Situation Awareness and the Human-Machine Interface

"People think computers will keep them from making mistakes. They're wrong. With computers you make mistakes faster." Adam Osborne

This essay may appear to be about aviation, but it is actually about how computerised control systems and plant operators (or pilots) communicate with each other, and the design of the communications interface. The examples are taken from aviation because they are well-documented; they also make clear the crucial role of clarity and reliability in ensuring the pilot-operator can control the plant/plane safely.

What follows is a brief description of three separate air crashes, which took place over thirteen years, featuring two completely different designs of airliner (the Boeing 757 and the Airbus 330), and yet the accidents had some similar circumstances. All three accidents were thoroughly investigated and are well-documented, and each has even been the subject of its own television documentary.

All three accidents involved aircraft with digital (computerised) cockpits, where the pilots received all their information and alarms about the state of the aircraft from computer displays. All three aircraft suffered blocked Pitot tubes which led to erroneous airspeed indications. In each case the pilots lost 'Situation Awareness' for a critical short period of time, and aircraft that were otherwise in perfect flying condition crashed with the loss of all passengers and crew. 'Situation Awareness' is an expression used to describe the knowledge that any pilot-operator should have of the current circumstances in which he is operating.

The aviation and nuclear industries, especially, spend a lot of effort and time worrying about the ergonomics and design of the 'human-machine interface', that is, the layout of the control panels, instruments, warning lights and alarm messages, and the design of the way in which the operator-pilot controls the machine. 'Old' aircraft technology used mechanical-hydraulic control systems with discrete analogue-electrical-pneumatic instrumentation. However, these were difficult to maintain, because there were lots of mechanical elements that were prone to failure. The instrumentation required a great deal of wiring and cables. Also, there was no intelligence in the instruments; the pilot had to interpret what he saw to make the right decisions. Finally, the pilot could also fly the aircraft in any way he (or she) chose, which included making mistakes.

The two types of aircraft discussed below (two crashes involving the Boeing 757 in 1996, and an Airbus 330 crash in 2009) belonged to different generations of aircraft. The Boeing 757 used an intermediate mixture of conventional and digital systems; it had conventional flight controls with fully digital Electronic Flight Information Systems. By comparison, the Airbus 330 uses full 'fly-by-wire' in addition to digital displays and alarms[1]. In fly-by-wire systems, there is no direct mechanical

[1] Fly-by-wire technology is also gradually entering the automobile industry, with electronic throttles, brakes, and even steering becoming more common. Mercedes-Benz have even shown a concept car without a steering wheel, where the car is steered with an aircraft-like control-stick.

linkage between the pilot's hands on the control column and the aircraft's control surfaces (ailerons, elevators and rudder).

Modern airliners such as the Airbus 330, and also power stations and other process plant, have microprocessor-based instrumentation and control systems that offer fantastic advantages over old technology. A modern civil airliner will more-or-less fly itself, with the pilot's role reduced to monitoring and oversight under normal conditions. The pilot's job becomes one of ensuring that the flight control systems are doing what they are supposed to be doing, while being ready to resume manual control if necessary. Also, the amount of cables and wires can be greatly reduced because digital signals can be multiplexed with many signals being transmitted on a single cable. Meanwhile, the microprocessor-based systems can include control, indication, alarm, and also 'protection' functions: the software can have the aircraft's 'safe flight envelope' within its programming, to ensure that appropriate action is taken if the aircraft is, for example, flying too slow, or too fast, or at too high an angle of attack.

Older aircraft had controls that were hydraulically linked to the aircraft control surfaces, which meant the pilot got 'force feedback', that is, if the rudder (or elevator or aileron) was being pushed into the airstream, the pilot would feel that he had to push harder. Hence, the pilot could fly by 'feel', at least to some extent. In modern aircraft, the mechanical linkage between the pilot's controls and the control surface on the wings or tailplane is completely broken – all signals are electrical – so the pilot will receive no 'force feedback' unless the design engineers chose to simulate it in their designs. This aspect – the design of the control column – is important, as we shall see.

Also in older aircraft, each instrument was a 'stand-alone' item. It received a signal from a sensor, and it displayed a value. In computer-based instrumentation and control systems, the signals from all the sensors are processed through a few microprocessors, possibly with similar application software, and probably with a common operating system. With modern equipment, the separation between instruments becomes blurred. One disadvantage of this is that, when an instrument fault (or, even worse, a series of faults) occurs, the pilots of modern aircraft may wonder whether the problem is really with the *instruments*, or whether the fault might instead be in the *system*. This confusion may cause brief but important delays in crises, as we shall see. If the pilot is thinking, "Maybe this problem isn't just an instrument fault - maybe the whole computer system has gone crazy", it may freeze his decision-making with catastrophic results.

Let me emphasise one issue: I am in no way advocating 'turning back the clock'. Computer-based instrumentation and control systems are here to stay and offer huge advantages and reduced risks. However, as well as reducing some risks, they also introduce some new ones, and engineers have to be careful when designing such systems. I am in no doubt that the net effects of computerised instrumentation and control systems are beneficial to safety and costs, but care has to be taken.

One further introductory comment: The aviation industry has a long and dishonourable history of laying the blame for accidents on pilots who are conveniently dead. The pilots will almost certainly be named in enquiry reports and their mistakes under the most extreme pressures will be analysed in great detail by, as they say in the United States, 'Monday morning quarterbacks'. Meanwhile, the

individual design engineers whose decisions may have contributed to the accidents may remain anonymous.

A NOTE ON PITOT TUBES

A Pitot tube is a simple device to produce a measure of airspeed. Pitot tubes are mounted on the outside of an aircraft's fuselage, pointing into the airflow. They measure the difference between the dynamic pressure of the air (the pressure measured when pointing into the direction of airflow), and the static pressure (measured perpendicular to the airflow). This pressure difference is proportional to the square of the airspeed.

