National Aeronautics and Space Administration

SYSTEM FAILURE CASE STUDIES

JANUARY 2012 VOLUME 6 ISSUE 1

Safe Anyway

On September 2, 2006, Nimrod MR2 XV230, a reconnaissance aircraft in the Royal Air Force, flew over Southern Afghanistan in support of a NATO-led offensive against the Taliban. Several hours after takeoff, the 14-member crew paused operations for in-flight refueling, then prepared to resume its mission. But not long after the Nimrod disengaged from the Tristar airborne tanker, two nearly simultaneous warnings alerted the crew to fire and smoke in the aircraft's bomb and elevator bays. The pilots declared a Mayday and initiated an emergency landing, but the fire that raged below the cabin gave them no chance to survive. Minutes later, the aircraft depressurized, and a Harrier G7 pilot nearby saw the aircraft explode in mid-descent. All 14 servicemen lost their lives in the disaster.

What Happened

Fire, Decompression, and Explosion

On September 2, 2006, coalition forces mounted an offensive to clear the Taliban from the city of Panjwayi, Afghanistan. Manned by a 14-member crew, Nimrod MR2 XV230 flew over hostile territory in support of the operation, and paused for a 10-minute rendezvous with a Tristar in-flight refueling aircraft. Minutes after Nimrod disengaged from the tanker, alarms alerted the crew to fire in the bomb bay, located beneath the cabin floor. Smoke began seeping into the cabin. Less than a minute later, the aircraft depressurized, forcing the crew to don oxygen masks. As the captain declared a Mayday and began emergency landing procedures, a Harrier G7 pilot, flying several thousand feet above XV230, reported flames trailing from the starboard wing roots and aft fuselage. Nimrod crewmembers corroborated the report, describing fire emanating from the starboard engines and the aileron bay. This was the last transmission. Moments later, the aircraft exploded at an altitude of approximately 3000 feet, and debris plummeted onto the terrain below. No one on board survived.

The hostile area in which the wreckage landed made it difficult for combat and rescue teams to recover the victims and flight recorders, but they did so within 21 hours of the crash. Hostile forces then converged upon the area and removed most of the debris. How could an aircraft that had seemed to operate safely for 36 years simply explode inflight?

Figure 1: Nimrod in flight. Paired engines can be seen embedded in the wings, close to where the wings connect to the fuselage.

Background: An Airframe and Air Force Evolves

From First Passenger Jet to Cold Warrior

Nimrod XV230 entered service in October 1969 as the first of 38 new maritime strike/reconnaissance jets built for the Royal Air Force (RAF). Hawker Siddeley, now a part of British Aerospace (BAE Systems), modified the design of the De Havilland Comet—the first production commercial jetliner—for the job. New, more efficient turbofan engines replaced turbojets, and to increase mission endurance, engines were cross connected via internal ducting to

British Reconnaissance Aircraft Crashes over Afghanistan, 14 Dead.

Proximate Causes:

- Fuel in dry bay ignites after exposure to pressurized hot air duct surface
- Fire causes fuel in tanks to boil; increased pressure from boiling causes tanks to explode

Underlying Issues:

