NASA SAFETY CENTER

SYSTEM FAILURE CASE STUDY

August 2012 *Volume 6 Issue 7*

"What's Happening?"

The Loss of Air France Flight 447

May 31, 2009: Air France (AF) flight AF447 departed from Rio de Janeiro-Galeão International Airport en route to Paris-Charles de Gaulle Airport with a manifest of 216 passengers and 12 crew members. The flight was normal and maintained contact with Brazilian flight controllers until 1 hour into the flight when communications mysteriously ceased. Thirty-six minutes later, the Aircraft Communications Addressing and Reporting System (ACARS) transmitted a position message. A day later, Air France officially informed the Bureau d'Enquêtes et d'Analyses (BEA), the French aviation safety agency, that AF447 had been lost over the Atlantic Ocean. French and Brazilian investigation efforts began discovering bodies and aircraft wreckage on June 6, 2009. There were no survivors.

PROXIMATE CAUSES

- Cyclical series of erroneous inputs based on a cascade of prompts from aircraft systems
- Failure to identify unreliable airspeed indication
- Failure to identify the approach to stall or fully stalled condition
- Inability to apply appropriate stall recovery controls

UNDERLYING ISSUES

- Design of aircraft systems
- Pilot and copilot training

AFTERMATH

- Changes to training and aircraft systems by Airbus, Air France prior to final report
- Improvements called for in oversight inspection practices, inflight transmission of aircraft performance and location data, air traffic control flight following, search and rescue procedures, and aircraft salvage

Background

The Airbus A330

The Airbus A330, a long-range, wide-body passenger jet considered by many to be a technological tour de force of fly-by-wire controls, is constantly managed by redundant computers through which all human, hardware, and software commands pass.

Governed by a built-in hierarchy of software-driven "laws," the A330 that departed from Rio de Janeiro and became AF447 had received all required maintenance for flight by Air France and was certified as airworthy. As with any unit within a transportation fleet, the aircraft awaited various upgrades when time and components became available. One upgrade on the horizon for the A330 was an installation of a new set of three pitot tubes. These electrically heated probes project out from the aircraft into the flight path and collect air used to measure speed through the airmass (airspeed). Over several years, incidents of pitot tube blockage as a result of ice buildup, despite operative heating, came to the attention of airline operators, aircraft manufacturers, and international regulators as a safety issue, but not as a critical one. Installation of a new and more capable set of probes awaited this aircraft in just a few weeks.

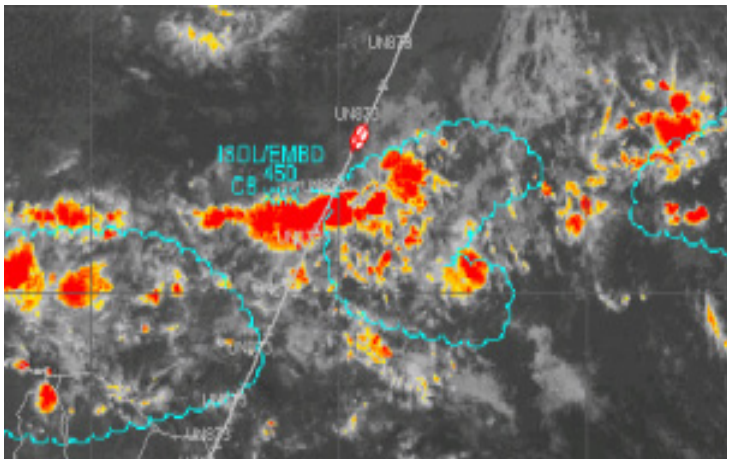

Figure 1: Storm clusters along AF447's flightpath.

The Intertropical Convergence Zone (ITCZ)

Meteorological conditions were typical for the month of June; powerful convective storm clusters on AF447's flightpath were identified and forecast to the crew and schedulers (Figure 1). Oceanic flights regularly traverse these conditions by using onboard radar to avoid such hazards when visual navigation fails (e.g., at night). In darkness, safe and comfortable flight depended on crew decisions taken from radar imagery.

Several other aircraft flying the same path and altitude closely before and after AF447 altered their routes to avoid significant cloud masses containing ice crystals that could rapidly block small openings in the aircraft despite anti-icing systems such as the heated pitot tube.

Mishap Event Sequence

Approaching a band of storms in the ITCZ, the aircraft flew in and out of light turbulence. The captain acted as "pilot not flying" (PNF) and the first officer acted as "pilot flying" (PF). The captain called the second officer to the cockpit as relief so the captain could rest. The three discussed the weather conditions and then the captain departed.