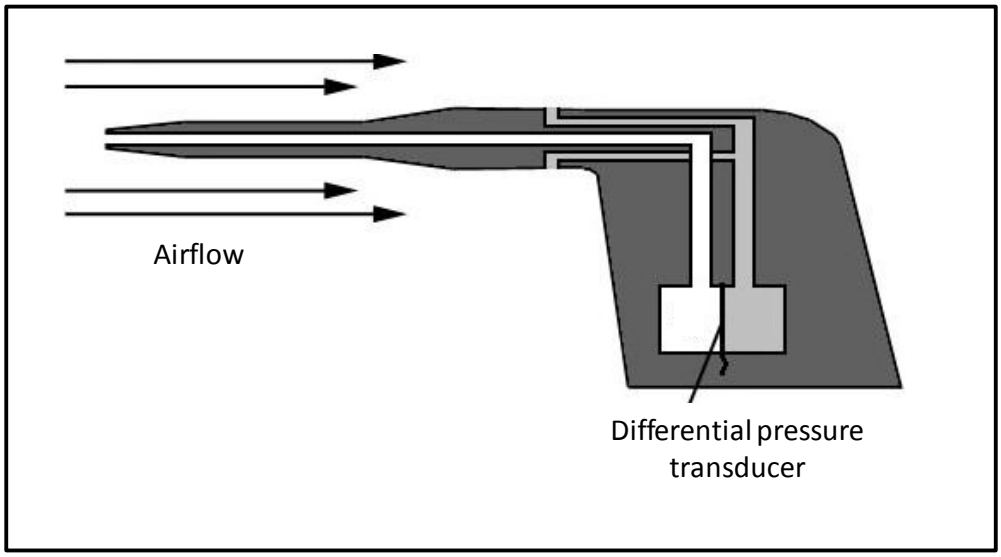


Fig 1 Pitot tube

BIRGENAIR 301, 6TH FEBRUARY 1996[2]

This flight was a charter flight taking 176 mostly German tourists home from a holiday in the Dominican Republic to Frankfurt via Gander in Newfoundland. There were 13 crew members on board.

The original aircraft had mechanical problems, so at a late stage a Birgenair Boeing 757 was substituted which had been sitting on the runway at Puerto Plata airport for three weeks. Hence the flight was several hours late and it took off in darkness.

[2] Flight Safety Foundation, *Erroneous airspeed indications cited in Boeing 757 control loss*, Accident Prevention, Volume 56 No 10, October 1999

Birgenair was a Turkish-owned airline and the crew were all Turkish; Captain Ahmet Erdem, First Officer Aykut Gergin and relief pilot Muhlis Evrenesoglu.

As the plane was accelerating in darkness for take-off at 2342:26 hours local time, Captain Erdem saw that his air speed indicator (ASI) was not working.

Five sources of velocity information were available to the crew. They included Captain Erdem's airspeed indicator, the First Officer Gergin's airspeed indicator, a standby airspeed indicator in the centre of the instrument panel, a groundspeed readout on Captain Erdem's Electronic Flight Information System (EFIS) display, and a groundspeed readout on First Officer Gergin's display.

Erdem should have aborted take-off as soon as he realised his ASI was not working; the purpose of checking the instruments during acceleration is to verify proper operation of the instrumentation. Instead, Erdem asked "Is yours working?"When Gergen said it was, Erdem said "You tell me", meaning that the co-pilot should tell the Captain at which point the aircraft was at the 'Vee One' speed of 80 knots. (At Vee One the plane is rotated, i.e. the nose of the plane is raised off the ground.)

The plane then continued to take off normally.

If Captain Erdem had aborted takeoff, calculations performed later confirmed that there was enough runway left for safe deceleration.

At 2343:00, Captain Erdem said "It began to operate", meaning that his airspeed indication was working again.

After wheels-up, the autopilot was engaged and the climb continued normally. Unfortunately, the auto-pilot was selected to use Erdem's (faulty) airspeed indicator.

Two minutes after take-off, at 2344:25, the captain noted computer alarms *mach speed trim* and *rudder ratio*. The meaning of these alarms was not known to the crew and was not, at that time, included in the flight manual. Erdem said immediately afterwards "There is something wrong, there are some problems." Fifteen seconds later he said again "Okay there is something crazy, do you see it?" to which First Officer Gergen replied "There is something crazy there at this moment - two hundred only is mine and decreasing, sir", meaning his airspeed indicator was only showing 200 knots.

The Captain said, "Both of them are wrong. What can we do?" followed by "Alternate is correct", presumably meaning that the standby airspeed indicator in the centre of the instrument panel was working properly.

At 2345:04 Erdem said something prescient: "As aircraft was not flying and on ground something happening is (un)usual" (*sic*). Erdem was belatedly showing concern that the aircraft had been sitting on the runway for three weeks.

Subsequent investigations of the aircraft wreckage could find no blockages in the Pitot tubes. However, there was a known problem at Puerto Plata airport with a particular species of wasp, the mud dauber wasp, which may have built nests inside the Pitot tubes during the aircraft's three-week stay on the runway at Puerto Plata.

It appears the aircrew became overwhelmed by the number of conflicting audible warnings and alarms that their flight displays presented to them, some of which seemed almost meaningless. Also, the behaviour of Captain Erdem's airspeed indicator was curious; it wasn't working, then it began to work and indeed started to show excessive speed. It is likely that the blockage in the Pitot tube caused by the mud dauber wasp had completely blocked the Pitot tube, trapping air inside it. As the aircraft continued to climb, the trapped air expanded, causing a false signal indicating *high* speed, and generating more alarms.

Erdem's indicated airspeed reached 350 knots, and this incorrect high-speed signal was used by the auto-pilot, which therefore raised the nose of the aircraft to almost twenty degrees in order to slow the plane down. At 2345:39, Erdem instructed Gergen to "Pull the airspeed", meaning to silence the overspeed warning alarm.

Faced with confusing alarms and at least one indication that his speed was excessive, Erdem made a bad decision; he decided the aircraft was travelling too fast, and pulled back the throttles.

At 2345:52 the stick-shaker began to operate and continued until the crash. The stick-shaker is a device used to tell the pilots that they are close to stall speed – the control column is made to vibrate as an inescapable warning of low speed. The aircraft was at 7132 feet and Erdem's faulty airspeed indicator was showing 323 knots, when the true speed was less than 200 knots

As the stick-shaker activated, the auto-pilot was disengaged automatically because it had reached the end of the range of its 'operational authority' – just at the point that Erdem was extremely confused. He had within a few seconds received 'high speed' alarms and stick-shaking indicating 'low speed'. Which should he believe, if any?

