RISK AWARE
Insights in Risk Management
Issue 10

Equipment failures – examples from US civil aviation

Aircraft systems provide an interesting insight into many of the principles of Failure Modes and Effects Analysis (FMEA). Redundant systems, layered protections and detection of faults are important parts of modern aviation designs.

Although many potential failure modes can be anticipated in advance, it often happens that mishaps and actual failures are sources of much additional information. Not all mishaps result in loss of life – but sadly in two of the cases outlined here, aircraft were on landing approaches where very little time was available for the flight crews to identify the failure and take corrective actions. All lives were lost on both aircraft.

The two tragic accidents were eventually traced to the same failure – although in the first accident other causes were wrongly attributed initially.

The accidents

A United Airlines Boeing 737 collided with terrain when approaching Colorado Springs, CO airport in 1991[1]. In similar circumstances a USAir Boeing 737 was lost on approach to Pittsburgh, PA airport in 1994[2]. In both cases the aircraft experienced sudden and excessive roll and heading changes, thought to be initiated by turbulence. Owing to altitude, airspeed and other factors, the crews were unable to regain control prior to impact.

Until the detailed investigation of the Pittsburgh accident, the most likely cause of the earlier accident was listed as wind shear due to "mountain rotors," a type of horizontal axis vortex air flow common in the Colorado Springs area in windy conditions, in the lee of the mountains.

At Pittsburgh, wake turbulence from other aircraft was suspected. It was only after methodical testing of various possibilities that focus was brought onto hydraulic component failure – eventually leading to a re-investigation of the Colorado Springs accident. Further evidence came from a 1996 report of a 737 aircraft encountering similar unexplained problems mid flight over Richmond, VA, this time with no injuries and control being regained soon after.

What went wrong?

In the Pittsburgh investigation, NTSB faced several possibilities that may have explained a sudden roll and turning motion. The investigation had ruled out in-flight fire, bomb explosion, structural failure and the like, and was now focusing on aircraft equipment failure. Initially there was not much emphasis on the hydraulic systems given the in-built redundancy provided by two active pump systems plus a standby system. The investigation listed:

- Engine failure
- Engine thrust failure (eg thrust reverser deployment)
- Asymmetric spoiler/aileron activation
- Transient electronic signals causing uncommanded flight control movements
- Yaw damper malfunction
- Rudder cable broken

As it happened, none of these was able to explain the sudden aircraft movement encountered. It was noted that problems from transient electronic signals would have been easily overcome by the flight crew simply reverting to manual controls.

Finally the rudder Power Control Unit (PCU) was suspected. Like power steering in a car, it is able to function in manual mode in the event hydraulic pressure is lost. It was found that under some circumstances the control servo valve was able to jam in an overtravel position, causing the main actuator cylinder to drive the rudder fully to one side, without any flight crew inputs. The same type of PCU was implicated at Colorado Springs and Richmond.

Once the uncommanded rudder move occurred, several other things conspired to make the situation critical:

- The flight crew were not aware that the rudder had made an uncommanded move. They immediately tried to use the cockpit control pedals to steer the aircraft back onto course, but could not successfully overcome the hydraulic pressure opposing. The pedals and mechanical cables were designed to provide rudder movement in the event of hydraulic pressure failure.
- In some circumstances it was possible to counteract an uncommanded rudder movement by using other controls, but USAir flight crew training had not yet addressed that issue.
- The design of the 737 rudder was one of a single panel – meaning that other panels were not available to counteract an uncommanded move. Most other comparable aircraft at the time had split panel rudders.
- There was very little time to react – the initial rudder move occurred only 27 seconds before eventual impact.

What can these accidents tell us about FMEA?

- Redundancy is an important design issue in safety-critical systems. This may include active redundancy, where a parallel system continues to provide the function, or passive systems where switchover is required.
- Detecting a fault and alerting operators is important.
- Contingency measures (training, etc) may be necessary in order to deal with certain failure types.
- Past failures and anomalies build up a body of evidence. Appropriate culture and investigation systems are needed to encourage reporting. The report of the Richmond incident was a key part in improving the knowledge base.
- The body of evidence comes from the industry and the world, not just the local enterprise.
- High consequence failures demand a rigorous approach.

References:

1. National Transportation Safety Board, 1992. *United Airlines Flight 585... Colorado Springs, Colorado, Mar 3, 1991.* Aircraft Accident Report NTSB/AAR-92/06, Washington DC.
2. National Transportation Safety Board, 1999. *USAir Flight 427... near Aliquippa, Pennsylvania, Sep 8, 1994.* Aircraft Accident Report NTSB/AAR-99/01, Washington DC.

For more information, please contact:

Advitech Pty Limited
1 Elizabeth Street
Tighes Hill Newcastle NSW 2297

Tel 02 4961 6544
mail@advitech.com.au
http://www.advitech.com.au