National Aeronautics and Space Administration

System Failure Case Studies

AUGUST 2008 Volume 2 Issue 6

No Left Turns

On July 19, 1989, after a catastrophic engine failure and loss of hydraulic flight controls, United Airlines Flight 232 crashed in an attempted emergency landing at Sioux Gateway Airport in Sioux City, Iowa. Mid-flight, the tail mounted engine on the McDonnell Douglas DC-10 exploded, subsequently severing the plane's hydraulic control systems and leaving control of the aircraft nearly impossible. While the pilots were able to maneuver the plane to the closest runway, 111 of the 296 people on board died in the crash. Many safety and quality control questions emerged from this disaster, including flight control systems failure, jet engine construction processes and testing, pilot training, and flight procedures.

BACKGROUND

United Airlines Flight 232 was en route from Denver, Colorado to Philadelphia, Pennsylvania with a planned stop in Chicago, Illinois. The plane was a McDonnell Douglas DC-10 with three General Electric engines, one on each wing and one mounted in the tail structure (Figure 1). The tail mounted engine (engine #2) had no previously recorded problems and had been inspected approximately one year prior to the crash. The engine had already undergone five other inspections and was 1,101 take-off/landing cycles below the mandatory engine lifetime maximum of 18,000 cycles. While the engine was over fifteen years old, it was compliant with Federal Aviation Administration (FAA) standards. The plane was piloted by Captain Alfred C. Haynes, a former Marine pilot with thirty-three years of flight service with United Airlines. The copilot was William R. Records, and the cockpit also held flight engineer Dudley J. Dvorak and a pilot trainee. Additionally, DC-10 flight instructor, Captain Dennis E. Fitch was a passenger on the plane.

Hydraulic Controls

The principal controls of the DC-10 aircraft (rudder, elevator, ailerons) as well as the wing flaps, brakes, and landing gear all functioned with a hydraulic system. The hydraulic controls were designed to operate with three independent systems to provide full operation and control in the event that one or two of the hydraulic systems failed (a two-fault tolerant design). However, there were no additional provisions for manual control of the aircraft. This meant that at least one hydraulic system had to be operational with hydraulic fluid and pressure in order to control the aircraft.

Figure 1: McDonnell Douglas DC-10 aircraft.

WHAT HAPPENED?

Engine Failure

Not long after the flight reached its cruising altitude of 37,000 feet, at 3:16 pm on July 19, 1989, the crew and passengers felt and heard the explosive rupture of the #2 engine from the rear of the plane followed by severe vibrations. The fan rotor disk on the front of the engine had

United Airlines Flight 232 crash killed 111 passengers.

Proximate Cause:

- The fan rotor assembly catastrophically failed due to prolonged fatigue stresses, exploding the engine and severing the hydraulic lines

Underlying Issues:

- The engine manufacturing process left microscopic defects below the surface in the engine fan rotor
- Multiple inspections failed to identify crack growth
- There was no contingency for the loss of hydraulic controls in system design, procedures, or training

failed, resulting in the fan blades breaking into sharp fragments and ripping the engine apart. The explosive release of engine pieces and fan blades tore gashes into the aircraft stabilizers in the rear of the plane and severed the first and third systems' hydraulic lines (Figure 2). Additionally, parts of the first and second hydraulic systems were ripped off with the initial explosion of the engine. The gashes in the hydraulic lines and missing parts of the system forced a loss of pressure and quick loss of the hydraulic fluid in all three systems. Within two minutes of the explosion, all hydraulic fluid had completely drained from the lines.

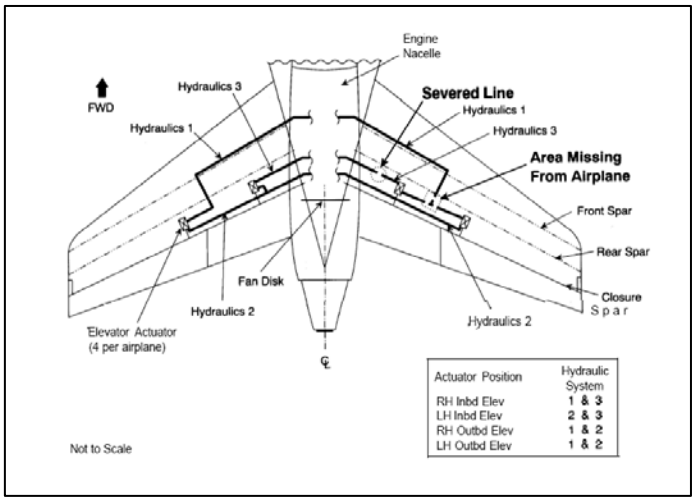

Figure 2: Schematic of hydraulic lines.