The auto-pilot, before it had disengaged, had raised the nose of the aircraft, and Erdem had pulled back the throttles thinking he was going too fast, when the exact opposite was required; he needed urgently to lower the nose and increase the throttles, but he could not make sense of the conflicting warnings.

The aircraft was almost stalled. At 2346:00, the relief pilot Evrenesoglu said "ADI", referring to the Attitude Director Indicator; he was presumably pointing out the high nose-up attitude of the plane. Erdem continued to struggle with the controls, increasing thrust and trying to lower the nose, but the Angle of Attack was so high that the engines lost thrust. The left engine compressor stalled before the right engine, twisting the plane round and placing it into a full stall.

Erdem's last words were, "Thrust, don't pull back, don't pull back, please don't pull back. What's happening?"

The aircraft hit the sea twenty kilometres from the Puerto Plata at 2347:17, and all on board were killed. The entire flight had lasted less than five minutes, and it had been less than three minutes since the alarms *mach speed trim* and *rudder ratio* had been received.

The official report placed the blame on the crew. The probable cause was "the crew's failure to recognize the activation of the stick shaker as a warning of imminent entrance to the stall, and the failure of the crew to execute the procedures for recovery from the onset of loss of control." The Boeing 757 Operations Manual did indeed contain procedures for conducting a flight with an

untrustworthy airspeed indicator. The procedures included recommended pitch attitudes and throttle settings for climb, cruise and landing.

The accident report said, "While the flight continued to climb, the crew members did not discuss or demonstrate that these procedures were available. They never focussed their attention on the enormous pitch attitude that developed or the alternate sources of velocity information that were present in various indicators in the cockpit.....During the final two minutes of the flight, the crew did not take proper actions necessary to prevent the loss of control of the aircraft."

Post-accident tests in a flight simulator showed that a recovery from the stall might have been possible with full power and proper positioning of the flight controls, that is, normal stall recovery techniques. I have little doubt that in a controlled simulator environment a recovery would have been possible. I also fully accept that Erdem should have aborted the flight at take-off when he saw his airspeed indicator was faulty. However, the alarms generated by the Electronic Flight Information System were so cryptic as to be meaningless: The alarms *mach speed trim* and *rudder ratio* received at 2344:25 were actually intended by the system designers to warn of discrepancy between the airspeed indications, but this was not mentioned in the flight manual, so no pilot could reasonably be expected to know that.

Contradictory alarms led to the aircrew losing 'Situation Awareness'. In the darkness, they had no other information except their instrumentation, and that instrumentation was not helpful.

The US National Transportation Safety Board (NTSB) issued various Safety Recommendations on 31st May 1996. These included a recommendation that the Boeing 757 flight manual should be revised to notify pilots that "Simultaneous activation of the *mach speed trim* and *rudder ratio* advisories is an indication of an airspeed discrepancy". The NTSB also required Boeing to modify the alarm system to include a "caution" alert when an erroneous airspeed indication is selected. Various other changes to the flight manual were also instructed. Simulator training was changed so that "the student is trained to appropriately respond to the effects of a blocked Pitot tube".

Personally, I can be irritated when accident reports, with perfect twenty-twenty hindsight, blame the pilot-operator. There were less than three minutes between receipt of the incomprehensible *mach speed ratio* and *rudder trim* alarms, and the crash into the sea. In my mind, this accident was caused by poor design of the human-machine interface, which was then compounded by pilot errors – and not the other way round.

AEROPERU 603, 2ND OCTOBER 1996[3]

The Aeroperu 603 accident was a sequel to the Birgenair accident above. It happened a few months later and, crucially, before the NTSB Safety Recommendations arising from the Birgenair accident had achieved wide circulation.

[3] Accident of the Boeing 757-200 aircraft operated by Empresa de Transporte Aereo del Peru SA, 2 October 1996, Accident Investigation Board, Ministry of Transport, Communications, Housing and Construction, Directortate General of Air Transport, Lima, December 1996

Aeroperu 603 was a scheduled flight of a Boeing 757 from Jorge Chavez International Airport, Lima, Peru to Santiago, Chile, carrying 61 passengers and 9 crew members. On the flight deck were Captain Eric Schreiber and First Officer David Fernandez.

The plane took off at 0042 hours local time, that is, in absolute darkness. The weather was low cloud, with the cloud base at about 270 metres, so the pilots will have had no visual reference points.

Immediately after take-off the crew noticed that the altimeters were not responding. Within a further minute, they realised there was also a problem with air speed indication also and, at 0043:06, *mach speed ratio* and *rudder trim* alarms were received (as for Birgenair 301). Because the Aeroperu crew had not seen the notifications about the Birgenair crash, they too did not know the meaning of these alarms.

The official report notes "From 00:43:31 the crew start to receive *rudder ratio* and *mach speed trim* warnings, which are repeated throughout the flight, distracting their attention and adding to the problem of multiple alarms and warnings which saturate and bewilder them, creating confusion and chaos which they do not manage to control, neglecting the flight and not paying attention to those alarms which are genuine." The cockpit voice recorder showed the pilots fretting about the significance of these alarms throughout the short flight.

At 0044:32, the crew declared an emergency.

At 0055:07, the flight crew requested, "You're going to have to help us with altitudes and speed if that's possible."

The two flight crew were now over the ocean and trying to fly the aircraft manually to return to Lima in darkness, all the time with abnormal or non-functioning altitude and airspeed indications, and with the Electronic Flight Information System generating lots of alarms.

The tower at Lima was asked to provide altitude readings from their ground radar, which had recently been returned to service after a major service. The tower responded by providing altitude data from their screens which the air traffic controller believed were generated from the radar systems, but which were *actually* data provided by the aircraft's own communications data link with the ground; that is, the tower was reading simply back the same faulty altitude data.

Some efforts were made to revert to autopilot, but these were unsuccessful and the pilots reverted to manual control. The pilots struggled with knowing which, if any, instruments were credible – at 0052:52 Captain Schreiber said "Fuck! Basic instruments! Let's go to basic instruments!"