The co-pilots identified upcoming clouds on the radar that they were unable to avoid by climbing above their current 35,000-ft altitude. The PF made a slight turn and the PNF switched on engine de-icing equipment. Reducing power to slow entry into turbulence for passenger comfort, AF447 entered icing conditions. At 2 hr and 10 min into the flight, the autopilot suddenly disconnected. The Airbus 330 computers warned the crew of this through a cockpit Electronic Centralized Aircraft Monitoring (ECAMS) display. The PF took the controls manually—an unfavorable scenario considering turbulence and the difficulty presented by flying in the thin atmosphere. The conditions triggered the computers to switch to a mode called "Alternate Law." Many safety protections were lost, including automatic prevention of stall. Due to the thin air density at 35,000 ft, aircraft controllability was poor compared to that in the denser air below. The safe margin between maximum safe airspeed and stall airspeed was sharply reduced. Flying manually at the current altitude, a pilot could easily overspeed or stall the aircraft in seconds if control inputs were too large. Taking the controls at night, in turbulent weather, with reduced power, the PF did something startling—he raised the nose of the aircraft. For reasons he did not understand, cockpit airspeed indication was increasing toward overspeed. But in reality, the A330's airspeed was dropping rapidly. All three pitot tubes had become blocked with ice and were sending wildly variable and unreliable data to the computers. The computers were programmed to vote on the majority of readings and display an ECAMS warning to check for unreliable airspeed. The PNF was trained to read and respond to ECAMS displays, but Air France crew training also relied on the captain's leadership to direct cockpit tasking in emergencies. The captain was still missing from the cockpit. The PNF started to call out the many ECAMS messages such as loss of autothrust and reconfiguration to alternate law, possibly adding to the confusion. For the next 40 seconds, the crew maintained the low-power, high-pitch condition. Designed to assist pilot inputs within its software logic rules, the A330 automatically helped the PF maintain the commanded pitch, trimming out the aerodynamic load on the aircraft's elevators so that high pitch became the aerodynamically stable attitude of the aircraft (Figure 2). As the aircraft slowed, the angle between its path and the relative wind (called angle of attack) increased toward stall. But despite an audible, repeated synthetic voice stall warning, the crew never reacted as if they had entered a stall.

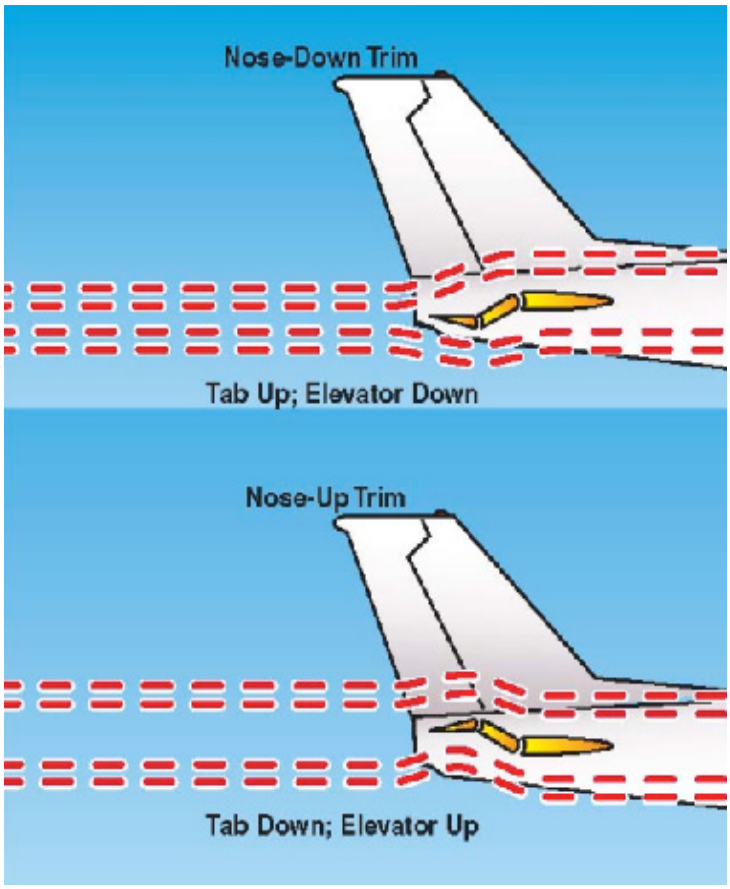

Figure 2: Trim tabs relieve pilot workload by aerodynamically countering pressures on a control surface.

