« Back | Print

Air France Crash Underscores Challenge of Designing Complex Automated Systems

An engineer/pilot's view on what went wrong with Flight 447

John Loughmiller, Contributing Editor -- Design News, June 4, 2009

On May 31, 2009, four hours into a trip from Rio de Janeiro to Paris, **Air France Flight 447**, an Airbus A330-200, encountered heavy turbulence. Fifteen minutes later, an automated system began sending messages documenting a worsening situation as first one and then another of the redundant electrical systems failed until all four were gone. Among the last messages sent was one advising that the cabin pressurization system had also failed suggesting an in-flight breakup.

The circumstances surrounding this flight underscore the diabolical challenge of designing complex, automated systems for multiple contingencies and then managing the consequences of the design choices made. Since I have a couple hats in my collection, one for when I'm being an engineer and another for when I'm being a pilot, the crash brought these challenges into sharp focus. It also reminded me of 30+ years of pilot concerns about Fly-By-Wire flight control systems.

In a **Fly-By-Wire system**, electric motors and actuators operate the flight surfaces via wires or fiber optic strands. Multiple computers provide continual oversight of the process. Designers employ software to prevent what they consider to be dangerous or illogical user inputs from the pilot in an attempt to reduce pilot error and thereby increase safety. Unfortunately there have been accidents – some fatal – because designers didn't adequately anticipate abnormal flight regimes.

In a fully implemented Fly-By-Wire system, there's no reversion to manual control. Pilots are system managers, making requests of the computers, which then decide whether the requests are reasonable. They control the movement of control surfaces using a set of rules or "laws." On an Airbus for example, four operational laws govern its operation: Normal, Normal Alternate, Abnormal Alternate and Direct Law. As systems fail, control authority changes, eventually offering the pilot control only of elevator trim, rudder and thrust of the airplane's engines in the Direct Law mode.

With four electrical systems and multiple computers, the odds of ever getting to Direct Law are remote. But Flight 447 lost all of the electrical buses plus cabin pressurization in a thunderstorm, which was something the designers probably listed as an extremely unlikely possibility. Manual reversion in this case may not have helped, but it certainly could not have hurt. In a dire emergency, a pilot needs access to every flight control on the airplane. After all, if things are really bad, why make them worse by restricting a pilot's options to the point that he or she is little more than a passenger?

To an aeronautical designer, there's a tightrope to walk that's both long and very far above the ground. Involving non-designers in the process isn't something that's normally high on their list of priorities since outsiders (pilots in this case) will frequently want to add features that translate to added cost. Still, most airline pilots I know who make their living in a Fly-By-Wire airplane don't object to the software itself. They appreciate the smooth way the computers execute the flight surface movements.

What they hate is the lack of full control of the airplane in an emergency. This desire is at variance with an aircraft designer's mindset that tries to prevent mistakes by restricting the actions a pilot can take. While these design objectives work well in normal operations, should things go horribly bad, as they did with Flight 447, the design rules may be in conflict with what's required to extricate oneself from disaster. This is the pilot's case in a nutshell.

John Hansman, a pilot and an Aeronautical Professor at M.I.T. specializing in aircraft design, has studied the differences in the Fly-By-Wire control philosophy and the more traditional approach to aircraft control. In his opinion, Fly-By-Wire gives more decision authority to the aircraft systems and less to the pilot, whereas traditional systems provide dynamic feedback

on the operation of the aircraft but leave most of the decisions to the pilot. Hansman feels that by allowing computers to make critical decisions when operating in an abnormal flight regime, designers place a tremendous burden on themselves to anticipate all possible emergency modes and design the system to react appropriately.

But what's appropriate? That's at the core of the debate. Although there are budget constraints in any design, Hansman has an approach that may help. He tells his students, who may well be the next generation of Boeing or Airbus designers, that to make correct decisions, particularly when designing complex machines like airplanes, it's critical to involve end users early in the design process. He teaches that both the designer and the end user have a mental model of how something should work. However, the two models are frequently at variance with one another.

An example: A designer working on flight dynamic issues notes there are many reports of pilots getting the airplane to assume a steep angle of attack coupled with a decay in air-speed to decay. This set of conditions is precisely what killed New York Yankee catcher Thurmond Munson as he approached an airport in his Cessna Citation business jet. The designer's solution was to examine the amount of pitch up requested by the pilot, and as it increased, cause the engines to spool up so that the aircraft can't slow down. This strategy worked fine until a combination of events that had not been modeled during the design phase fooled the system. Although the pilot steadily increased the pitch, the engines didn't spool up. The pilot should have immediately lowered the nose and manually increased the thrust but, relying on the automation, he didn't, and the airplane crashed short of the runway. It was a case of pilot and designer error.

Another example: A pilot descended below the normal Initial Approach Fix (IAF) altitude because the weather was excellent and he was flying a visual approach. Once past the IAF, he commanded the aircraft to fly the approach. He thought it would simply continue on towards the runway, capturing the glide slope from below instead of from above which is the way it works when you start at the IAF. Instead, the aircraft went into an immediate climb and attempted to reach the altitude required at the IAF even though that point was behind the aircraft by this time. The pilot decoupled the aircraft from the autopilot but placed the airplane back in the approach mode once he'd satisfied himself that the system was working properly. The aircraft once again started climbing, giving the passengers a carnival ride they didn't expect. The designer in this case never anticipated the pilot would attempt to fly a precision approach from a point other than where the approach is normally begun.

We may never know what happened to Flight 447. But the dialogue that will emerge from this event will be invaluable to system designers, as they continue in their quest to design higher degrees of safety into their automated systems.

*Contributing Editor John Loughmiller is an Electronics Engineer specializing in Single Channel Per Carrier communications systems and control logic system design for automated communications devices. He's also a 4,500 hour commercial pilot, flight instructor and aircraft owner and is a Lead Safety Team Representative for the **Federal Aviation Administration**.*

Read additional in-depth Air France crash coverage at Flightglobal:
Investigators confirm airspeed problem on Air France A330
AF447 accident - icing, pitot tubes and radar in the frame

« Back | **Print**

© 2009 Reed Business Information, a division of Reed Elsevier Inc. All rights reserved.