Loss of Control

The aircraft immediately began descending and banking to the right. The pilots quickly disengaged the autopilot, shut down the #2 engine, and attempted to correct the plane's roll, but the aircraft did not respond to any controls movements. The pilots then noticed that the hydraulic gauges read empty and realized that they had no control of the aircraft. "The damage was so catastrophic," noted Captain Haynes, "that United's flight manuals have no instructions on how to proceed."

As the plane continued to descend, Captain Fitch, a DC-10 flight instructor riding in the cabin, quickly came forward and offered his assistance. The pilots gladly accepted. To bring the plane out of a roll and level it out, Captain Fitch only had the left and right engine throttles to control the plane. While the plane was slow to react, constant manipulation of the throttles leveled it out. But in using the throttles, they could only control one axis of motion at a time. They were able to raise or lower the nose by speeding up or slowing down the engines, and they could make unstable but manageable turns to the right by slowing one engine down and speeding up the other. However, they could only turn right, meaning that to turn 60 degrees to the left, they had to turn 300 degrees to the right. In addition, to maintain a constant heading, they kept the left throttle at 100 percent and the right at 73 percent. In order to remain level, the aircraft had to maintain a high level of speed.

Emergency Landing

The nearest runway for an attempt at an emergency landing was in Sioux City, Iowa. With Captain Fitch on the floor to closely manipulate the throttles and Captain Haynes spotting the aircraft's responses, the pilots worked together to make three large looping turns, trying to line up the plane with Runway 31. Unsuccessful, they were only able to line up to the shorter Runway 22 at the airport, which also had an undesirable 11-knot tail wind on their approach. According to communications between the pilots and traffic controllers, given the tentative control over the plane, the pilots wanted to get on the ground immediately and did not want to risk flying to a larger airport. While descending, the plane would occasionally dip and bank to the right without warning, but the pilots were able to correct this each time. As the plane neared the end of its approach, Captain Haynes attempted to decrease the speed, causing the plane to roll to the right. The pilots tried to correct this by quickly accelerating, but it was too late.

At a speed of about 191 knots (220 mph) and at a 20 degree roll to the right, the right wing touched ground first, followed by the right engine and then the wheels. The right engine quickly burst into flames after contact with the ground, and the plane skidded along the side of the runway. The fiery right wing and tail portion of the plane broke off as the main body caught fire and slid into a corn field on the right side of the runway. The nose of the plane, including the cockpit, snapped off as the main fuselage finally stopped near the end of the runway in the tall corn stalks at 4:00 pm, approximately 44 minutes after the explosion of the tail engine.

Rescue Teams

Rescue teams were in place on the ground when the plane crashed, and within seconds, fire fighters were spraying down the blazing aircraft. While some of the passengers were able to evacuate the burning plane, many were trapped inside. Roads to the airport were shut down, and medical teams were standing by as the rescuers attempted to clear the plane and get people to the hospital as quickly as possible. While the rescue process was praised by the FAA for its level of preparedness, many passengers died of asphyxiation as they were trapped inside of the burning plane. Overall, 111 of the 296 passengers and crew on board died in the event.

Proximate Cause

According to the National Transportation Safety Board (NTSB), this disaster was initiated by at least one crack in the fan rotor, originating from the manufacturing and

propagating due to long-term fatigue stress. This resulted in the catastrophic separation, fragmentation, and expulsion of the Stage 1 fan rotor assembly in the #2 engine.

Underlying Issues

Latent Manufacturing Defects

The series of events that led to this disaster were ultimately traced back to the initial production of the engine by General Electric Aircraft Engines (GEAE). The NTSB Accident Report cited the initial problem in the manufacturing of the fan rotor.