AF447 plummeted. The crew's dialogue taken from recovered flight recorder data indicates they reacted to several of the many cues on the instrument panel but could not comprehend the situation. One cue that called for attention, reinforced to the PF over thousands of hours of flying, was the Flight Director (FD), a set of vertical and horizontal needles appearing on the attitude indicator (artificial horizon) (Figure 3). The FD advises the PF how high or low to pitch the nose and which way to roll the wings. The FD had disconnected itself along with the autopilot, but re-connected itself seconds later. Post-crash analysis showed that many PF control inputs seemed to match FD cues, cues that were unreliable because of the airspeed indication problem. The FD had prompted the PF to pitch AF447's nose up.

AF447 was in a full stall—a condition the crew had never trained for in an A330. Worse, the aircraft had by now trimmed itself to stay stalled. All pilots are trained to recover from stalls in small aircraft by regaining lift and airspeed. Since many crashes historically have stalled close to the ground, stall prevention procedures such as Air France's employed minimal nose-down pitch and maximum power. This was taught to reduce altitude loss close to the ground. While effective as an A330 approaches a stall in low-altitude controlled flight, this technique fails to regain lift or airspeed after fully stalling at higher altitudes. Once stalled at high angle of attack and pitch angle, pilot action to increase thrust actually pitches the nose up higher because of the underwing engine thrust relative to the aircraft's center of gravity. A concerted effort to lower the nose and reduce thrust could have possibly recovered AF447 early in the stall, but the crew had not even recognized the unreliable airspeed or the stall. The stall warning system blared on and off, triggered by accurate angle of attack data fed to the computers, but not displayed visually to the pilots. They fought valiantly to understand and recover, with the returning Captain's help, for almost four minutes before slamming into the water at over 11,00ft/min (approximately 100 mph).

Investigation

The complex BEA salvage effort to locate the wreckage and the vital flight data and cockpit voice recorder finally concluded successfully in April 2011. The final BEA report was published on July 5, 2012. For brevity's sake in this study, selected summaries of the 51 findings, 10 causes, and 41 recommendations are presented in three areas: proximate causes, design, and training.

Proximate Causes

AF447 crashed because of a cyclical series of erroneous inputs based on unreliable prompts from aircraft systems; a cycle that fed on itself to the extent that control was never regained. The BEA's final report attributes multiple factors to the AF447 mishap: temporary and repeated inconsistencies and loss of airspeed indication; inappropriate control inputs; failure to identify unreliable indicated speed; the approach to stall; the full stall state; and the inability to apply an appropriate response in these flight regimes.

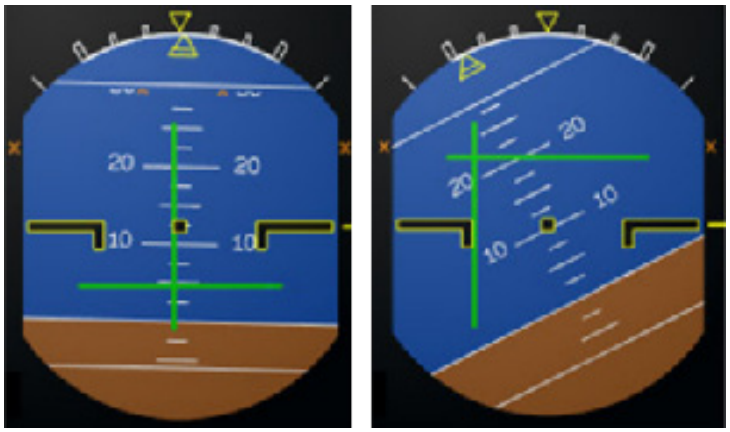

Figure 3: The left FD is directing the pilot to maneuver the aircraft down approximately 5 degrees. The right FD is directing the pilot to pitch the aircraft up over 10 degrees and to roll the left.

Underlying Issues

Design

Airspeed inconsistencies, which began after pitot tube icing, were recognized by the A330 flight computer but difficult to detect on cockpit displays according to 13 other crews who had previously experienced airspeed indication issues.

In addition, the A330 Alternate Law regime provided no angle of attack flight control protection. This permitted the PF to attain stall angle of attack and the aircraft to trim itself to maintain a high-pitch angle. The FD, using unreliable airspeed measurements because of the blocked pitot tubes, at best offered the PF confusing prompts, and at worst, encouraged self-defeating, pitch-up maneuvers. Eleven seconds after the autopilot disconnected, the PNF said, "We've lost the speeds…alternate law protections," but the crew's later words and actions lacked evidence that they comprehended which cues should drive decisions to employ emergency procedures such as Unreliable Airspeed or Stall Recovery. The PNF asked during the stall, "Do you understand what's happening or not?" and "What's happening?" But the PF could only answer, "We're losing control of the airplane here."

