National Aeronautics and Space Administration

System Failure Case Studies

OCTOBER 2008 Volume 2 Issue 8

THAT SINKING FEELING

On March 20, 2001, the largest offshore oil production platform in the world sank to the bottom of the ocean about 150 kilometers off the coast of Brazil. A series of explosions claimed the lives of 11 crew members and crippled one of the four main support columns, which resulted in the massive flooding of Petrobras Platform 36 through an improbable but devastating chain of events. Approximately 1,200 m^3 of diesel oil and 300 m^3 of oil spilled into the Atlantic Ocean's Campos Basin, and the $496 million rig was declared a total loss.

BACKGROUND

The Petrobras Platform 36 (P-36) oil rig was originally built in 1994 as a drilling platform but was later converted to a deep-water semi-submersible production platform to service a different offshore oil field than initially intended. Modifications for the conversion increased the deck load and required the addition of stability boxes to the two pontoons and four columns that supported the rig. As a semi-submersible platform, P-36 was supported solely by buoyancy.

In May 2000, the converted oil rig commenced operations in the Roncador Field of the Campos Basin, a site managed by the Brazilian state-owned oil company, Petroleo Brasilerio or Petrobras. For safety purposes and pressure-relief, production platforms contain emergency drain tanks (EDTs) for storage of fluids that have become trapped or under excessive pressure in the production pipes. EDTs are usually located on the bottom deck of an oil rig, but in this case they were installed inside of the two aft (rear) support columns to save space and money as a part of "an aggressive and innovative program of cost cutting on P-36 production facilities," according to Petrobras executives. Petrobras extolled that "the project successfully rejected the established constricting and negative influences of prescriptive engineering, onerous quality requirements, and outdated concepts of inspection and client control" and that the "elimination of these unnecessary straitjackets" was delivering superior financial performance. However, there was no mention of any analyses performed to determine the effect of these innovations on safety margins or overall safety.

Figure 1: Petrobras P-36 sinks into the Atlantic Ocean.

Since 1999, Petrobras had been increasing oil production by double-digit percentages in efforts to capitalize on high petroleum prices and strong demand. At the same time, the company's environmental and safety record experienced growing scrutiny from the media. According to the Sole Petroleum Workers Federation (FUP), from January 2000 up to the P-36 accident, the oil workers' unions had recorded 95 significant accidents within Petrobras units, of which 18 were fatal.

In March 2001, a series of explosions sank Petrobras Platform 36.

Proximate Cause:

- Leakage of volatile fluids burst a shut down emergency drain tank and set off a violent chain of events

Underlying Issues:

- A corporate focus on cost-cutting over safety
- Poor design of individual parts with regards to a system safety context
- Component failure without sufficient backups
- Lack of training and communication

