

System Failure Case Studies

JANUARY 2007

Volume 1 Issue 3

ALMOST PERFECT

On the morning of January 19, 1995, a final series of flight tests was conducted for the first of two aircraft built for the X-31 Enhanced Fighter Mobility Demonstrator program. While executing a sequence of maneuvers for the third and final flight of the day, the pilot noticed a discrepancy in his air speed indication. About two minutes later, the aircraft began to oscillate out of control, pitched up violently, departed into a spin, and crashed. The pilot ejected safely and was recovered less than one mile from the crash site. An investigation of the X-31 crash examined the mechanical, procedural, and human systems that supported X-31 and continue to support projects throughout the aerospace community.



The X-31 in flight over Edwards Air Force Base.

BACKGROUND: ENHANCED FIGHTER MANEUVERABILITY DEMONSTRATOR

The X-31 program began in the early 1980's to explore the tactical utility of a thrust-vector aircraft with advanced flight control systems. The X-31 aircraft was designed specifically for this task, with large paddles to redirect exhaust flow as well as an advanced "fly-by-wire" flight control system. Thrust vectoring refers to an aircraft's ability to redirect the thrust from its main engine in a direction other than straight backward. The technique is used to provide vertical thrust to aircraft such as the Hawker-Siddeley Harrier and the F-22A Raptor for vertical and/or short take-off and landing (VTOL / STOL).

To control the thrust-vectoring paddles and flight surfaces of the X-31, a complex flight control system (FCS) was developed. The system included four digital flight control computers. Three synchronous main computers drove the flight control surfaces. The fourth computer served as a tie-breaker in case the three main computers produced conflicting commands. The FCS relied on inputs from sensors throughout the aircraft to achieve its high level of control and maneuverability. One of the key inputs required for the FCS was air speed. Air speed for the X-31 (and most conventional aircraft) is calculated based on inputs from a device called a Pitot tube.

The air data computer (ADC) determines the velocity of airflow from the pressure difference between the static air pressure and the pressure created by air flow in the direction of travel in the Pitot tube. On the X-31, the Pitot tube provided air speed data to instruments in the cockpit, the aircraft's flight control computers, and the mission control center monitors at Dryden Flight Research Center.

In January of 1995, the X-31 lost control, resulting in the first crash in more than 520 successful flights.

Proximate Cause:

- Blocked Pitot tube (due to icing) caused erroneous readings to be sent to the flight control computers

Underlying Issues:

- Incomplete/improper interpretation of hazards analysis
- Breakdown in configuration management and change documentation
- Failure to impose proper ops controls and take preventative action

WHAT HAPPENED?

The Crash

On January 19, 1995, the flight began as expected, but a review of flight data shows that air speed indication began to show errors about 20 minutes into the flight. At some point later, the pilot turned on the Pitot heat switch (a sign that he suspected problems with the air speed indicator). He then informed the control room, "Pitot heat turned on, remind me to turn it off later."

Difficulties Emerge

In the control room, a discussion began among some of the project engineers as to whether or not the Pitot heat was operable. Meanwhile, the pilot noticed further errors in air speed indication and informed the control room, "Airspeed is off, 207 knots at 20 degrees [angle of attack] AoA." When interviewed after the mishap, other X-31 pilots stated that air speed should have been around 150 knots at 20 degrees AoA. Unknown to the pilot and the control room, ice had begun to accumulate around the Pitot tube, blocking air flow and contributing to an extremely hazardous situation.

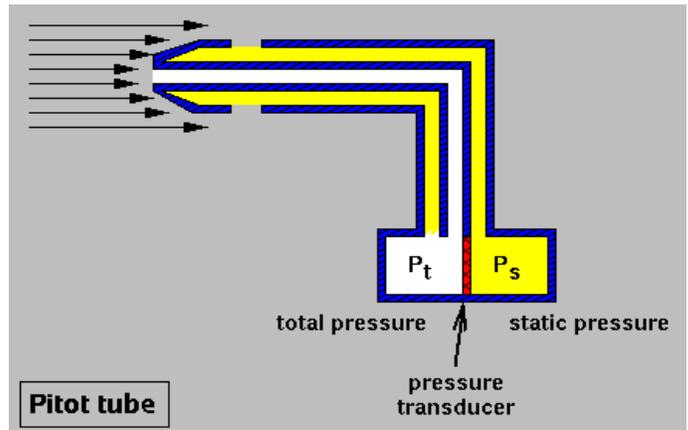
More than two minutes after informing the control room about turning on the Pitot heat, the control room informed the pilot that the Pitot heat "...may not be hooked up." Nine seconds after receiving this message, a warning tone sounded and the pilot identified the master caution light. The aircraft began to oscillate out of control then violently pitched upward. The pilot ejected before the aircraft departed into a spin moments later. The aircraft subsequently crashed into an area of vacant desert.



