



SYSTEM FAILURE CASE STUDIES

MARCH 2012 VOLUME 6 ISSUE 3

Out of Line

Peaceful. Typical. Nondescript. These words should have described San Bruno, California on September 9, 2010. But residents of San Bruno's Crestmoor neighborhood will likely recall that day as one of horror and of grief—a day when some of them lost everything. That evening, a massive explosion occurred and a gas line leak fed an inferno that reduced the area to rubble. Witnesses likened the scene that followed to a war zone. Some residents narrowly escaped injury and many were hospitalized; others suffered the irrevocable loss of friends and family members. The gas line owner, Pacific Gas and Electric Company (PG&E), estimated the costs of damages at \$763 million.

BACKGROUND

Line 132: Construction

PG&E is an intrastate natural gas supplier whose customer base sprawls across Northern and Central California. The company owns and operates thousands of miles of distribution lines that stretch from as far north as Eureka to as far south as Bakersfield. Residents located in the peninsula between the San Francisco Bay and the Pacific Ocean receive service from one of three natural gas transmission lines—Line 101, 109, or 132.

Line 132 was constructed in phases, from 1944 to 1948, out of steel pipe segments with longitudinal welds (welds along the length of the pipe) that ranged in diameter from 24- to 36-inches. To form the finished product, these segments were bonded to one another with girth welds (welds along the circumference of the pipe). Testing standards for newly fabricated pipe did not exist at the time of its construction; consequently Line 132 went into service without undergoing the same pressure tests to which new pipelines are subjected today.

In 1955, however, the American Society of Mechanical Engineers (ASME) set forth a voluntary national consensus standard that called for transmission lines to undergo rigorous testing prior to entering service. PG&E encountered an opportunity to apply these new standards in 1956, when PG&E was requested to relocate 1,851 feet of Line 132 to accommodate new residential construction. PG&E agreed to move the requested segment of Line 132, and dispatched its own crews to perform the relocation. However, no record of pressure testing, or weld inspections of the relocated pipeline has ever been found.



Figure 1: The 2010 gas explosion and fire in San Bruno, California decimated the entire neighborhood of Crestmoor.

Line 132: Operation

PG&E manages gas transmission pipelines through a Supervisory Control and Data Acquisition (SCADA) control center. Stations along each of PG&E's transmission lines transmit data including pressure, flow, and valve positions to SCADA operators. These operators monitor the data, watch for anomalies, dispatch technicians, and coordinate maintenance work.

One of five lines that originate at Milpitas Terminal, Line 132 extends north for 46 miles to Martin Station. Line 132 connects to Lines 101 and 109 at many locations, which also service the peninsula region (Figure 2). Milpitas is an unmanned station that

Gas line ruptures, causes explosion in California suburb: 8 dead.

Proximate Causes:

- Improperly welded seam in gas transmission line weakens structural integrity
- Electrical malfunction at control station causes a pressure spike resulting in ruptured pipe

Underlying Issues:

- Poor quality control
- Inadequate integrity management
- Absence of emergency response plans

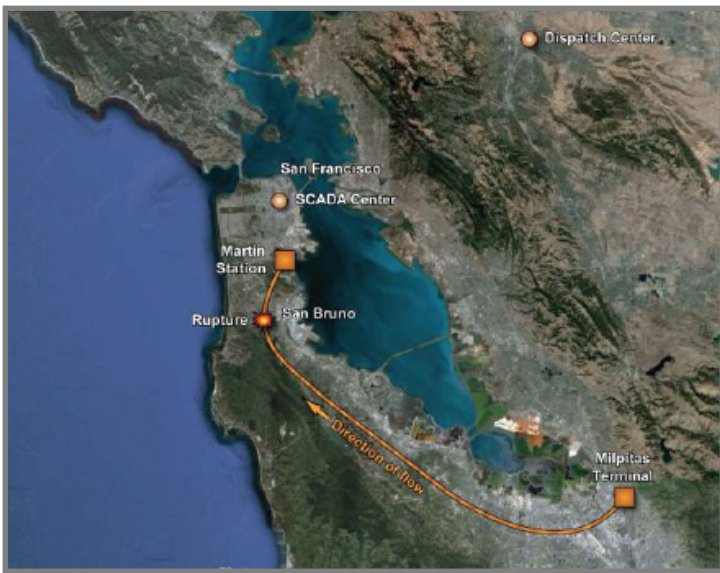


Figure 2: Line 132 originates at Milpitas Terminal and ends at Martin Station.

regulates outgoing pressure based on a pre-programmed control logic. Operators at SCADA can also control the regulator valves remotely. Thus, the line's outgoing pressure is limited to a certain level by both automated controls and remote monitoring. In the case of Line 132, that level—known as the maximum operating pressure (MOP)—was 375 psig (pounds per square inch, gauge).