Low-speed stall warnings or overspeed alarms were received several times (0057:12, 0058:25, 0059:08, 0059:27, 0059:35, 0059:41 and 0059:46). The pilots discussed again which air speed indications they could believe. At 0059:11 Captain Schreiber said "Fucking shit! I have speed brakes, everything has gone, all instruments went to shit, everything has gone, all of them." Between 0100:19 and 0100:27, there was an exchange between the pilots about whether or not they were stalling. One said "We're not stalling. It's fictitious, it's fictitious."

Lima was meanwhile trying to prepare another plane so that it could fly alongside to guide them back. At 0102:41, Lima advised that the plane would take off in about 15 minutes to give help.

Between 0102 and 0104, 'Low terrain' alarms, wind-shear alarms, and ground proximity warning alarms all sounded. At 0105:52, they were 50 miles from Lima, heading west. Lima Air Traffic Control said they were at 10000 feet, but that was based on the faulty data from the aircraft's communication link. They were actually below 4000 feet.

At 0107 hours they were at 4000 feet (although they believed they were much higher) and they held this altitude for one minute, before beginning a slow descent. At 0109:36, Lima Air Traffic Control said "Altitude is 9700 and speed is 240 knots, 51 miles from Lima." Again, their altitude was actually much lower. They continued descending but their actual height was now below 1000 feet.

At 0110:17, "low terrain" audible alarms started and sounded twenty-two times for the remainder of the flight, but Lima Air Traffic Control again advised at 0110:18 that their altitude was 9700 feet.

At 0110:57, there was a sound of impact as the plane touched the sea. First Officer Fernandez was able to shout "We are impacting water!" before the fatal second impact at 0111:16. The flight data recorder showed the plane had been descending at a ten degree angle at the time of first impact, when the left wing and engine touched the water. It then climbed to 200 feet before inverting and crashing into the sea.

The flight had lasted thirty-one minutes. All seventy people on board were killed immediately and the plane sank into deep water. The crash, in air accident terminology, was categorised as "Controlled Flight into Terrain" (CFIT), since the plane remained more-or-less in the control of the pilots until impact.

Throughout the flight, Schreiber and Fernandez had to cope with multiple, repetitive alarms, many of them spurious, while trying to cope with a full-scale emergency. Both were hopelessly overloaded with information; they were trying to separate genuine information from false. As the official report put it, "The crew were over-saturated with erroneous information."

Their confusion was compounded by Lima Air Traffic Control sending altitude information that the pilots believed was being sourced completely independently from the air traffic control radar, when it was actually just data from the planes own malfunctioning systems sent to Lima on the aircraft's communications data link. The pilots probably thought the *only* information they could rely on was the height and speed information they were receiving over the radio – yet this was just the plane's own false readings, being recycled to them from Air Traffic Control.

There actually was one reliable instrument – the radio altimeter – but Schreiber and Fernandez were unable to recognise this in the confusion. The radio altimeter had provided the "low terrain" alarms which sounded repeatedly during the last minute of the flight. (One issue is not clear to me: Did the pilots' training mean that they should have known which individual instruments - barometric pressure or radio altimeter - were responsible for each alarm? I suspect, from the confusion, that the answer was 'no'.)

I have no doubt that, if I were a pilot in their situation, my working hypothesis would have been that there had been a complete failure of the aircraft's computer-based flight instrumentation systems.

Faced with multiple-instrument failure and numerous apparently spurious alarms, no other explanation would have seemed possible on first diagnosis. (Indeed, some initial news reports of the accident stated that “the plane’s whole system completely failed”.)

What had actually happened was however far more prosaic. Debris recovered from the seabed showed that the Pitot tubes (used for air speed indication) and also the static pressure ports (used for barometric altitude measurement) had been covered by masking tape. This tape was used when the aircraft was polished. Quality control checks should have taken place to confirm the tape was removed – an (unnamed) duty supervisor and line chief were responsible. One of the pilots should also have carried out visual checks as part of pre-flight checks.

The crew were unaware of the meaning of the *mach speed ratio* and *rudder trim* alarms, because they had never seen the National Transport Safety Board (NTSB) Safety Recommendations from the Birgenair 301 accident. The report into the Aeroperu accident noted pithily that the NTSB Safety Recommendations “were not distributed with the necessary urgency”.

The recycling of bad altitude information by Lima Air Traffic Control was a further layer of confusion in this accident. Improved training for Lima air traffic controllers was recommended.

Above all, the dreadful story of this accident shows the importance of not overwhelming the pilot-operators with huge numbers of alarms, many of them repetitive and/or meaningless, because this distracts them from trying to analyse the problem, and destroys their ‘Situation Awareness’.

A NOTE ON HIGH ALTITUDE UPSETS AND ANGLE OF ATTACK

Before discussing the last of the three related aircraft crashes, there is a need for a brief aside on ‘High Altitude Upsets’. An ‘upset’ is aviation jargon for loss of control, usually through stalling. At high altitude, the ‘flight envelope’ – that is, the scope for the aircraft to change velocity or increase altitude – can be very restricted. This is because the thin air at altitude has two effects; first, the speed of sound becomes lower at higher altitude and, second, the aircraft’s stalling speed is greater in the thin air.

Hence, if an aircraft is flying straight and level at high subsonic speed at high altitude, and the pilot tries to accelerate, he may get close enough to the speed of sound to cause buffeting (the ‘sound barrier’). Also, if he tries to slow down, the aircraft may approach its stall speed – at which point the pilot will also feel buffeting due to stall effects. ‘Buffet’ feels like vertical vibration which can reach 0.2 g.

Finally, if the pilot tries to climb upwards from a cruise at high subsonic speed and high altitude, the increased Angle of Attack in the thin air may also induce buffeting prior to stalling.

The situation described above is known to test pilots as ‘coffin corner’.

