Diatribe 188

Planely disastrous. Did Computer Failure Bring Down Air France 447?

Speculation abounds following a plane crash. Mechanical flaws, terrorism, pilot error, and weather are the usual suspects. But in the tech age, where even your toaster is digital, IT systems must be added to the list. In the Air France disaster, there's a particularly urgent need for government authorities to eye the aircraft's on-board computer system as a possible culprit.

That's a quote from a US blog dealing with the recent crash of a an Air France 447, an Airbus 330 on June 3, off the coast of Mexico. 228 souls, men, women and children, passengers and crew, perished, and no-one survived. At the time, the aircraft was largely under the control of ADIRU, an electronic inertial reference system which interacts with the auto-pilot

By way of contrast, earlier, on Jan.15th, another Airbus, at that time a 320, ditched in New York's Hudson river after birds hit both engines which died, and nobody was even injured let alone lost. Control of that plane was manual, having not yet reached an altitude where the computers take over, in the hands of Capt. "Sully" Sullenberger, a former U.S. Air Force fighter pilot, former safety chairman of the Air Line Pilots Association, scholarly author on aviation safety, graduate of the U.S. Air Force Academy, and recently appointed Visiting Scholar at the University of California, Berkeley. Sullenberger was ably assisted by a crew who not only carefully instructed the passengers on what to do, but safely guided them to their rescuers who had been summoned by radio. Sullenberger, after executing a perfect "landing" on the river, topped his performance by twice walking the length of the half-submerged aircraft to make sure that all passengers were out.

The majority of the blogs relating to the Mexican disaster were clearly lodged by industry representatives, insisted that at this time it was not yet possible to draw any conclusion regarding the latest event. From this they also decided that currently nothing can be done about it. If I were an intending passenger on an Airbus, I would not be likely to agree with their suggestion, so much the more so as there were accidents with our very own Airbuses too.

One which reached prominence happened to a Qantas Airbus 330. Last year it started porpoising wildly while at cruising altitude, from memory somewhere over Western Australia. 51 passengers were injured, with damage ranging from broken bones to spinal trauma.

The accident report issued by the Australian Transport Safety Bureau tells us: *About two minutes after the initial fault, the air data inertial reference unit (ADIRU) generated very high, random and incorrect values for the aircraft's angle of attack.*

Apart from this near crash, there were other warnings. Also last year, the US Federal Aviation Administration issued an airworthiness directive warning airlines about an "unsafe condition" associated with ADIRUs aboard Airbus 319, 320 and 321 models. The directive warned that the equipment was sending out bogus navigational fault warnings that could "result in loss of one source of critical altitude and airspeed data and reduce the ability of the air crew to control the airplane". Earlier direct transmissions to Paris from the craft had indicated danger signals from the ADIRU system. Indeed, later evidence showed that the crew had actually attempted to turn the plane back before the crash.

In 1990, while the Australian Hawke “Labor” government conspired with the tycoon Peter Abeles to lock out the experienced pilots of this country who were, amongst other things, demanding a say in air safety, I happened to be travelling to Sydney on unavoidable business sitting next to one of the locked-out captains who told me then about the difficulty of interfacing the human crew with what was then just the auto pilot. As a systems designer of sorts myself, this was not news to me.

The technical problems are these: Pilots’ decisions regarding aircraft control are, amongst other things, based on instrument readings, control responses and control tower instructions. In the normal course of flying a plane, these details are acquired as you go along. If, on the other hand, you have to hand over control from machine to human, all this has to be done over a short period if not instantly. If this happens at a time of stress, mistakes are even more likely than if it happens in the normal course of events.

Once upon a time, pilots flew planes by the use of hands and feet on column and pedals. With to-day’s 200 ton monsters, control surfaces are difficult to operate this way. Also, steel cables and hydraulic lines are heavy, and have to be duplicated or triplicated for safety. All that lifting capacity can be diverted to lifting passengers and cargo by operating controls and surfaces independently. The Airbus series of planes is therefore flown, as they say, by wire, using electrics or hydraulics. The human pilot’s commands are fed into the computer and the computer passes these commands on to the plane’s control surfaces, if it wants to, after subjecting the computer’s decision to the scrutiny of sundry mathematical processes. As a sop to the human pilot some pressures are simulated on pedals and stick to make the slave at the controls feel that he or she is in charge. Boeings are similar, but there at least the option exists for the pilot to exercise the ultimate control should the computers fail. No such options exist for the Airbus. The electronics can over-ride the human pilot.

Spare a thought or two for him or her. World-wide, pilots would know what happened in Western Australia where they had to wrestle with the Airbus controls while passengers had their bones broken, and where a major disaster was avoided by a whisker. So far, the only steps taken to avoid disasters like the Mexican is to duplicate, triplicate or quadruplicate the faulty system.

Every pilot, no matter how experienced, currently flying an Airbus relying on ADIRU – as most of them appear to be – would have to remember that they are at the mercy of a machine which has proved faulty and undoubtedly will prove so again It may well result in a situation which is beyond any pilot’s control. And since Abeles’ victory, aircraft captains cannot even refuse to fly the faulty planes. All this would do wonders for morale.

There used to be a saying at Telstra that nowadays telephone exchanges were staffed by a man and a dog. The man is there to feed the dog and the dog is trained to stop the man from getting to the equipment. This fly-by-wire seems to follow a similar philosophy. Because the flight computers are programmed with the parameters which represent the limits of what the plane can do, they are made the masters of the human pilot.

I remember a paper by an Indian academic which argued that in order to create safe systems they had to have a maximum of sophisticated technology backed up by the best available staff training. This is a nonsense. Good staff training can only be achieved by allowing staff maximum interaction to permit familiarity with the system. This was amply proved in disasters like Three Mile Island nuclear power station where human operators were given a few seconds to deal with a mass of complex problems after the automatic controls gave up. So did the operators.

Step aside, Sully Sullenberger, we can no longer afford the likes of you at the aircraft’s controls.