In the industry, gas pipeline operators determine a line's MOP, to create a safety margin below the line's maximum allowable operating pressure, or MAOP. The formula for determining MAOP is defined in the Code of Federal Regulations (CFR) for natural gas transmission by pipeline, and MAOP varies depending on the properties of the pipe. However, a line's MOP is limited by the lowest MAOP of any other line connected to that line. For instance, Line 132's MAOP was 400 psig, but since Line 132 was also connected to Line 109 (whose MAOP was 375 psig), Line 132's MOP was limited to 375 psig. MAOP is used to determine zoning for residential, industrial, or other uses in consideration of potential gas explosion effects.

Safety Regulations

In 1970, new federal regulations required newly constructed gas transmission lines to undergo an extensive pressure test prior to entering service. The results of that test would determine the pipe segment's MAOP. However, a grandfather clause allowed operators to set the MAOP of pipelines constructed prior to 1970 at "the highest actual operating pressure to which a segment was subjected during the preceding 5 years." Based on this clause, PG&E set the MAOP for Line 132 at 400 psig since this was the highest recorded pressure Line 132 experienced in the previous 5 years.

Both interstate and intrastate operators own lines of vastly different ages, manufacturing histories, materials, and properties. Formulating a single rule that would ensure the safety of all of these pipes was impossible, so in 2004, the Pipeline and Hazardous Materials Safety Administration (PHMSA) passed performance-based regulations allowing pipeline operators to formulate their own integrity management program (IMP). By publishing this standard, PHMSA sought to improve safety for the thousands of miles of gas transmission lines crossing the nation. The IMP was required to be structured such that owners could effectively identify high-

consequence areas, recognize potential hazards, address significant threats, and prioritize line segments for testing and mitigation.

WHAT HAPPENED

Power Replacement and Overpressure

On September 9, 2010, PG&E technicians were dispatched to the Milpitas terminal to replace electronic systems as part of an upgrade to the station's power supplies. To accomplish the upgrade, the technicians needed to remove power. After doing so, they encountered an unexpected power loss at a local control panel. PG&E did not have a plan for this contingency. Instead of re-energizing the circuit, the technicians tried to reroute power from an alternate source. Their attempts, however, caused erratic output voltages to send an erroneous low pressure signal to the regulating valve controllers, affecting valve position sensors which triggered over 60 alarms at SCADA.

The alarms prompted SCADA operators to inform the Milpitas technicians that SCADA's readings indicated an abnormally high pressure at the Milpitas Terminal. Technicians confirmed that the erratic voltages had sent an erroneous low-pressure signal to the regulator valves, causing them to open fully. To complicate matters, the regulator valves could no longer be controlled because of power loss, so outgoing pressure was now solely controlled by monitor valves—a last line of defense against overpressure.

The monitor valves were set to prevent outgoing pressure from exceeding 386 psig. SCADA, however, informed Milpitas that their consoles indicated a pressure of nearly 500 psig on downstream pipelines. At 5:52 p.m. Pacific Standard Time, the operator asked the Milpitas technicians to place a pressure gauge on Line 132. Due to a lag in the monitor valve response time, the resulting reading showed an outgoing pressure of 396 psig—a value below the Line's MAOP of 400 psig, but well above the MOP of 375 psig. At 6:02 p.m., a SCADA operator called another PG&E monitoring facility and said, "we've got a major problem at Milpitas and we've over pressured the whole peninsula."

Explosion and Fire

At 6:11 p.m., San Bruno emergency dispatchers received the first of many 9-1-1 calls regarding a massive explosion and fire in the Crestmoor neighborhood. San Bruno firefighters, who heard and saw the explosion from their station, arrived on the scene minutes later. Meanwhile, an off-duty PG&E employee notified PG&E dispatch of an explosion in the San Bruno vicinity.