Three large, heat-resistant paddles on the rear of the X-31 were used to re-direct the engine exhaust and provide thrust-vectoring flight control. (Note the Pitot tube that is visible at the front of the aircraft.)

PROXIMATE CAUSE

The Mishap Investigation Board found that "The [Pitot tube] icing led to incorrect total air pressure data being sent to the flight control computers (FCC) by the Pitot-static system. This resulted in the aircraft becoming unstable as it accelerated and descended to return for landing."



The Pitot tube measures air speed by evaluating the difference between the static air pressure and the total air pressure induced by the airflow.

UNDERLYING ISSUES

The underlying causes of the mishap, as reported by the Board, were inaccurate system safety analyses and a breakdown in the appropriate dissemination of safety-critical information.

Incomplete Hazards Analysis

A hazard analysis completed in February of 1988 correctly identified the hazard for loss of Pitot-static signal and identified the cause as a plugged tube, though it was not categorized as a critical failure. During this analysis (and others that followed) it was assumed that the ADC control system's ability to detect invalid air data and the availability of reversionary (or "back-up") flight control modes completely addressed the hazard.

The Mishap Investigation Board reported, "The error in this case was in confusing the probability and the severity of the hazard." Because the probability of total pressure being lost in the Pitot tube was low, the unlikelihood of failure was erroneously perceived as a means of controlling the risk, even though they had several indications that such a failure would be severe. A lack of documentation of the significance of this risk also meant future program personnel would probably not be made aware of this hazard.

The problem throughout all the hazard analyses was "...the misconception that the FCS was capable of detecting the full range of Pitot-static failures." In fact, the ADC's ability to detect errors was limited to abrupt failures, such as those due to a bird strike or debris suddenly damaging or plugging the Pitot tube. On the day of the crash, the Pitot tube failure was due to a gradual accumulation of ice. The X-31 was restricted to flying in clear skies where icing is normally not a concern, and the ADC was unable to detect the gradual failure that prevented the air flow into the Pitot tube.

Failed Configuration Management

The flawed assumptions of the hazard analysis were compounded by a breakdown in configuration management processes. In the original X-31 design, the Pitot tube was mounted on a device called a Rosemount probe. To improve air speed indication at high AoAs, the Rosemount probe was replaced with a Kiel probe that included a slight bend in the placement of the Pitot tube.



The Kiel probe design angled the Pitot tube 10 degrees from the centerline of the aircraft. This design enabled more accurate air speed indication at high angles of attack.

When the Kiel probe was installed, it was not equipped with Pitot heat. (The Rosemount probe had included Pitot heat.) This change introduced two factors that increased the risk of icing on the Pitot tube: 1) the design of the Kiel probe is inherently more prone to icing and 2) the Kiel probe did not have heat.

Three documents were released in connection with the change-out of the Rosemount probe for the Kiel probe: a configuration change request, an engineering order, and a work order. The Mishap Investigation Board could not confirm that the configuration change had been circulated to the team members (4 of the 5 test pilots thought Pitot heat was operable on the Kiel probe). Furthermore, none of these documents mentioned placarding the cockpit Pitot heat switch as “Inoperative.”

The mishap investigation revealed that a temporary operating procedure (TOP) written to address the operation of the Kiel probe without heat was never reviewed, approved, or distributed. The lack of formal tracking or follow-up on this change meant most of the pilots and many team members were unaware of the absence of heat on the Pitot tube.

Inadequate Operational Controls/Intervention

In addition to the improper assumptions in the hazard analyses and the breakdown in configuration management processes, several other “safety nets” might have helped the X-31 operations team avoid disaster on the day of the accident. Since the hazard analyses had not identified the loss of signal from the Pitot tube as a critical failure, it was not included in the standard pre-flight brief of accepted risks. As the pilot and control room observed the sequence of events leading up to the crash, they were not

all aware of the severe consequences posed by this risk. Despite their hazard analyses, risk lists, safety procedures, and experiences, the team was unable to identify the data error and avoid the crash.

If the team had identified an FCS input problem, having a ready backup system might have changed the course of events. A reversionary flight mode could have been used to safely return the aircraft to the ground. By selecting a reversionary flight mode, the effects of erroneous air speed indication could have been removed in two minutes. However, the team did not regularly test the use of these reversionary systems. In those cases where the test pilot did switch to a reversionary mode, the switch was only made after discussion and consensus with the control room that it was the appropriate course of action. As a result, the pilot and the control room may have been apprehensive to select this mode without receiving indication to do so from the FCS.

The control room was configured to observe all critical systems and data indication on the X-31, and constant “hot mike” communication existed between the pilot and control room. The test flight also incorporated a chase plane that followed along to assist in observing the flight. In typical test flights, chase pilots are included in “hot mike” conversations and serve as an extra set of eyes to help maintain flight safety during tests and maneuvers.

