National Aeronautics and Space Administration

NASA SAFETY CENTER

SYSTEM FAILURE CASE STUDY

May 2013 Volume 7 Issue 4

The Case for Safety

The North Sea Piper Alpha Disaster

July 6, 1988, Piper Oilfield, North Sea: As shifts changed and the night crew aboard Piper Alpha assumed duties for the evening, one of the platform's two condensate pumps failed. The crew worked to resolve the issue before platform production was affected. But unknown to the night shift, the failure occurred only hours after a critical pressure safety valve had just been removed from the other condensate pump system and was temporarily replaced with a hand-tightened blind flange. As the night crew turned on the alternate condensate pump system, the blind flange failed under the high pressure, resulting in a chain reaction of explosions and failures across Piper Alpha that killed 167 workers in the world's deadliest offshore oil industry disaster.

PROXIMATE CAUSE

- Simultaneous maintenance work on the pump and safety valve resulted in a condensate leak.

UNDERLYING ISSUES

- Defeated Design
- Negligent Culture

AFTERMATH

- The Cullen Inquiry resulted in 106 recommendations for changes to North Sea safety procedures—all of which were accepted by the industry.
- The Health and Safety Executive was to bear responsibility for North Sea safety moving forward, replacing the Department of Energy's obligation, based on a conflict of interest for one organization to oversee both production and safety.

Background

Piper Alpha

Constructed for oil collection by McDermott Engineering and operated by Occidental Group, Piper Alpha was located 120 miles northeast of Aberdeen, Scotland. It began exporting oil from the Piper Oilfield (discovered in 1973) to the Flotta Terminal on the Orkney Isles in 1976. Modular in design, the four main operating areas of the platform were separated by firewalls designed to withstand oil fires, and arranged so that hazardous operating areas were located far from personnel and command areas. Piper Alpha was equipped with both diesel and electric seawater pumps to supply its automatic firefighting system.

Gas Conversion

To extract oil from beneath the ocean floor, wells initially extract a combination of oil, natural gas, and salt-water brine that is pumped to the platform. Once there, gas and water are separated from the oil in production separators. Gas is separated off and cooled to remove the gas condensate liquid. Condensate is pumped back into the oil and the mixture travels to the shore refinery. Excess gas is then flared (burned) off.

Flaring was a common practice until 1978, when United Kingdom (UK) gas conservation policy requirements called for Occidental to modify the platform to process the gas for production. After modification, Piper Alpha processed gas and sent it to the MCP-01 compression platform. Piper Alpha additionally served as a hub, connecting the gas lines of two other Piper field platforms, Claymore and Tartan, to MCP-01. Totaled, Piper Alpha was connected to four different transport risers.

Figure 1. Piper Alpha before the fire. Source: BBC.

Although compliant with UK gas conservation policy, the modifications to Piper Alpha broke from the safe design concept that separated hazardous and sensitive areas of the platforms. A hazardous Gas Compression Module (GCM) was installed next to the platform control room. This new "Phase 2" operating mode, with the active GCM, was maintained as the normal operating state until 1980.

Throughout the late 1980s, major maintenance projects were underway, including a change-out of the GCM. Occidental decided to operate in Phase 1 mode during this work instead of halting production entirely (as originally planned), claiming that established procedures would be adequate during renovation. Piper Alpha continued to export just under 120,000 barrels of oil and approximately 33 million standard cubic feet of gas per day.

What Happened

On July 6, a worker performing routine maintenance removed the pressure safety valve (used to regulate pressure in case of an overpressure) from Pump A—one of two Piper Alpha condensate pumps that moved condensate down the pipeline to the coast. Beyond the routine maintenance, a 2-week long overhaul had been pending for Pump A, but the overhaul had not yet begun. The worker used a blind flange (round metal plate) to seal off the open pipe. Since the maintenance could not be completed before the 6 p.m. shift change, the worker left the hand-tightened flange in place, opting to complete a permit stating that Pump A was not ready for operation and must not be activated.

At 9:45 p.m., the second shift was faced with a hydrate (ice-like, crystalline structures of water and gas molecules that form under certain pressure and temperature conditions) buildup that blocked the gas compression system. The blockage resulted in failure of Pump B, which would halt all offshore production on the Piper Oilfield unless it (or Pump A) could be restarted. Workers combed through maintenance records to see if Pump A was clear for activation. Although the permit for the overhaul was found, the permit pertaining to the routine maintenance and missing safety valve was not: the worker who removed the safety valve placed that permit in a box near the valve, as the location-based permit system had outlined. Additionally, the missing valve-cum-blind flange was located behind other equipment several feet above the rig's deck, making visual identification of the safety issue highly improbable.