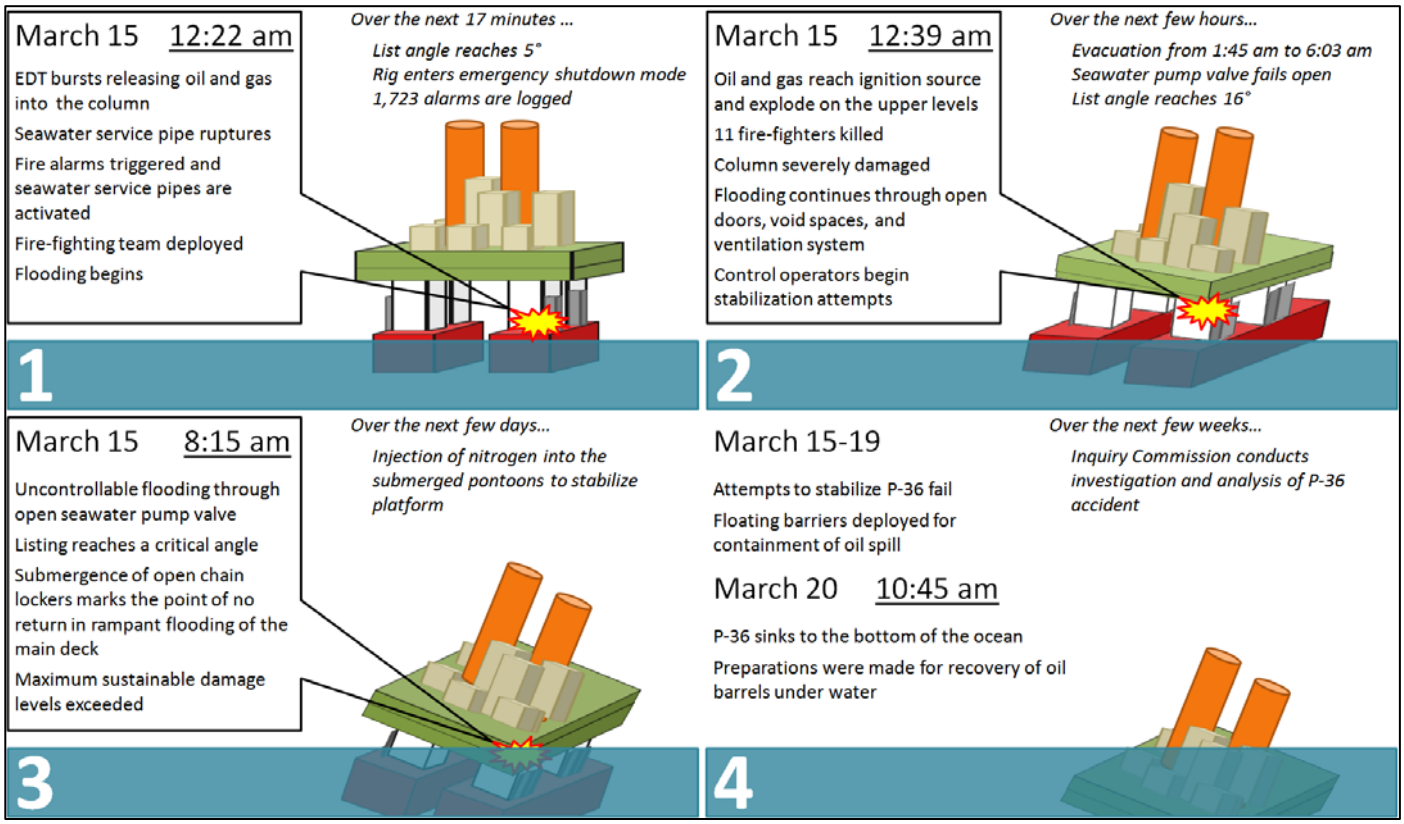

Figure 2: Sequence of events that culminated with the sinking of the world's largest oil rig, P-36.

What Happened?

EDT Rupture

Since February 2001, the starboard (right-side) EDT had been shut down and isolated from the rest of the system for repairs, leaving only the port (left-side) EDT for operations. But on March 14, for unknown reasons, the port EDT pump took an hour to activate allowing a buildup of oil, gas, and water in the pipes connected to both EDTs. According to the Final Report by the Inquiry Commission, this mixture of vapor and fluids entered the starboard EDT through a leaky valve that was in the closed position. As the mixture filled the isolated EDT, the internal pressure rose until the tank finally burst at 12:22 am on March 15. The rupture not only released oil and gas into the starboard support column, it damaged the seawater service pipe (feedline to the fire-fighting system that ran up along the side of the EDT inside of the column), which initiated flooding of the column. Within 5 minutes, the rig had begun to list, and the platform entered an emergency shutdown mode. Fire-fighters were immediately deployed to the starboard aft column.

Upper Level Gas Explosion

An estimated 1,300 m^3 of gas escaped the burst EDT and collected on the upper levels of the platform. Meanwhile, the fire-fighting water supply experienced low pressure because the damaged seawater service pipe was flooding the column and its compartments instead of supplying water to the fire-fighters. Tragically, the fire-fighting team arrived at the column just as the rising gas encountered an ignition source and exploded. 10 fire-fighters were killed immediately, and 1 died a week later. The column suffered severe damage, and platform stability was further compromised. Evacuation of the rig began at 1:45 am.

The Tipping Point

Flooding progressed through the ventilation shafts which linked every room on every level of the column. Doors to the ballast tank and stability box (accessed through the column) had been left open for a scheduled inspection and flooded easily. The fire-fighting team had opened the water-sealed doors between levels in the column to access the hazard. With no one left to close them, these doorways facilitated flooding of the upper levels.