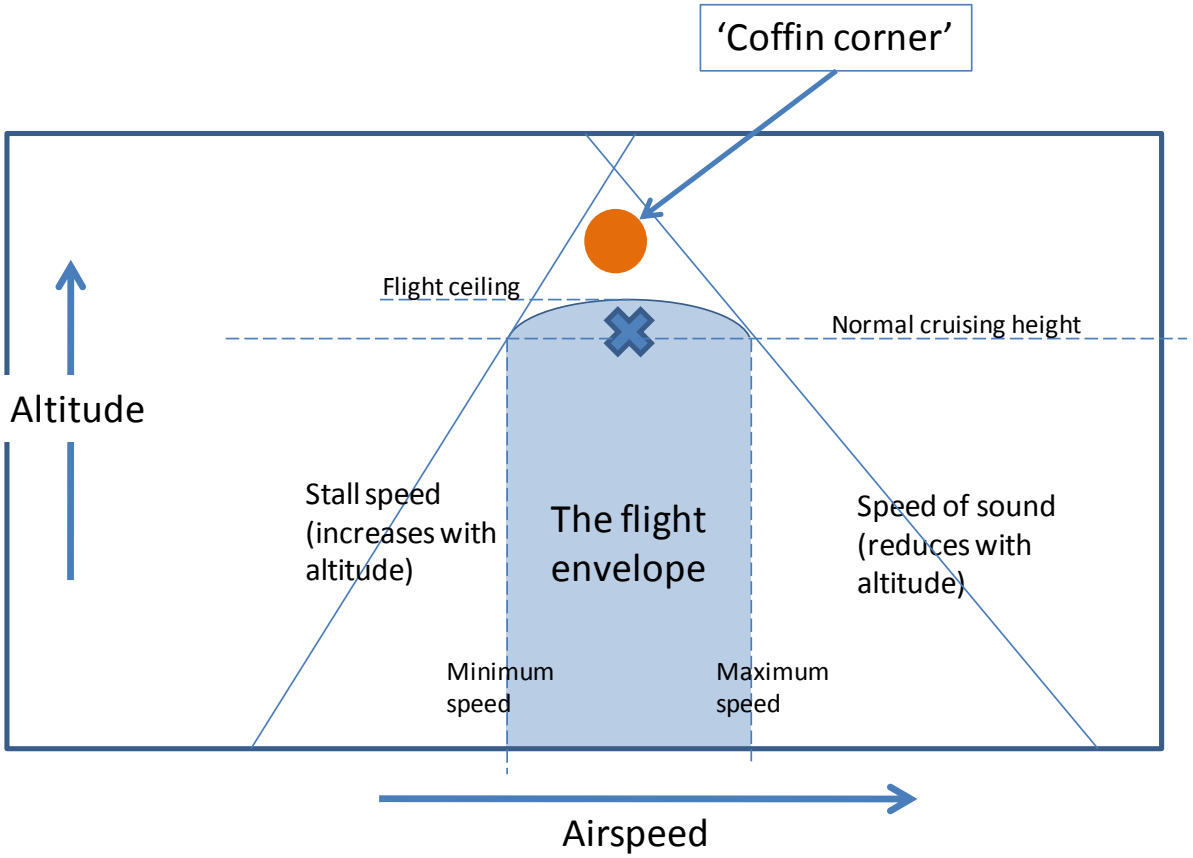


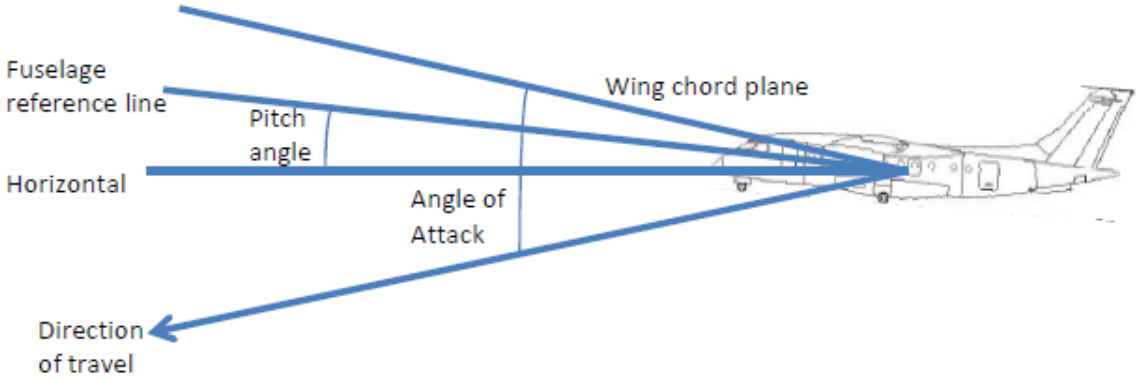
Fig 2 Schematic diagram illustrating 'coffin corner': If the pilot accelerates from typical high altitude cruise conditions, he will feel sonic buffeting. If he decelerates, he may approach stall conditions. If he tries to climb, the increased angle of attack may cause stall buffeting.

Mishaps due to 'coffin corner' have largely been confined to experimental aircraft under test conditions, although some civil aviation accidents did occur in early jet travel, some fatal. Notable incidents with successful recovery include a high altitude stall of a Pan American Boeing 707 while cruising over the Atlantic at 35000 feet in February 1959. Happily, the pilot was able to recover control, but by that time the aircraft was at 6000 feet.

Another example where the pilot managed to achieve a successful recovery was in July 1963, when a United Airlines Boeing 720 stalled while encountering turbulence during climbing at 37000 feet; in this case the pilot recovered control at 14000 feet. The latter incident was a trigger for change – margins were increased on all jet aircraft so that pilots would have more opportunity to avoid high altitude stall.

A more recent incident happened in February 1985 when a China Airlines Boeing 747SP lost control after a single-engine 'flame-out' when cruising at 41000 feet over the Pacific Ocean. The pilot recovered control at 11000 feet, although the plane exceeded its maximum operating speed twice during the dive. It suffered structural damage and two occupants received serious injuries.

Also in the following example, the difference between 'Angle of Attack' and 'Pitch angle' is significant. This difference is best understood with reference to the diagram below.



11-3: This diagram illustrates the difference between Angle of Attack and Pitch angle.

Angle of Attack (AOA) is the angle between the wing's chord plane (an imaginary line drawn between the leading edge and the trailing edge of the wing) and the plane's direction of travel. Angle of Attack is important for determining stall speed. *Pitch Angle*, however, is the angle between the fuselage centre line and horizontal. When flying in darkness on instruments, the key difference between AOA and Pitch Angle is that AOA (which matters for stall avoidance) is not a parameter that a pilot can 'feel'; he is dependent on his instruments. However, Pitch Angle is a parameter that pilots may have some awareness of, since it will affect how they feel in their seats, but it is not directly important for stall avoidance.