In 1971, eighteen years prior to the failure, during the purification of the titanium-alloy rotor, a "hard alpha inclusion" (a microstructural defect that occurs from an inadequate vacuum during melt processing) formed within a cavity in the rotor. The rotor left the foundry with the defect unnoticed after its initial certification process. During the rotor's normal use, one, if not more, fatigue cracks initiated from this defect area and grew (through sub-critical crack growth) until finally the rotor failed. The fatigued region on the inside diameter of the disk where the crack(s) propagated is shown in Figure 3.

As part of the engine certification process in 1971, GEAE presented their calculations to the FAA, indicating that a "defect-free" engine would not fail within a life of 54,000 take-off/landing cycles. The FAA set the safety limit at 18,000 cycles, representing a factor of safety of 3. The engine that failed was only at 16,899 cycles, well within the limits. In addition, the engine had already undergone six mandatory shop visits, and there had never been any abnormal engine operation reported.

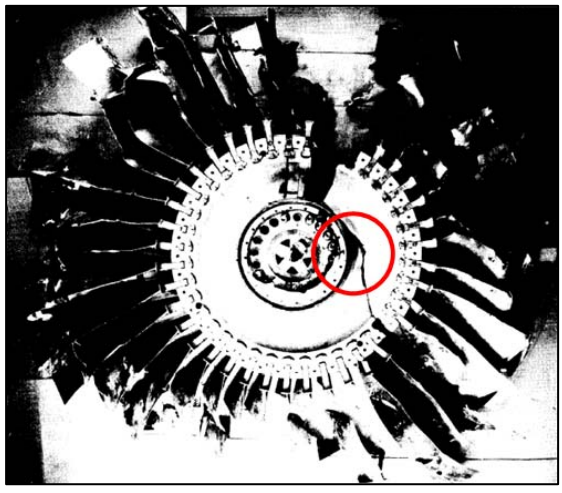

Figure 3: Reconstruction of the broken rotor. The red circle shows the initial area of separation in the Stage 1 fan rotor disk.

Failed Detection

The rotor had undergone an inspection approximately one year prior to failing, during which the United Airlines inspectors performed a Fluorescent (dye) Penetrant Inspection (FPI), a process of checking parts for cracks. The NTSB also conducted an in depth analysis of the rotor after the crash. They found slight discoloration around the area of the crack, indicating that United Airlines inspection teams had indeed examined that area with the FPI technique prior to the engine failure. GEAE fracture mechanics experts estimated that at the time of the last inspection there must have been a crack almost 0.5 inches long along the inner bore surface of the rotor. Further, the NTSB noted that a crack of this size, if it truly existed at the time of the inspection, should have had a high probability of detection if the inspection was done correctly. Because of this, the NTSB cited human error for failing to identify the crack during the sixth shop visit.

United Airlines Procedures

The United Airlines flight manual had procedures for a partial loss of aircraft control but nothing for a complete hydraulic failure. The control system itself had no contingency for total hydraulic failure. A DC-10 pilot noted soon after the crash, "We have procedures for what to do if you lose some of your controls but nothing for a total failure … We could add a page to the manual, but we might as well write on it, 'Good luck.'" The pilots had never trained for this type of disaster but were miraculously able to steer the plane to a runway using only the two remaining engines.

Aftermath

Improved Manufacturing Process

Within ten years of the crash, individual passenger lawsuits against United Airlines and General Electric totaled more than $100 million. GEAE claimed responsibility for the faulty engine construction. Ironically, just one year after GEAE created the faulty rotor, they upgraded the rotor manufacturing practice to a premium quality triple-melt process that greatly reduced the risk of internal flaws. So while the defective manufacturing practice was revealed in the crash, this process had already been fixed for 18 years. This allowed the FAA to focus on just the remaining rotors created under the old manufacturing process. The FAA called for a thorough investigation of these parts using a handheld immersion-ultrasonic procedure that could detect cracks of at least 0.1 inches. GEAE safely replaced all of the potentially faulty rotors (two were found) and added this technique along with a third to the inspection procedures manual.