Workers, believing Pump A to be safe for use, activated it at 9:55 p.m. The high-pressure gas leaking through the hand-tightened, failing blind flange whistled and triggered six alarms before igniting and exploding moments later. Firewalls designed to withstand burning oil, crumbled under the overpressure from the detonating gas. The emergency stop system was activated and incoming oil and gas sea lines were sealed. Under Piper Alpha's original oil production design, the emergency action would have isolated the individual units on the platform and contained the fire, but fire spread through broken firewalls to the damaged separation module (where gas and water were separated from harvested oil), igniting a small condensate pipe that was ruptured by the initial explosion. Occidental issued no orders to either Tartan or Claymore to shut down and operators believed they did not have authority to stop export from Piper Alpha.

At 10:04 p.m., platform workers evacuated the control room, leaving the platform with no way to manage the disaster. From the control room, firefighting systems were placed under manual control that evening according to procedure established by the rig manager. That deactivated automatic firefighting water pumps when divers were working in the water, as they had been earlier that day. No platform-wide emergency communications or evacuation orders were given. The crew, unable to approach the lifeboat stations because of the flames, gathered in the fireproof living quarters and waited for instructions.

Tartan and Claymore's continued production forced continuous

Figure 2. The smoke reached hundreds of feet above Piper Alpha, preventing rescue helicopters from approaching. Source: Technologism.net.

fuel into the blaze, preventing the fire from burning out. Smoke filled the living quarters. Numerous valiant but unsuccessful attempts to reach the water pumping machinery were made. At 10:20 p.m., Tartan's gas line burst—feeding 16.5 to 33 tons of gas per second into Piper Alpha, which ignited immediately.

Helicopter rescue was impossible because of the wind, smoke, and flames. Rig personnel began jumping from various levels of the 175-foot platform. The *Tharos*, a firefighting vessel, attempted to draw alongside Piper Alpha and fight the inferno at 10:30 p.m., but was restricted because its water cannons possessed enough pressure to kill platform workers if hit directly. Twenty minutes later, the *Tharos* had to leave the platform after the second gas line from MCP-01 ruptured, feeding more gas into the fire. The flame jets reached hundreds of feet into the air and temperatures rose so high that areas of the steel rig and portions of the *Tharos* began melting. The explosion killed two rescue crewmen and six Piper Alpha survivors who jumped to into the sea. Remaining crew were left trapped in the blazing crew quarters. Claymore shut down after this second major explosion; Tartan platform management was given orders not to stop production, given the consequential cost to Occidental.

At 11:20 p.m., the scorched and melting utilities module and crew quarters slid into the sea. The rest of the platform followed piece by piece until 12:45 a.m., July 7. The oil wells module was the only remaining section left above the waves. Of the 226 platform personnel, 61 survived. 167 Piper Alpha crewmen and rescue personnel were lost.

Proximate Cause

In November 1988, a public inquiry, led by Lord William Cullen, was initiated to investigate and establish the cause of the catastrophe, reaching a conclusion almost exactly 2 years later in November of 1990. The Cullen Inquiry concluded that the simultaneous maintenance work on the pump and safety valve resulted in the condensate leak.

Underlying Issues

Defeated Design

Piper Alpha's inadequate permit and lockout/tagout system resulted in gaps in multiple levels of safety. While second shift engineers earnestly believed that all documents were accounted for before beginning Pump A start-up, a decentralized system inhibited the sharing of critical information. A lack of informal "between shift" talks compounded lax communication issues. The reliance on individual safety practices in lieu of a strong system safety culture allowed errors to find holes in the layers of controls.

No backup procedures existed in case of loss of the platform control room and organization disintegrated. The Piper Alpha refit performed in the 1980s was not paralleled with revised safety measures, even while the expansion into gas production defeated firewalls made to oil fire specification.

Figure 3. The remaining oil wells module continued to burn for weeks until famed firefighter, Red Adair, and his team extinguished the remains. Source: BBC.

Negligent Culture

Although Piper Alpha was equipped with automated fire-fighting equipment, a procedure established by platform management had deactivated automation of the system when divers were working in the water, thus preventing them from being ingested through automated water pump caged intakes. It was customary for divers to work up to 12 hours a day during summer months in the North Sea, but divers did not see significant risk unless they were working closer than 10 to15 feet from any of the intakes. Earlier audit recommendations suggested that pumps remain in automatic mode if divers were not working in the vicinity of the intakes, but this recommendation was never implemented.

Multiple 16- and 18-inch-diameter gas pipelines were connected to Piper Alpha. The length and diameter of these pipelines fell under scrutiny of a study performed 2 years earlier by Occidental management. The study warned that it would take several hours to reduce the pipelines' pressure in an emergency, and that it would not be possible to fight a fire while fuel was forced though them. Management admitted that the devastation of the pipelines would end in disaster, but Claymore and Tartan production was not halted with the first emergency call during the Piper Alpha fire.