AIR FRANCE 447, 1ST JUNE 2009

This accident has been the subject of extremely detailed analysis and reporting by the French authorities.[4] It has also been the subject of much news reporting and television documentaries, some of which have been a little hysterical, perhaps with some justification. It is truly one of the most bizarre accidents, where one co-pilot behaved in a very strange manner indeed – apparently unaware what he was doing, almost like he was frozen in complete panic - but the other pilots could not see what he was doing so they could not interpret the instrumentation properly.

Air France 447 (AF447) was a scheduled overnight flight from Rio de Janeiro to Paris on 1st June 2009. (It actually left Rio on the late evening of 31st May.) There were 216 passengers and 12 crew members on board. In mid-flight, while over the South Atlantic, the aircraft simply 'vanished'. No Mayday calls were received and, because the plane was in mid-Atlantic, there were no radar records available. Initially, terrorist action was suspected, especially after some floating debris and bodies were discovered.

The aircraft was an Airbus A330-200, registration number F-GZCP, with a fully digital cockpit and full 'fly-by-wire' controls.

The investigation of this accident was an enormous undertaking, and involved the French and Brazilian air forces and navies. One French nuclear submarine was involved as were various remotely operated vehicles (ROV's). Wreckage of the plane was eventually found 3980 metres underwater in the Atlantic Ocean at about 3 degrees north, 30 degrees west. The debris was spread over an area of seabed 600 metres by 200 metres.

Eventually 154 bodies were recovered, either on the surface or in the wreckage deep underwater; the remaining 74 were never found.

The flight data recorders and cockpit voice recorders were not recovered until 12th May 2011, almost two years after the accident.

The basic facts are as set out in the opening paragraphs of the final French report:

"At around 0202 hours, the Captain left the cockpit. At around 0208, the crew made a course change of 12 degrees to the left, probably to avoid returns detected by the weather radar. At 0210:05, likely following the obstruction of the Pitot probes by ice crystals, the speed indications were incorrect and some automatic systems disconnected.....(The co-pilots) were rejoined 1 minute 30 seconds later by the Captain, while the aeroplane was in a stall situation that lasted until the impact with the sea at 0214:28."

In a little over four minutes, the plane had fallen from its cruising height of 35000 feet into the sea. There were no electrical or mechanical malfunctions. A perfectly healthy plane had fallen out of the sky.

[4] Bureau d'Enquetes et d'Analyses, Final report on the the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro-Paris, 27 July 2012. Available to download from www.bea.aero/en/enquetes/flight.af.447/rapport.final.en.php

In September 2007, Airbus had made recommendations to change the model of Pitot tubes installed in Airbus A320, A330 and A340 aircraft, due to a problem with water ingress. This was not an Airworthiness Directive, so Air France decided to replace the Pitot tubes on A330 planes only when failure occurred. From May 2008, Air France had some incidents involving loss of airspeed data during flights, apparently due to temporary icing of the Pitot tubes. Air France began to accelerate the Pitot tube replacement programme on A330 aircraft; this was actually completed by 17th June 2009, but F-GZCP had not been upgraded at the time of the crash on 1st June 2009.

The recovered flight data recorders and cockpit voice recordings enabled the detail of what had happened to be worked out.

Just after midnight, the aircraft was in cruise at 35000 feet, with autopilot and auto-thrust engaged, with Captain Marc Dubois, aged 58, flying the plane. Dubois had first received a commercial pilot's licence in 1977 and had eleven thousand flying hours.

His co-pilot in the right-hand seat was 32 year old Pierre-Cedric Bonin. Bonin had 2936 flying hours and had received his professional pilot's licence in 2001.

The relief pilot was 37 year old David Robert, with 6547 flying hours. He received his professional pilot's licence in 1993.

At 0136, the plane was approaching a tropical storm and entered high-level cloud. At 0151, the electrical storm caused the cockpit to be illuminated by St Elmo's fire, where luminous plasma is formed around pointed objects because of the strong electrical field. It is harmless but is often found in thunderstorms near the equator. (This incident with St Elmo's fire should be irrelevant, but there have been suggestions that it 'spooked' co-pilot Bonin who had not seen it before.)

Cruise altitude was 35000 feet, lower than normal, because the plane was heavy with fuel, and the air temperature was relatively high so the air was thinner than normal at that height.

At about 0200, the relief pilot David Robert returned to the cockpit after his break. Captain Dubois stood up and gave Robert the left hand seat. Dubois left Bonin in control, although David was the more experienced. At 0202 Dubois went out of the cabin to go for a sleep.

At 0205:55, Robert called one of the cabin crew to warn that the plane would be entering turbulent air shortly. She agreed to forewarn the other flight attendants that there would shortly be an announcement to return to seats and fit safety belts.

Robert began to examine the weather radar for the storm ahead. He realised they were heading straight towards an area of strong storm activity. At 0208:07, Robert said to Bonin "You can possibly pull a bit to the left."

There was a noise interpreted as ice crystals hitting the plane, and shortly after there was an alarm indicating that the autopilot has disconnected. This was caused by the Pitot tubes icing over. Temporarily, the pilots had lost all airspeed indications. This should not have been a problem – other

pilots have flown simulations where they have been able to continue quite safely. However, neither Bonin nor Robert had received training in dealing with loss of Indicated Air Speed at high altitude, or in flying the plane in such conditions.

> Once the autopilot was disconnected, the flight control computer changed from “normal law” to “alternate law”, as programmed to do so, in recognition that, because there were some problematic instruments, the pilots should receive more discretion in their actions. “Alternate law” allowed the pilots much greater scope in their actions than would normally be the case.

Until 0210, everything was basically OK. At 0210:06, Bonin said “I have the controls”, and Robert replied “OK”. At this point, for reasons that are not clear – and never will be – Bonin put the plane into a steep climb. The flight control computer issued a chime warning they were leaving the programmed altitude, and the stall warning sounded, “Stall”, in English. This alarm thereafter sounded 75 times before the crash.