The aural stall warning system appears to have been ignored. Post-crash investigators postulated that the aural cues did not register with the pilots because of the lack of exposure to stalls, aircraft buffet (also present during overspeed), and associated warnings. Even some crews previously exposed to transient A330 stall warnings disregarded them as spurious. Installation of an angle-of-attack indicator in the cockpit using data already available to the computers could have provided the key crosscheck to diagnose unreliable airspeed, as well as a key flight instrument to safely fly the aircraft in that condition.

The flight director needles likely provided confusing and unreliable cues, misleading the pilots. Once source information was determined to be unreliable, the disconnected FD should have remained disconnected until the crew determined reliable source data (in this case airspeed) was regained, and they could re-engage it themselves.

It is important to note that unlike most aircraft with two sets of cockpit controls, the Airbus sidestick controllers used for pitch and roll inputs are not cross-connected. Thus, in the AF 447 final descent, the PNF had no physical cue that the PF was commanding nose-up most of the time. No recommendations were made in the report, but training and procedures to address this unique design would preclude negative transfer of training from other aircraft with cross-connected controls.

Training

Minimal training for the manual aircraft handling at high altitude, especially in approach to stall and stall regimes, was part of a larger, standardized training package for the family of Airbus aircraft according to test pilots who were previously the only aircrew to actually experience full airborne stalls in these aircraft. The data package gathered from flight tests and used for simulator programming did not include out-of-control stalled flight data because no requirement for such data was made. Therefore, even if crews desired to practice full stalls in the simulator, true stall performance from which to perform recoveries that would actually work in the aircraft could not be simulated. Even if the simulator had such fidelity, the crews lacked recurrent training in the effects of altitude changes on aerodynamic controllability. Other Airbus crews could have made the large sidestick inputs that bled off kinetic energy and allowed AF447 to stall.

Investigators found a lack of crew coordination in the AF447 crew when faced with this emergency; but they also found that other crews could have met the same fate. Within the European Aviation Safety Agency (EASA), no standardized instruction or instructor qualification existed in this area, called Crew Resource Management (CRM). Observed examples of CRM training lacked a surprise factor that would challenge crews to overcome truly unplanned events through leadership and teamwork.

Aftermath

Several BEA recommendations were made in interim reports and acted upon by Airbus, Air France, and other organizations prior to the final report. Besides addressing training and the aircraft systems, improvements were called for in oversight inspection practices, inflight transmission of aircraft performance and location data, air traffic control flight following, search and rescue procedures, and aircraft salvage.

Relevance to NASA

Design of innovative, complex human-operated systems presents incredible challenge on many fronts. For example, mechanically advanced aircraft without computers and software in the control loop were understood by their pilots on a level deep enough to ensure rapid, effective reactions versus all but the most insidious hazardous conditions. But as hardware evolved, it seemed clear that automation could preclude human choices that resulted in bad outcomes—commonly called errors. Increased software-controlled automation of operator tasks has increased operator training workload to merely understand all modes of normal operation. Additionally, off-normal failure modes have increased. To truly comprehend one instrument indication, the operator must understand all ways that indication can occur; otherwise, the operator cannot troubleshoot failure in time to intervene effectively. Complex systems test the real-time limits of diagnostic skill when failure indications proliferate. What is real and what is a false indication? Is there a common thread between multiple different warnings? Does the procedure actually address how the system is behaving? Which option will improve the situation right now? These are questions the expert operator expects to answer in seconds when time-critical failures occur. Only when design and training respect the day-to-day limits of human comprehension and team performance can reliable operation continue.

Training must build confidence in one's mastery of not only the system in all its changing, dynamic modes but the surrounding environment. One interface between training and design is testing. Cost and schedule limits to test scenarios raise the question, among others, "What scenarios describe unacceptable risks?" If the system is entering service in an operational role as opposed to an experimental test role and there is risk to the public, data must be gathered to mitigate needless risks to a level acceptable to the public. NASA and commercial companies share technologies to open the high ground of space to commerce, just as the airways began to open nearly a century ago. Both would be well-served to study the Air France 447 disaster.

References

A330 Flight Laws. Nov, 2005. PDF. http:// http://www.smartcockpit.com/data/pdfs/plane/airbus/A330/instructor/A_0-Flight_Laws.pdf [accessed July 18, 2012]

Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile, Government of France. *Final Report On 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*. July, 2012. English Trans.

Wainwright, William. 1999. "Airplane Upset Recovery." FAST24: Airbus Technical Digest: May 1999: 18–23

SYSTEM FAILURE CASE STUDY

NSC

NASA SAFETY CENTER

Responsible NASA Official: Steve Lilley steve.k.lilley@nasa.gov