Aftermath

Because of damages costing almost $3.4 billion, the Piper Alpha disaster was the largest man-made disaster at the time and continues to be the worst offshore oil disaster in terms of life lost and industry impact. Although the Cullen Inquiry found Occidental guilty of inadequate maintenance and safety procedures, no criminal charges were brought against the company.

The inquiry resulted in 106 recommendations for changes to North Sea safety procedures—all 106 were accepted by the industry. The most significant recommendation was for the Health and Safety Executive (the UK's body responsible for encouragement, regulation, and enforcement of workplace health, safety and welfare, and occupational safety research) to bear responsibility for North Sea safety, replacing the UK's Department of Energy's obligation. This was based on a conflict of interest for one organization to oversee both production and safety.

Of note, the Piper Alpha disaster was the catalyst for the UK's development of "Safety Case" requirements. According to the UK Defence Standard 00-56 Issue 4, "A Safety Case is 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 environment." An evidence-driven approach is contrasted to a prescriptive safety approach common to safety methodology typically used in the United States. Such prescriptive processes are assumed to ensure safety and do not necessarily require corresponding evidence to validate a safety measure's effectiveness at ensuring that risks are kept As Low As Reasonably Practicable (ALARP).

As noted in the Health and Safety Executive's Key Programme 3 (KP3) report—a 3-year investigation into the safety and integrity of over 100 offshore installations—North Sea production facilities are beginning to approach the end of intended use lifespans and legacy issues continue to be revealed. Legacy issues correlate to lack of investment in infrastructure when oil prices declined during the 1990s.

Relevance to NASA

After the Apollo 1 capsule fire, NASA was witness to a flurry of advancements in its reporting systems—most notably the Agency-wide centralization of all reports and status changes to the various systems of the Apollo capsule. This centralization combatted "structural secrecy," a phrase referring to a system or organization that prevents critical information from reaching those who need it. Furthermore, NASA commissioned the development of policies and procedures that became models for civilian space flight safety activities. Many of the same engineers and companies that had established formal system safety defense programs also were involved in space programs, and the systems engineering and system safety technology and management activities were transferred to space programs.

The reporting systems triggered by the Apollo disaster eventually fell to the wayside. Production was placed ahead of scrutinizing system safety concerns, a practice that culminated in hesitation to report O-ring failures that later played into the Challenger disaster. Without new development in manned spaceflight, many effective NASA system safety practices had been replaced by reliability engineering and other approaches to safety used by industries with very different requirements.

Fortunately, the UK's movement toward Safety Cases after the Piper Alpha disaster finds a parallel in NASA system safety engineering and methodology as Risk-Informed Safety Cases (RISC). The RISC is developed beginning early in the systems development lifecycle and reviewed at each major milestone. Then it plays a key role in NASA's acceptance and possibly certification (if applicable) of the newly developed system. It remains useful throughout the lifecycle, including the operational phase. Beyond using evidential assurance that a system is safe, system safety methodology seeks out hazards and flaws that may compromise a system down the line, assuring safety at any given moment within operation context. More information on System Safety at NASA can be found in the NASA System Safety Handbook.

The Piper Alpha disaster, one of the earlier offshore platform disasters, continues to serve as an industry example of what happens when production, schedule, and cost come before investments in comprehensive system safety. NASA must remember its shortfalls in parallel and remain vigilant in system safety practices.

References

Key Programme 3: Asset Integrity. Health and Safety Executive, Hazardous Installations Directorate. July 2009.

Incidents: Piper Alpha. http://www.stb07.com/incidents/piper-alpha-fire-explosion.html Accessed January 9, 2013.

Leveson, Nancy. "The Use of Safety Cases in Certification and Regulation." *Journal of System Safety*, Nov. 2011.

NASA System Safety Handbook, Vol. 1, System Safety Framework and Concepts for Implementation. NASA/SP-20120-580, Version 1.0. November 2011.

Piper Alpha. http://www.oilrigdisasters.co.uk/ Accessed January 9, 2013.

The Hon. Lord Cullen, The Public Inquiry into the Piper Alpha Disaster. The Department of Energy. Vol 1-2. November 1990.

Twenty Years On: Piper Alpha's Legacy. July 23, 2008. http://www.lloyds.com/News-and-Insight/News-and-Features/Archive/2008/07/Twenty_years_on_Piper_Alphas_legacy_23072008 Accessed March 4, 2013.

UK Defence Standard 00-56 Issue 4 http://www.dstan.mod.uk/standards/defstans/00/056/02000400.pdf

SYSTEM FAILURE CASE STUDY

NSC

NASA SAFETY CENTER

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