Throughout the remainder of the flight, neither of the pilots made any reference to the repeated stall alarms.

> A pilot’s training is always that, in reaction to an approach to stall, the controls should be pushed forward. Bonin kept pulling his control back. A key feature of the Airbus controls is that the pilots control the plane using small side sticks at their sides, almost like games controllers. The right hand pilot’s control stick is on the right hand side, and the left hand pilot’s control stick is on the left hand side. The two pilots’ sticks move independently, so the pilot on the left hand seat cannot feel what the pilot on the right hand seat is doing. Furthermore, it may not be clear to the non-flying pilot what inputs the flying pilot is making because small wrist movements are enough to cause a control input. Robert will, presumably, have been looking at the instrumentation and not at Bonin’s right hand.
>
> One other crucial point at this juncture was that neither out-ranked the other in seniority. When the Captain was present, it was clear who was calling the shots – but until Captain Dubois returned to the cockpit, Bonin and Robert were effectively equals.

11-4: Airbus A330 cockpit showing the positions of the control sticks for the two pilots, on the extreme right and extreme left. (www.airliners.net)

At 0210:07 Robert said “What’s that?” Bonin replied, “There’s no good speed indication”. The plane was now climbing at 7000 feet per minute, and the speed had dropped dramatically to about 110 knots. By 0210:25, the altitude had increased to over 36000 feet.

At 0210:27, Robert said twice “Pay attention to your speed”. Bonin said, “OK, OK, I am descending” but he continued to climb. At 0210:31, Robert said, “Descend – it says we are going up – descend”. Bonin replied “OK”, but Robert said again “Descend”. Bonin said “Here we go, we’re descending” but the plane continued to climb.

(The official French report is strangely coy about being openly or excessively critical of Bonin. The report refers to “inappropriate pilot inputs”. The report does not actually name any of the three pilots.)

At 0210:41, Bonin said (bizarrely) “Yeah, we’re in a climb”.

At 0210:49, Robert was sufficiently worried to use a pushbutton to call Captain Dubois back to the cockpit.

At 0210:56, the engine thrust levers were set to TOGA. ‘TOGA’ means ‘Take Off, Go Around’. Bonin had selected high thrust and raised the nose as if he were climbing away from an aborted landing.

By 0211:03, the ice had melted and the Pitot tubes had unblocked themselves. All the instruments were again functioning normally. From this point onwards there was nothing – *nothing at all* –

wrong with the plane, except the behaviour of Bonin. Bonin announced, again bizarrely, "I am in TOGA, no?" Robert was clearly extremely anxious: "Damn, where is the captain?"

At this point, shortly after 0211, the aircraft was properly stalled. With the engines at full thrust, the pitch angle reached a maximum of 17.9 degrees. The aircraft reached its maximum altitude at 0211:10 of 37924 feet. After this time, the plane descended continuously until the crash. All this time, Bonin kept pulling back his control stick. If he had released his stick the plane would have assumed a nose-down attitude and the plane would have recovered from the stall.

At 0211:21, Robert was becoming desperate. Presumably unaware that Bonin was holding his stick back, he shouted "What the hell is happening? I don't understand what is happening."

At 0211:32 Bonin said "Damn, I have lost control of the plane, I have lost control of the plane!" Robert replied "Left seat taking control!" However, Robert too seems to have missed the point that the plane had stalled (despite the 'Stall' alarm which has been sounding continuously for the last 90 seconds). Robert now pulled back on the stick also – but the plane was stalled, the nose was pitched upwards, the plane was falling at about 6000 feet per minute, and the Angle of Attack was approaching 30 degrees. There were continuous alarms going off in the cockpit: stall warning voice alarms, stall warning chime alarms, chimes warning about altitude, a chirp alarm called a 'cricket'. Shortly after, Bonin resumed control.

At 0211:43, Captain Dubois entered the cockpit. "What the hell are you doing?" he asked, not unreasonably. Both Bonin and Robert said, more-or-less simultaneously, "We've lost control of the plane!" Rate of descent was now 10000 feet per minute, and the Angle of Attack reached 41 degrees. The plane remained more-or-less in this situation for the whole descent.

Dubois did not try to take one of the pilot's seats – he left Bonin and Robert in control. With the stall alarms still calling out every few seconds, no-one discussed the possibility that the aircraft might have stalled. Bonin was still holding his stick back which Captain Dubois, like Robert, did not notice.

For the next minute and a half, the three pilots were unable to work out what was happening, and whether in fact the plane was stalled, despite all the instrumentation telling a consistent story. They even had some exchanges about whether they were descending or climbing. Meanwhile the stall alarm was repeating every few seconds. The one piece of crucial information that Dubois and Robert failed to notice was that, throughout, Bonin was holding his stick back.

(A reminder: It was the middle of the night above the mid-Atlantic, so there were no visual points of reference. Also, the plane was falling at more-or-less constant speed so the pilots will not at this point have been feeling any gross vertical acceleration. Their only sensory input information was as follows:

- What they could deduce from their instruments;
- They should have been able to feel that the nose was pitched up;
- They should also have been aware of buffeting – vertical vibrations – caused by the stalled airflow over the wings;
- They should also have felt pressure changes in their ears as the altitude reduced.)

At 10000 feet Robert tried to take control again. He pushed his stick forward but, with Bonin holding his stick back, the control system averaged the two inputs so the nose remained high.

At 0213:40 (when their altitude was about 9000 feet), Bonin suddenly realised what he had been doing. “But I’ve been at maximum nose-up for a while!” At last, Robert put the nose down and the plane began to regain speed, but it was too late and the plane was now too low to manage a recovery.

At 0214:23, Robert said “Damn we’re going to crash, this can’t be true!” The aircraft hit the sea at 0214:28. Their vertical speed was about 10000 feet per minute, their horizontal speed was about 100 kilometres per hour, the plane was pitched upwards about 15 degrees, and the Angle of Attack was about 40 degrees. The engines were at full throttle.

There had been no Mayday call. There had been no communications with the passengers, most of whom will have been asleep, at least at the onset of the problems. Some passengers will have been woken up by the pitching-up, the buffeting and the changes in air pressure, just in time to wonder what on earth was happening to their plane.