As the seawater pump room at the bottom of the column (inside the pontoon) flooded itself through the ruptured seawater service pipe, the pump eventually short circuited and shut down. However, the "fail-set" valve (designed to lock in the failed position) left the aperture to the ocean open, allowing the uncontrollable entry of seawater. As the pontoon tanks flooded, ballast control operators tried to stabilize the platform by pumping water into the port forward column (the column diagonally opposite to the starboard aft column). Efforts to counterbalance the rig worked temporarily but were ultimately unable to offset the rate of uncontrolled flooding of the damaged column.

The platform was finally abandoned at 6:03 am. By 8:15 am, the platform list had become so significant that the

openings to the chain lockers on the corner of the main deck were submerged, initiating massive flooding of the top levels and marking the point of no return. Over the next few days, nitrogen was pumped into the submerged pontoon in attempts to stabilize and salvage the rig. By 10:45 am on March 20, 2001, P-36 had sunk about 1,360 meters to the ocean floor and was declared a total loss.

Proximate Cause

The final report from the P-36 Accident Inquiry Commission concluded that a complex series of improbable events (predominately in emergency systems) caused the P-36 disaster and that almost every contributing factor represented an opportunity to break the chain of events. The principal trigger event was the leakage of a mixture of water, oil, and gas into the shut down EDT, which built up excessive internal pressure and ultimately ruptured the tank. The tank's proximity to key structural and operational elements served as the catalyst for the successive events that culminated with the sinking of P-36.

Underlying Issues

Focus on Cost-Cutting

Statements issued by Petrobras executives articulated the company's singular prioritization of financial performance. FUP heavily criticized the company's stance as sacrificial to the safety of Petrobras operations and responsible for a series of previous mishaps, including two pipe bursts, a toxic spill, and the deaths of 81 workers over the previous three years. FUP publicly blamed Petrobras management and "cutbacks," quoting downsizing of the workforce to almost half the size of a decade earlier and outsourcing to subcontractors with less training despite an increase in production and activities. The focus on financial performance directly lead to the decisions to design the EDTs into the support column, not to stop operations to investigate abnormal activity.

"THE PROJECT SUCCESSFULLY REJECTED … PRESCRIPTIVE ENGINEERING, ONEROUS QUALITY REQUIREMENTS, AND OUTDATED CONCEPTS OF INSPECTION …"

A PETROBRAS EXECUTIVE, PRIOR TO THE ACCIDENT, ON DELIVERING SUPERIOR FINANCIALS

Poor Design

The placement of the EDTs in the support columns and their close proximity to the seawater service pipes used for fire-fighting created an opportunity for a common mode of failure and was a large contributor to this disaster. Seawater fire-fighting systems present significant flooding risk if integrity is not protected. The P-36 Accident Inquiry Commission reported that the placement of EDTs in support columns was common industry practice but then recommended against doing so in future designs. Moreover, there was no evidence of risk or hazard analyses conducted prior to the decision to place the EDTs in the support columns or regarding the proximity of the seawater service pipe to tanks involved in production operations. Additionally, there were no apparent methods to inform the operators that a ruptured pipe was flooding the column. Finally, 1,723 alarms were triggered in the 17 minutes between the EDT burst and the upper level explosion. There was no system in place to prioritize these alarm entries or aid the control operators in addressing the overwhelming number of alarms.

Component Failure

In the series of failures of various pumps and valves, a lack of backup systems stood out as a common thread. The unexplained delay in the drainage pump of the port EDT allowed backflow of fluids for about an hour. These fluids were able to leak through a closed starboard EDT valve, which had no secondary protection in place to prevent leakage. After the tank burst ruptured the seawater pipes, flooding eventually shorted the seawater pump. The valves (which were fail-set by design) failed in the open position, which then allowed uncontrolled flooding of the column. While the fail-set option was not necessarily at fault, there was no backup system to control the flow of seawater once the pump had short circuited from the flood. Additionally, failure of the watertight dampers in the ventilation system facilitated flooding of the upper levels.

Lack of Training and Communication

Both the Inquiry Commission and the oil workers' union (FUP) cited deficiencies in the procedures and training to deal with emergency situation stability and ballast. The Inquiry Commission reported that when the ballast tank and stability box were opened for inspection, the crew did not follow the contingency procedures to prevent flooding. Additionally, no one closed the water sealed doors opened by the fire-fighting team. FUP blamed Petrobras' usage of subcontracted workers. They quoted that of the 81 workers who had been killed on Petrobras sites over the three previous years, 66 were subcontracted workers. FUP cited that these workers had less training and that few were aware of their rights to halt work if imminent danger was perceived.

