

## Tragic Failures of the Boeing 747 & Therac-25

Some of the most well documented and publicized airplane crashes are associated with the Boeing-737. The Boeing-737 is a family the most common and best-selling aircrafts in the world. These airplanes were known for being very versatile and efficient, being used commonly for short to medium length flights. One of the 737 variants, known as the Boeing 737 MAX series, including the MAX 7, MAX 8, MAX 9, and MAX 10 models. These MAX models sported more fuel-efficient engines, updated avionics and, more complex and newer flight control systems.

However, two planes from the Boeing 737 MAX series experienced two major crashes, one involving the Ethiopian Airlines Flight 302 and the other with the Lion Air Flight 610 both within 2018-2019. The main determined causes for both flights were with the *Maneuvering Characteristics Augmentation System*, which was designed to automatically adjust the aircraft's angle of attack to prevent stalling.

The issue with the MCAS was twofold: faulty sensor readings and inadequate pilot training. Firstly, during both flights faulty sensor readings caused the MCAS to trigger when it was not needed, causing the MCAS to point the aircraft downwards until the pilots lost control of the airplane. The other issue was that the pilots did not have much training on the new MCAS system and thus did not know how to respond during the crashes.

The failures of the MCAS system were largely attributed to criticisms in the software design of the systems. Rather than being normal “software bugs”, but rather some design flaws and shortcomings in its implementation. For one, the MCAS relied on only one sensor for data readings, so if that one sensor failed, the MCAS system would faultily activate. Rather, the system should have applied redundancy by having multiple sensors. The MCAS also made very quick and jerky instructions which made it harder for the pilots to control the plane. One non-software cause of the failures were that that process of certifying the 737 MAX planes had many lapses in oversight and communication meaning that there needed to be more strict rules for certifying planes to be able to fly.

One of the factors from Nancy Leveson’s article “*Medical Devices: The Therac-25*” that resonates with the issues from the Boeing 737 MAX series was their overconfidence in software. It is a common issue throughout all kinds of software applications to rely too heavily on code that could have issues.

This was a huge issue in the Therac-25, which heavily depended on its software to work properly and safely. Even with this in mind, the Theracs main safety analysis which allowed it to be used did not check the software whatsoever. Even when there were issues, people assumed it was the hardware rather than anything. This highlights how there is often a heavy overreliance on software and many people often assume that because “computers are always right”, there can never be any issues with code. It is likely that when the Boeing 747 MAX Series were getting certified, there were many checks on the hardware aspect of the plane but little inspection into possible software bugs or design issues.

We see overreliance on software code for almost all applications of software, but it is especially dangerous when we have an overreliance on code that can directly harm other people, such as the Therac-52 and the Boeing 747 MAX Series. One of the biggest issues with this stems from the fact that most common people are taught to believe that computers are always right and that if something went wrong, it was user error and a human messed something up, but the reality is that computers can often be wrong due to a wide plethora of different software bugs. For this reason, it is important that we teach the public of the faultability of code so that they are more aware of the issues that can stem from software. In this way we can lower the general reliance that people place upon software.

Another factor from Nancy Leveson’s article “*Medical Devices: The Therac-25*” that connects to the crashes from the Boeing 747 MAX Series is confusing reliability with safety. In the Therac-25, because there were thousands of uses of the machine that did not result in any damage or failure, THE COMPANY assumed that there could be no issue with there machine. However, even if their machine appeared to be reliable, that doesn’t necessarily mean its safe. This point connects to the overreliance on software (the last point) because when people see that software or machines are reliable, they heavily rely on it without stopping to consider whether it is fully safe.

This was illustrated with the Boeing 747 MAX Series because the committee that certificated and allowed the Boeing 747 MAX Series to fly likely looked to all of Boeing’s successful planes as reasoning to assume that their new planes are just as safe. They fell into the trap of assuming that reliability means safety. Rather, the committee should have been more critical of both the software and hardware of the Boeing 747 MAX Series regardless of what past outcomes had been.

The last factor from “*Medical Devices: The Therac-25*” that relates to the crashes from the Boeing 747 MAX Series is User Government Oversight and Standards. Similarly to how the FDA has had to

improve their procedures for medical machines to be more stricter and look into software issues more because they had failed see the initial issues with the Therac-25, the Boeing 747 MAX Series were too easily certificated.