topic.