The “hot mike” system in the chase plane had been producing a lot of static and was completely disabled for most of the test flights. The chase pilot was unable to assist in diagnosing the problem and had no indication that anything was wrong until the X-31 began to fly erratically. If he had been able to listen to the team’s communications, the chase pilot could have helped identify the air speed indication problem that eventually led to the crash.

RECOMMENDATIONS CALLED FOR A MORE ROBUST IMPLEMENTATION OF EXISTING PRACTICES

PROBLEM RESOLUTION

The Mishap Investigation Board made several recommendations for action that were required to be completed before the remaining X-31 aircraft could return to flight. These recommendations did not call for sweeping changes in safety processes and procedures, program personnel, or system design. Rather, they called for a more robust implementation of existing practices. It appears this was the primary failure at the X-31 program: a failure to rigorously execute existing procedures and practices to effectively reduce program risk.



The X-31 (top) with the F-18 chase plane (bottom).

LESSONS LEARNED FOR NASA

Hazards analyses and risk management processes are commonplace throughout NASA. The problem for the X-31 team was not whether they applied the right analytical methods and tools to the situation at hand, but whether they rigorously applied those analyses and properly interpreted the results. Failure to recognize the flight safety criticality of Pitot tube operability and an unfounded belief that backup flight modes and/or the FCS represented viable mitigations to loss of high fidelity Pitot tube air speed data are reminders of one globally applicable lesson: there is a need to aggressively test critical hardware/software systems in nominal and off-nominal operational regimes to flush out latent design defects and test assumptions concerning response and recovery.

Circumstances surrounding the crash of the X-31 shows how important it is for all project team members to fully understand and implement program processes and procedures. The X-31 team was recognized as a strong, highly capable team dedicated to quality. Even though they had accomplished a record number of successful test flights, they experienced difficulty in maintaining the level of rigor required to effectively understand and manage program risks. Minor lapses in completeness and attention to detail may not, by themselves, result in a serious failure. However, the convergence of multiple (small) failures can contribute to a chain of events that result in catastrophe – such as the crash of the X-31.

References:

“Ice In or On Static System Cause of X-31 Crash,” News Release: 95-33, NASA Dryden Flight Research Center, <http://www.nasa.gov/centers/dryden/news/NewsReleases/1995/95-33.html>, November 7, 1995.

“NASA 584 X-31 Mishap Investigation Report, Date of Mishap: January 19, 1995,” NASA Dryden Flight Research Center, August 18, 1995.

“NASA F-18 Retires to JetHawks Stadium,” *The Dryden X-Press*, <http://www.dfrc.nasa.gov/Newsroom/X-Press/1997/xp-97-04.html>, February 21, 1997.

Questions for Discussion

- To what degree has off-nominal testing been conducted to ensure operability?
- Have there been any process escapes in your project/program similar to those described as the underlying causes of the X-31 crash? If so, how were they identified and resolved?
- What other critical failures are you aware of that were not previously reported during safety in-briefs and proved later to be disastrous? How could they have been prevented?
- What assumptions have been made concerning backup, recovery, and functional redundancy systems within your program/project?
- What criteria are taken into consideration when a risk is assigned a level of criticality? How often are these criteria reviewed and assessed for changes?

“Pitot Tube,” Wikipedia, the Free Encyclopedia.

http://en.wikipedia.org/wiki/Pitot_tube.

Pitot Tube, [Online Image] Available,

<http://www.nasa.gov/centers/dryden/news/FactSheets/FS-009-DFRC.html>, May 15, 2006.

“Thrust Vectoring,” Wikipedia, the Free Encyclopedia,

http://en.wikipedia.org/wiki/Thrust_vectoring.

“X-31, Breaking the Chain,” *Lessons Learned*, DVD, Dryden Flight Research Center.

“X-31 Enhanced Fighter Maneuverability Demonstrator,” Fact Sheets, Dryden Flight Research Center,

<http://www.nasa.gov/centers/dryden/news/FactSheets/FS-009-DFRC.html>.

X-31 Kiel Probe Side View, X-31 in Flight, X-31 at High Angle of Attack, X-31 in Flight with F-18 Chase, [Online Image] Available <http://www.dfrc.nasa.gov/Gallery/Photo/X-31/index.html>, March 27, 1998.

SYSTEM FAILURE CASE STUDIES

A product of the NASA Safety Center

Executive Editor: Steve Wander

stephen.m.wander@nasa.gov

This is an internal NASA safety awareness training document based on information available in the public domain. The findings, proximate causes, and contributing factors identified in this case study do not necessarily represent those of the Agency. Sections of this case study were derived from multiple sources listed under References. Any misrepresentation or improper use of source material is unintentional.

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