At 6:23 p.m., PG&E deployed a gas service representative (GSR) to the scene to confirm the report. At 6:30 p.m., SCADA operators became aware that a rupture had probably occurred, but they were unable to determine its exact location. While SCADA attempted to identify the rupture site, an off-duty PG&E technician who was qualified to manually close mainline valves, saw media reports of the fire. He proceeded to Colma Yard, a PG&E facility, where his truck and tools were located. A second qualified technician joined him there. Using visual cues obtained from watching media reports, the two technicians determined the location of the rupture. At 7:06 p.m., they reported their plans to isolate the rupture to a supervisor, and proceeded to the nearest shutoff valve.

The two mechanics manually closed the mainline valve by 7:30 p.m. Twelve minutes later (and 91 minutes after the rupture), the

fire's intensity decreased enough to allow firefighters to approach the rupture site and initiate containment. Fires in the area continued raging 2 days after the initial blast. The gas explosion killed 8 and injured 58, affected 108 homes, and left behind a 72-foot long by 26-foot wide crater.

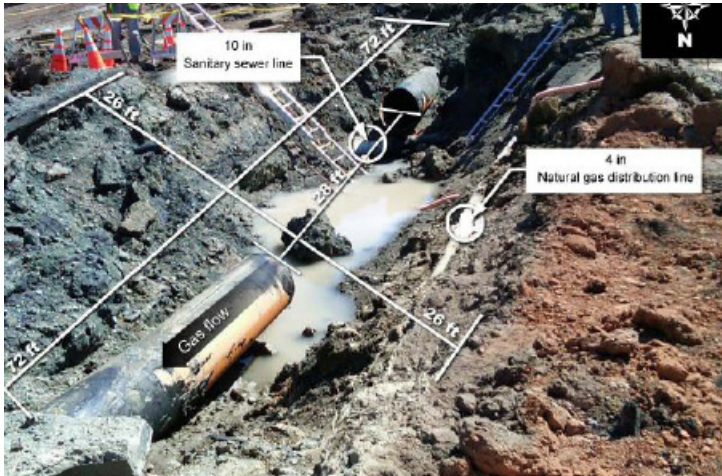


Figure 3: The ruptured segment of pipe, discovered 100 feet away from the crater, was 28 feet long and weighed approximately 3,000 pounds.

PROXIMATE CAUSE

The National Transportation Safety Board (NTSB) issued a report that attributed the explosion to a gas leak from a pipe segment, designated as segment 180, buried 3 feet beneath the intersection of Earl Avenue and Glenview Drive. Investigators discovered the ruptured segment 100 feet away from the crater that marked ground zero. Post-accident inspection revealed that segment 180 contained several shorter lengths with incomplete longitudinal welds—a defect that weakened the pipe's structural integrity and allowed a pre-existing crack in the seam to propagate. When subjected to the 396 psig pressure spike, the pipe ruptured despite the fact that this value still fell within the limits of the line's MAOP of 400 psig. The gas that spewed above ground ignited, killing and injuring residents while destroying property.

UNDERLYING ISSUES

Poor Quality Control

Results of the post-accident investigation showed that segment 180 was part of the 1956 relocation project. Per NTSB, the poorly welded seam in segment 180 would have been visible upon inspection. That the flaw escaped notice while the segment was relocated indicates a deficiency in PG&E quality control practices at the time, particularly since the relocation provided a good opportunity to inspect and test Line 132, and no record of such activities was located.

NTSB's investigation showed that the scope of PG&E's poor quality control practices extended beyond the 1956 relocation project. Nine months after the San Bruno explosion, NTSB received a report from PG&E that identified a gas leak in Line 132 in 1988, about 8.78 miles south of the rupture site. The 1988 report attributed the leak to a defect in the pipe's longitudinal seam. PG&E replaced 12 feet of pipe because of that leak. This incident should have prompted PG&E to test and inspect Line 132 for similar flaws, but no record of such actions was ever located. Then, in 2008, a natural gas explosion

involving a PG&E distribution line killed one person and injured five others. The subsequent NTSB investigation cited PG&E's use of inappropriate pipe material as a cause of the accident and delayed response as a contributory factor.

Inadequate Integrity Management

NTSB's analysis of PG&E's Integrity Management Program (IMP) revealed that the program was based on incomplete and inaccurate information about its pipes. PG&E records classified segment 180 as a seamless pipe, but in fact, the segment was composed of seam-welded pipe and contained several shorter lengths of pipes with incomplete longitudinal welds. Furthermore, steel grades, though unknown, were given "assumed" values and no steps to verify and correct the assumed values had taken place. NTSB stated that if overseeing bodies had required PG&E to correct its records, knowledge of the aging pipe's true properties may have prompted PG&E to test and ultimately repair or replace the faulty segment.