- Design flaws
- Improperly constructed Safety Case
- Organizational disarray

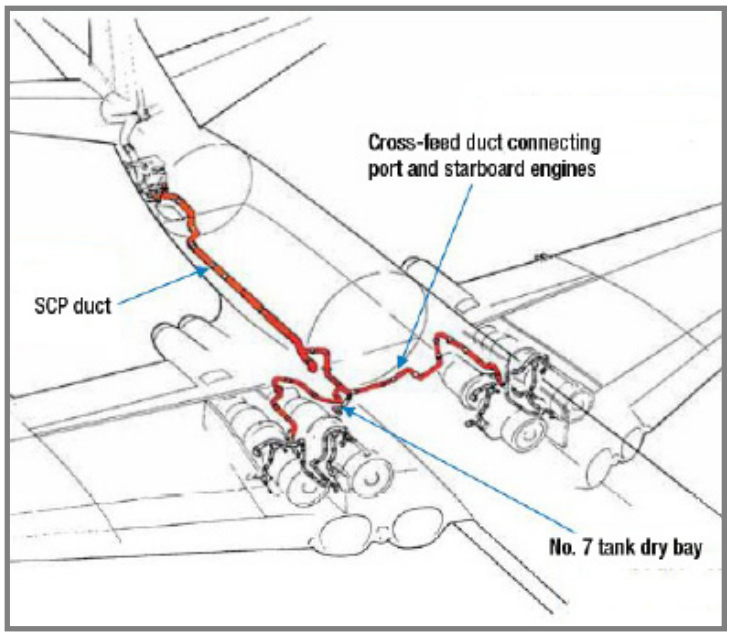

Figure 2: Nimrod's original design placed the cross-feed duct near the bottom of the No. 7 tank dry bay. After Nimrod was modified to include a supplemental conditioning pack, designers added the SCP duct as a branch from the original cross feed duct.

allow in-flight shutdown and restart using bleed air from operating engines. It would become routine to shut down two of the aircraft's four engines over the North Atlantic while loitering on-station in search of submarines over the next three decades (Figures 1 and 2). Still more design changes were needed to satisfy unprecedented high-altitude range and low-altitude endurance mission demands.

Four fuel tanks were added, two of which—called No. 7 port and No. 7 starboard tanks—lived near the inboard engines, next to that hot bleed air ducting at the wing root. The cross-feed duct passed through part of the bomb bay, an area called the No. 7 tank dry bay.

In 1979, Nimrod XV230 underwent a major fleet upgrade adding radars and other sensors. To cool the powerful new gear, designers added a supplementary conditioning pack (SCP) in the aircraft's tail region. The pack used engine bleed air branched off of the original cross-feed duct (Figure 2). Temperatures in the duct were hot: as much as 400°C.

Then, during the Falklands Conflict in 1982, an urgent requirement to add Air-to-Air Refueling (AAR) capability to eight Nimrods drove engineers to design and modify the XV230 and seven others with in-flight refueling probes in a scant eighteen days. Refuel supply tubing routed into the bomb bay; new relief valves would dump fuel into the atmosphere if refueling pressure exceeded safe limits.

Budget Cuts and the Safety Case

In 1998, the British Ministry of Defence (MOD) published its latest Defence Strategy Review. This policy document would mark a turning point for the safety culture of the RAF and other organizations. With manpower slashed by 7,000 and six major weapons programs reduced (including the Nimrod MR2), a shift toward rewarding cost-effective management over thorough, safety-first leadership commenced, later to be discovered by investigators of multiple mishaps. Lessons learned from previous disasters would fail to be applied despite force of law.

For example, in 2002, new military regulations required the completion of a "safety case" for its aging aircraft (over 30 years in service) to include the Nimrod fleet. Springing from the 1988 *Piper Alpha* offshore oilrig explosion that killed 167 men, a safety case would make a "structured argument, supported by a body of evidence that provides a compelling, comprehensible, and valid case that a system is safe for a given application in a given operating environment." Consultants or company employees prepare these cases, which require personnel to mitigate risks until the risks can be considered "as low as reasonably possible" (ALARP).

In compliance with this directive, the MOD contracted BAE Systems to formulate the case with help from an internally assembled Nimrod Integrated Project Team (Nimrod IPT). Defense analyst company QinetiQ would assist efforts as an independent advisor. Both companies with RAF oversight conducted a three phase approach (zonal inspection, hazard analysis, and hazard disposition) over almost four years, expending over £400,000 to complete the safety case--and failed to find the latent causes of XV230's loss.

Proximate Cause of Nimrod XV230 Explosion

Although enemy forces prevented the RAF from recovering most of XV230's wreckage, the Board of Inquiry (BOI) obtained enough material to determine that XV230's tragic end was the culmination of an event chain that began when jet fuel accumulated in the No. 7 dry bay. After conducting an extensive analysis, the BOI concluded that fuel arrived in the dry bay in one of two ways: A) it ejected from the No.1 tank's blow-off valve during AAR, tracked back along the fuselage, and entered the dry bay through ports or intakes; or B) fuel couplings in the dry bay failed, allowing fuel to escape from conduits in the dry bay and accumulate at the base of the compartment. Somehow, this fuel contacted the extremely hot SCP duct and self-ignited. Without fire detection or suppression systems in the dry bay, the fire spread to the bomb and aileron bays before alarms alerted the crew to its existence.