Petrobras released bulletins by managers written in the three days before the accident recommending that production be shut down to deal with a pressurization problem in the pipes, which could have been partially responsible for flooding of the isolated EDT. The head office had not been notified of such concerns, but the investigation ordered by the Petrobras President (completed a few days after the accident) found this situation to be acceptable on the basis that "there [was] no indication of foul play or

deliberate concealment of information." While it could not be proven that this condition directly caused the P-36 accident, FUP contended that it was indicative of management's negligence towards safety.

Aftermath

A detailed investigation was performed by an Inquiry Commission comprised of representatives from employees, unions, and universities, overseen by global risk management agency, DNV. Final results and future recommendations were presented to mass circulation media in a move considered unprecedented in Brazil. Suggested improvements included improving the definition of responsibilities and supervision during maintenance and operations, reviewing the size and skill of the platform crew with regards to specific installations, upgrading the emergency procedures and equipment, and reprioritizing scheduled maintenance programs. Along with internal dissemination, workshops were conducted with both the domestic and international oil exploration and production industry. An Operational Excellence Program was implemented for offshore installations. The Commission called for the re-analysis of risks associated with any designs similar to P-36. And, in addition to the corporate Benefits Policy for the families of the victims, Petrobras provided each family's children with fully-paid scholarships for education through college.

Applicability to NASA

Maintaining the integrity of safe operations during budget cuts and downsizing is a reality in every industry and absolutely critical during human space flight. While efficiency and performance are essential goals, they must not be allowed to marginalize safety. Staff should be well trained for emergency situations, and disaster protocols should be practiced beforehand.

It is not uncommon for NASA missions to face conditions that require the usage of machinery or software in applications other than for which they were originally intended. In these cases, designs and modifications must be carefully analyzed not only for a new set of failure modes but also for possible event chains that could be triggered by proximity to other systems. Redundant systems or backup strategies help stave off a single failure cascading into a full system collapse. This requires a holistic view of how each component functions in the entire system. Components must therefore be either properly isolated from one another or grouped in such a way that manages the effect of one part's failure on its neighboring components.

Emergency systems should, to the greatest extent possible, simplify complex situations instead of create more problems due to poor design or improper analysis of all failure modes. In the case where multiple alarms may be triggered at once, the operators need a real-time methodology to determine the priority of each alarm in order to address them effectively and in the proper sequence. Fail-set components must be well understood for how the potential fixed state will affect operations in an emergency. Communication, monitoring, and feedback loops must be designed to deliver real-time information concerning the identification and causes of failure.

Questions for Discussion

- Do you feel that safety and quality assurance are prioritized below schedule and cost?
- Do you know how a failure in your operation might affect other operations, or vice versa?
- Do you understand the priority of emergency actions if multiple alarms are triggered?
- Are non-standard conditions or modifications re-analyzed each time they occur?
- Do you have contingency plans or backup systems that you can communicate in real-time to a known point of contact?

References:

"Brazilian Oil Workers: for Safety's Sake, End Subcontracting Now," *ICM News*, No. 15, 2001.

"Giant Oil Rig Sinks Off Brazilian Coast," *Environment News Service*, March 20, 2001.

"Inquiry Commission P-36 Accident," *Final Report*, Rio de Janeiro, Brazil. June, 2001.

"P-36", *Daily Shipping Newsletter*, March 27, 2001, p 11.

Rios de Campos Rosa, R., "Overview and Comments about Petrobras 36: Her History and the Accident," *International Workshop for Fire and Blast Considerations in the Future Design of Offshore Facilities*, Houston, TX. June 2002.

Valerio, C. and Dias, R., "The Sinking of the P-36," *NPD seminar presentations 1-5.*, April 2002.

Vogler, F., "Oil Rig Sinks at Sea," *Schadenspiegal: Losses and Loss Prevention*, No.1, 2003, p 20-23, Petrobras P-36, [Image].

2001 Annual Report and *2002 Annual Report*, Petroleo Brasileiro S/A.

System Failure Case Studies
A product of the NASA Safety Center

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

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