Improved Hydraulic Design

As a direct result of the crash, on September 15, 1989, McConnell Douglas announced their design to enhance the redundant hydraulic system on all of their DC-10 aircrafts. They implemented a system of shut-off valves and automatic sensors to these valves when hydraulic pressure is low. This system locks pressure in the hydraulic reser-

voirs if a similar breach occurs on all three lines. This leaves the aircraft with minimal controls, but flight controls nonetheless.

Enhanced Training

The pilots had never trained for this type of disaster. In an attempt to recreate this scenario, the NTSB developed a simulation of the incident, and DC-10 rated pilots were asked to fly the simulation. Unfortunately, the simulation study concluded that "such a maneuver involved many unknown variables and was not trainable." Nonetheless, the NTSB delivered a letter to McDonnell Douglas describing multiple suggested techniques to maneuver and control a DC-10 under complete hydraulic loss using alternating engine speeds, but it was not a step-by-step manual for this scenario.

"We have procedures for what to do if you lose *some* of your controls but nothing for a total failure …

We could add a page to the manual, but we might as well write on it 'Good Luck.' "

Applicability to NASA

After a single failure drained the fluid in all three hydraulic systems on Flight 232, there were no provisions for manual command of plane's principle controls. Designs for key systems should protect against a single failure that could nullify redundancy.

The assumptions behind calculations of safety margins can prove critical, particularly when component lifetime is a significant issue. The original engine manufacturers used an imperfect process on a safety-critical part that resulted in latent defects. But when estimating the operating lifetime of the engine, it was assumed that all of the parts were defect free. This was a critical mistake that was never re-evaluated, even though the manufacturer abandoned that process over eighteen years before the failure. As NASA mission operations typically span multiple years, initial assumptions must be routinely questioned to ensure their current applicability, especially since, in space exploration, the replacement of critical parts is not always an option. This is particularly significant, since not all defects may be readily detectable early in a component's lifetime.

Additionally, this highlights the importance of maintaining a keen level of rigor throughout safety and maintenance checks, even after years of numerous successful inspections. Inspection procedures should recognize the possibility of human error and account for the tendency for complacency over time. Detailed quality control techniques are critical to a mission and project's success.

Operating procedures may not always include descriptions of all tasks, especially those that are more uncommon or unexpected. The pilots of Flight 232 had never trained for a complete loss of control but quickly responded using their knowledge of the aircraft. This case reminds NASA managers and astronauts of the importance of thorough understanding of systems and contingency plans, as well as off-nominal training, to enable better response to unplanned events.

Questions for Discussion

- Have you practiced for off-nominal or emergency situations?
- Have you ever been in a situation where operating procedures were not defined for a particular task? If so, how did you respond? Are there now operating procedures for that task?
- Are you confident in the maintenance procedures and quality control of safety critical parts?
- Are redundant systems thoroughly analyzed for and protected from common failure modes?

References:

Kilroy, Chris. *Special Report: United Airlines Flight 232*. AirDisaster.com. Website: http://www.airdisaster.com/special/special-ua232.shtml

Larson et al. *Responding to Emergencies: Lessons Learned and the Need for Analysis.* Interfaces 36(6). pg. 486-501. Informs 2006.

National Transportation Safety Board. Aircraft Accident Report: United Flight 232. McDonnell Douglas DC-10-10. Sioux City, Iowa, July 19, 1989. Hydraulic Lines, Reconstruction of Broken Rotor, [Images].

National Transportation Safety Board. Brief of Accident. Adopted 10/08/1992. DCA89MA063 File No. 437.

Parker, Laura, et al. "Pilots Added Page to DC-10 Manual; For 41 Harrowing Minutes, Cockpit Team Improvised in Flying Jet." The Washington Post. July 23, 1989.

McDonnell Douglas DC-10 aircraft. [Online image], http://www.flightsoft.com/fth4product.htm.

System Failure Case Studies
A product of the NASA Safety Center

Executive Editor: Steve Wander stephen.m.wander@nasa.gov
Developed by: ARES Corporation

We thank the NTSB for its cooperation and support during the development of this case study.

To view this document online and/or to find additional System Failure Case Studies, go to http://pbma.nasa.gov