Heat from the initial fire caused hydraulic fluid in the aileron bay to reach auto-ignition temperature and a secondary fire ensued. Before long, the aileron bay wall gave way and the aircraft depressurized. Even as damaged fuel lines fed the flames, increased airflow from the depressurization intensified the inferno. By this time, the pilots would have lost any ability to control the aircraft; the fire ravaged pulleys and cables upon which pilot inputs depended. Only minutes passed before fuel inside the tanks began to boil. As a result, pressure inside the tanks began rising, and finally a boiling liquid vapor expansion explosion tore the aircraft apart.

Underlying Issues

Design Flaws

Three major design flaws played crucial roles in the Nimrod's down-fall. Each was introduced more than a decade prior to the accident, and each defied design regulation in force at the time of its installation. These included the placement of the original cross-feed duct, the addition of the SCP duct, and the addition of the blow-off valves for in-flight refueling.

The cross-feed duct rested near the bottom of the No. 7 dry bay, beneath a labyrinth of fuel lines and other conduits. This design contradicted good engineering practice because it placed a potential ignition source (the extremely hot duct surface) in the vicinity of a

potential fuel source (possible fuel leaks from adjacent fuel lines) without designating the area as a fire zone and providing fire detection and suppression systems (Figure 3). Defense Standard 00-970 (at the time known as AvP970) states that configurations containing both potential ignition sources and potential fuel sources must be designated as fire zones, and that fuel lines must be placed as far from heat sources as possible.

Designers selected Refrasil insulation to cover the cross-feed duct and prevent it's extremely hot surface from damaging nearby structures. Refrasil is a fluid-impermeable substance which also protected the duct from contacting fuel leaking from above. The BOI found that at the time of the accident, the cross-feed duct was insufficiently protected from leaking fluids. In some sections, the Refrasil had deteriorated, in other sections, the duct was left un-insulated, and in still other sections, absorbent muffs (not made of Refrasil) could trap fuel against the duct's hot surface where it could self-ignite (Figure 4).
Damage to the cross-feed duct could compromise fuel couplings

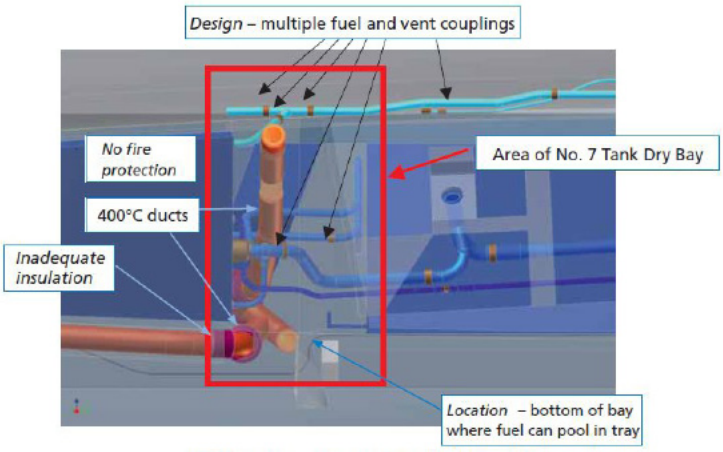

Figure 3: The red box indicates the area of the No. 7 tank dry bay. Many fuel lines occupied this space, and their proximity to the cross-feed/SCP duct should have caused the dry bay to be designated as a fire zone.

through hot air exposure. Fuel could then leak and collect at the base of the dry bay. The 1979 addition of the SCP duct exacerbated these risks, which the original cross-feed duct already posed. The SCP duct spanned the entire length of the No. 7 dry bay, increasing the area where an accident could occur. Designers were cognizant of the extreme temperatures to which the SCP duct surface could rise, so they encased it in Refrasil. Nevertheless, in 2004, hot air damaged several nearby fuel couplings. No one heeded this warning signal.

Not long after the Nimrod's AAR capabilities were installed in 1982, engineers discovered the location on the No. 5 tank was such that during flight, fuel exiting the No. 5 blow off valve could enter a port engine intake. Because this violated Defense Standard 00-970, which stated that blow-off valves could not be located where fuel discharge could pose a fire hazard, this valve was disabled. However, a similar risk existed for other blow-off valves, especially the valve associated with the No. 1 tank. Analysts suspected that fuel exiting the No. 1 tank's blow-off valve could track back along the fuselage and re-enter the aircraft through various ports and vent intakes. Recommendations to investigate this risk more comprehensively were shelved, and no further analysis was ever conducted.