An entirely healthy aircraft, in straight and level high-altitude cruise, had fallen out of the sky and crashed into the sea because one pilot held his control stick back and the other pilots could not work out what was happening.

The Final Report of the Bureau d’Enquetes et d’Analyses concludes, “The aeroplane went into a sustained stall, signalled by the stall warning and strong buffet. Despite these persistent symptoms, the crew never understood that they were stalling and consequently never applied a recovery manoeuvre. The combination of the ergonomics of the warning design, the conditions in which airline pilots are trained and exposed to stalls during their professional training and the process of recurrent training does not generate the expected behaviour in any acceptable reliable way.”

The immediate causes of this accident were:

1. Temporary freezing of the Pitot tubes caused confusion because of loss of all speed indications.
2. Bonin subsequently (and irrationally) pulled back his control stick and intermittently maintained it in that position for several minutes. This caused the aircraft to climb into a dangerously high, nose-up position and thereby stall. Bonin maintained his stick-back position even after the plane was stalling and losing altitude. By the time he had realised his error, it was too late to avoid the crash.
3. The design of the side-sticks meant that what Bonin was doing was not readily apparent either to Robert or to Dubois (when he returned to the cockpit). Furthermore, the design of the control system meant that Robert could not countermand what Bonin was doing.
4. Neither Bonin nor Robert had received training in high-altitude stall recovery.

A contributory factor appears to have been the sophistication of the computerised flight controls. After the two co-pilots had got into difficulties, they seemed to be blinded by the array of information available, and the sophistication of the different layers of automation. It was as if they were confused whether the loss of control was genuine, or whether the digital instrumentation systems were faulty and were giving them bad information. It was as if they were thinking, “Is this real or have the computer systems gone berserk?” That confusion, combined with Bonin’s irrational control stick inputs, caused fatal delays in their reactions.

Captain Solly Sullenberger, the now-retired airline pilot who famously and successfully ditched an Airbus A320 into the Hudson River, New York, on 15th January 2009 after both engines had been wrecked by bird strikes, was interviewed for the magazine *Aviation Week* (20th December 2011) regarding the AF447 accident. "I believe the transport airplane community, as a whole, would not expect the crew to lose all three speed indicators in the cockpit," he said.

Sullenberger went on to say that there is a need for the pilots to receive information about Angle of Attack. "We have to infer angle of attack indirectly by referencing speed. That makes stall recognition and recovery that much more difficult. For more than half a century, we've had the capability to display Angle of Attack in the cockpits of most jet transports, one of the most critical parameters, yet we choose not to do it."

Sullenberger was also critical of training. "Currently, to my knowledge, air transport pilots practice approaches to stalls, never actually stalling the aircraft. These manoeuvres are done at low altitude where they're taught to power out of the manoeuvre with minimum altitude loss." In some aircraft, pilots are taught to pull back on the stick, use maximum thrust and let the Angle of Attack protection adjust nose attitude for optimum wing performance. While this may work for *approach* to stall at low altitude, when the stick-shaker is warning that stall is imminent, it will not provide effective recovery after a high-altitude stall.

"They never get the chance to practice recovery from a high-altitude upset," he continued. "At altitude, you cannot power out of a stall without losing altitude."

Sullenberger also was worried about Situation Awareness in highly automated digital cockpits. "There are design issues in some aircraft that I've always wondered about. For instance, I think the industry should ask questions about situational awareness and non-moving auto-throttles. You lose that peripheral sense of where the thrust [command] is, especially in a big airplane where there is very little engine noise in the cockpit. In some fly-by-wire airplanes, the cockpit flight controls don't move. That's also part of the peripheral perception that pilots have learned to pick up on. But in some airplanes, that's missing and there is no control feel feedback.”

SYNTHESIS

The three accidents described above some aspects in common. The fault sequences of all three were initiated by Pitot tube blockage and loss of Indicated Air Speed. More importantly, however, there were fundamental flaws in the design of the human-machine interfaces which prevented the pilots from making appropriate responses. In all three cases, the pilots lost Situation Awareness.

In the first case (Birgenair 301, Boeing 757) the Pitot tube blockage was probably caused by wasps' nests. The alarms generated by the Electronic Flight Information System were unintelligible to the pilots (with simultaneous low- and high-speed alarms) in the less than three minutes they had to analyse what was happening. The plane stalled and crashed.

In the second accident (Aeroperu 603, Boeing 757) the Pitot tubes had been blocked by masking tape. The accident happened before the report on Birgenair 301 had been published. The same unintelligible alarms were generated. In addition, the static pressure sensors had been taped over, so the pilots were receiving false barometric altitude indications. The pilots were confused and asked Air Traffic Control to supply information, including readouts of their altitude, from the Lima radar. Unfortunately, the Air Traffic Controller in Lima did not realise that the height data on his radar screen were actually the same faulty data which the plane was transmitting to Air Traffic Control via a data downlink. The pilots therefore thought they were still several thousand feet in the air when their plane hit the sea. In this case, therefore, the design of the human-machine interface for the Air Traffic Controller was also faulty.

In the third accident (Air France 447, Airbus A330), temporary blockage of the Pitot tubes by icing was the starting point but, thereafter, the irrational inputs on his control stick from the right-hand seat co-pilot made the situation fatally worse. On the Airbus A330 control stick, small hand movements can make large control input signals, so it was not evident to the non-flying pilot what the flying pilot was doing.

There are many general lessons for design engineers from these (and other) accidents regarding the layout of the control and instrumentation systems – that is, the design of the human-machine interface.

- In fault conditions, the human-machine interface needs to provide clear, unambiguous information, and the pilot-operators must not be bombarded with too many alarms. The objective is to ensure that the pilot-operators can maintain Situation Awareness, that is, they need to be able to retain a good mental model of what state the machine-system is in. (Here 'machine-system' means aircraft, nuclear power station, etc.)
- Pilot-operators are usually not engineers; their default position *must* be to believe the data presented to them.
- AF447 poses an even more fundamental question for design engineers: Should design engineers have to consider the possibility of pilot-operators making completely irrational control inputs, or is it OK to assume that pilots are always rational? If the design engineer cannot assume a rational operator, what can he assume?