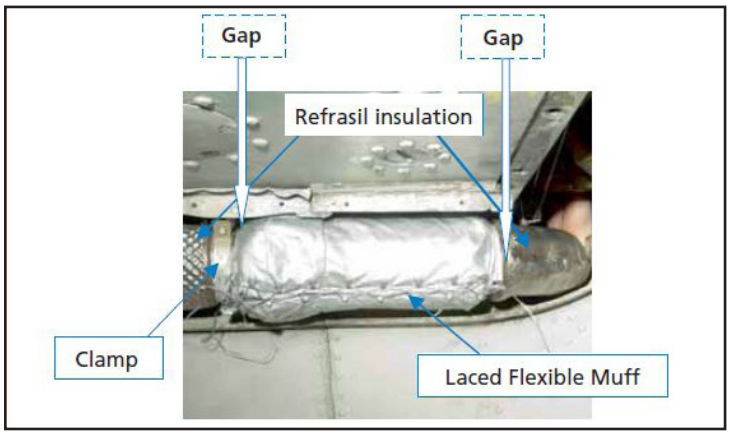

Figure 4: Section of cross-feed duct showing discontinuity of Refrasil insulation. Flexible muffs were used in place of Refrasil in several places. Note gaps between insulation types.

Improperly Constructed Safety Case

After the accident, Charles Haddon-Cave, Queen's Counsel, conducted the Nimrod Review. This study analyzed the BOI report and explored possible culpability for the disaster. According to Mr. Haddon-Cave, "The Nimrod Safety Case represented the best opportunity to capture the serious design flaws in the Nimrod which had lain dormant for years. If the Nimrod Safety Case had been drawn up with proper skill, care, and attention, the catastrophic fire risks to the Nimrod MR2 fleet presented by the cross-feed/SCP duct and the AAR modification would have been identified and dealt with, and the loss of XV230 in 2006 would have been avoided." The Nimrod Review concluded that those who formulated Nimrod's Safety Case suffered from a wide-spread assumption that the Nimrod was "safe anyway." They lost sight of the Safety Case's primary goals and reduced its construction to a mere formality. As a consequence, project planning suffered, standards slipped, and 14 people paid the ultimate price.

The Nimrod Review found the Safety Case project plagued with poorly estimated schedules and miscalculated costs. Fulfilling deadlines took precedence over satisfying requirements, and many identified hazards, including the ones that played primary roles in the disaster (e.g. deteriorating insulation) were left "open" and "unclassified." Of 105 identified hazards, 43 were left "open" and 32 were left "unclassified." Recommendations for many of these hazards stated only that "Further analytical techniques are required."

Some hazards were incorrectly assessed. The blow-off valves—which should have been identified as a fuel source and were not—comprise one such example. Similarly, the Nimrod Safety Case presented an opportunity to identify the No. 7 dry bay as a fire zone, but this hazard was also missed. Many omissions and missed assessments occurred during Phase One (Hazard Assessment) of the safety case--the foundation upon which all other phases would depend. These Phase One errors set the stage for the safety case's ultimate failure.

Organizational Disarray

During the years between 1998 and 2006, the MOD experienced significant changes in management structure. Over five years, the Ministry increased outsourcing to industry and reduced its budget by 20%. This upheaval diluted the airworthiness regime and shifted RAF focus from system safety to cost savings. A former senior

RAF officer told the Nimrod Review, "There was no doubt that the culture at the time had switched. In the days of Sir Colin Terry, you had to be on top of airworthiness. By 2004, you had to be on top of your budget, if you wanted to get ahead." In 1998, a Nimrod Airworthiness Review Team warned that increased demands and reduced resources would threaten safety standards. The Nimrod Board of Inquiry concluded that MOD management failed to safeguard the Nimrod fleet during the transitional period. Leadership did not enforce safety measures such as monitoring leak trends and analyzing historical duct failures. As aging aircraft, the Nimrod fleet required more attention as time marched forward; instead it received fewer resources and decreased vigilance. Eventually, the Nimrod Safety Case, riddled with errors and fatal flaws, glossed over glaring problems while propagating an illusion of airworthiness.

Aftermath

After the loss of XV230, an influx of intense scrutiny regarding fuel leak potential and cross-feed/SCP duct failure took place. Fuel system inspections—which were now conducted with tanks and lines under pressure—took place more frequently, and the RAF saw a subsequent rise in the number of reported fuel leaks. In addition, AAR required an express request from the force commander, and the procedure was restricted to flights whose operations could not take place without it. In November of 2007, Nimrod XV235 experienced a fuel leak in the bomb bay during an AAR procedure. Attempts to reproduce the leak after an emergency landing failed, and officials concluded that pre-flight system checks could not reliably predict leaks. AAR then ceased entirely.

The BOI released its final report, which contained 33 formal recommendations for the Nimrod fleet, in December of 2007. The RAF accepted 28 recommendations, fulfilled 3 through alternative means, and concluded that the remaining 2 were impractical given the remaining life of the Nimrod. In 2010, Nimrod performed its final operational flight, and the fleet was retired in March of that year. Its replacement, MRA4, had been scheduled to deploy in 2012, but cost overruns and budget cuts led officials to cancel the procurement.

For Future NASA Missions

Nimrod served the RAF for three decades, participated in every major conflict that occurred during those years, and experienced only two accidents prior to the loss of XV230. The apparent safety of the Nimrod lulled many, including BAE Systems, the Nimrod IPT, and QinetiQ, into a false sense of security. Seemingly, everyone assumed Nimrod was "safe anyway." But as Mr. Haddon-Cave points out in the Nimrod Review, "the non-occurrence of system accidents or incidents is no guarantee of a safe system." Unfortunately, history has seen many organizations, including NASA, fall victim to complacency and misplaced confidence. The Nimrod Review cited many parallels between the loss of XV230 and the loss of space shuttle Columbia. One was the "torrent of changes" and "organizational turmoil" that the MOD and NASA both faced just prior to the XV230 and Columbia disasters.

Since Columbia, NASA has seen the Constellation program cancelled, space flight privatized, and the SLS project announced. As a consequence, new managers (and new policies) have stepped in. New business units have formed. Divisions created for Constellation have been dissolved; new ones have taken their place. The Agency faces decisions on allocation of limited resources. Past experience has shown how major changes such as these can adversely impact organizational cultures. Change can shift organizational focus from safety to finance. Change can dilute safeguards. Change can compromise standards.

Questions for Discussion

- **What are some of the positive and negative ways that your team has been affected by recent organizational changes?**
- **How does your team identify and manage distractions that could compromise safety?**
- **Are there projects under your purview which your team assumes to be safe systems? Do you participate in any safeguards that have been reduced to "checkbox" exercises?**

But change is inevitable, and diligence can prevent us from re-living hard lessons from the past. We must remember that causal factors often run deeper than miscalculations or technical malfunctions. Avoiding those pitfalls (i.e., avoiding endemic organizational issues) means avoiding a mindset that past success guarantees safe systems. It means breaking down communication barriers. It means propagating an engaged culture. It means committing to "prove it's safe" when embarking on new designs, or reassessing aging (but evolving) designs. This is not the last time that NASA will weather the winds of change. NASA must sustain sound system safety practices through this time of change.

References

Haddon-Cave, Charles. The Nimrod Review: An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006. House of Commons Stationary Office: London, 2009.

"Nimrod officially retires after three decades." Accessed 22 Sept 2011. The Telegraph: 26 Mar 2010. < http://goo.gl/UdNJ4>

"Q & A: Nimrod MR2 Explosion." Channel4News. December 2007. < http://goo.gl/nRebR>

Rozen, Oren. "Nimrod Waddington 2005." Online Image. 2 July 2005. Accessed 23 Sept 2010. Wikimedia Commons. < http://goo.gl/iy2Pg>.

Steinzor, Rena. Lessons from the North Sea: Should "Safety Cases" Come to America?, 38 B.C. Envtl. Aff. L. Rev. 417 (2011), <http://goo.gl/E9IrC0>

SYSTEM FAILURE CASE STUDIES

NSC

NASA SAFETY CENTER

Responsible NASA Official: Steve Lilley Developed by: ARES Corporation

steve.k.lilley@nasa.gov

Thanks to [name] for [name] insightful peer review.