In addition to basing its program on incorrect information, the IMP also failed to account for the pipes' design and materials contribution to the risk of failure. It performed assessments without accounting for previously identified cracks in the pipes as threats to structural integrity and used examination methods that could not identify defects in longitudinal or girth welds.

During its investigation, NTSB discovered that PG&E employed a practice that undermined its own integrity management program. Increasing consumer demand meant increasing outgoing pressure on its lines. To avoid future pressure testing requirements and maintain the MAOP of Line 132, PG&E raised the pressure of its line periodically to classify any pipe defects as "stable" to prove that defects would not grow during service. When the director of the California Public Utilities Commission (CPUC) consumer protection and safety division discovered this practice, he stated, "artificially raising the pressure in a pipe that has identified integrity seam issues seems to be a wrong-headed approach to safety."

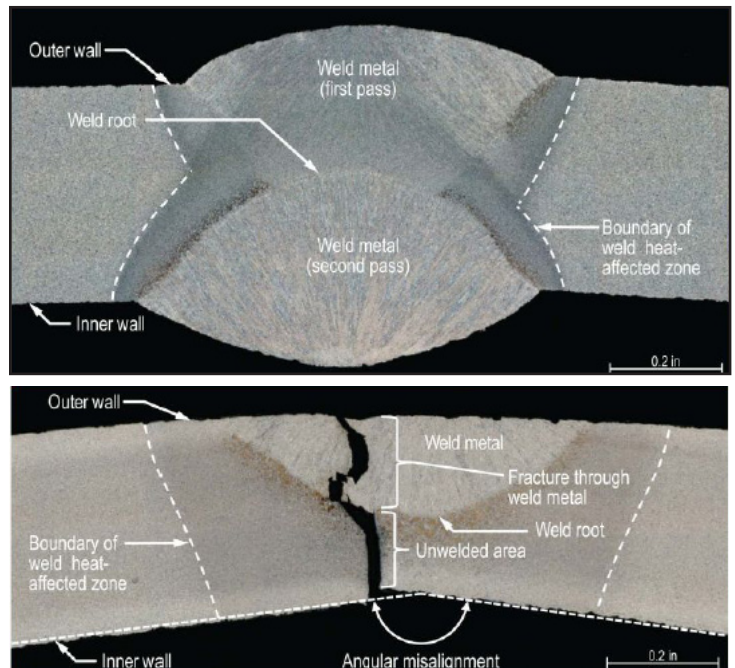


Figure 4: Top image shows a cross-section of a properly welded longitudinal seam. Bottom image shows a cross-section of the longitudinal seam in the ruptured pipe segment.

Flawed Emergency Response

The NTSB found that although a more rapid emergency response on PG&E's part would not have prevented the catastrophe, the effects of the fire would have been significantly reduced. After a delay in identifying the incident as a gas leak, PG&E's slow response allowed the continuously leaking gas to feed the flames. The fire burned so intensely that it prevented firefighters from initiating containment efforts immediately. If an off-duty technician had not acted on media reports, the 90 minutes between the rupture and the gas shutoff might even have been extended.

Per NTSB, PG&E should also have formulated emergency procedures, not only for a major event such as the San Bruno explosion, but also for maintenance activities such as the electrical work taking place at Milpitas. Loss of power at that station caused the pressure spike resulting in the rupture. If PG&E had formulated a plan for controlling the regulator valves during a power loss at Milpitas, the tragic events at San Bruno probably would not have occurred that day.

AFTERMATH

NTSB made several recommendations to PG&E such as establishing a comprehensive response plan for large scale emergencies, installing equipment to assist in identifying leak locations, adding automatic shutoff valves, and improving its integrity management program. NTSB also called upon overseeing bodies, including the CPUC and PHMSA, to enforce stricter pipeline safety regulations. In addition, NTSB called upon PHMSA to strike the grandfather clause from the CFR.

As of September 2011, PG&E projected it would test 786 miles of gas transmission pipelines and replace 186 miles of gas transmission pipelines by 2014. It also planned to install 68 new automated safety valves on the lines servicing the Peninsula. PG&E estimated total costs of planned safety improvements would reach \$2.18 billion.

FOR FUTURE NASA MISSIONS

The tragedy at San Bruno took place because a flaw was built into the system at inception and remained a latent hazard for more than 50 years. Although hindsight shows that opportunities arose to detect and correct that flaw, increased customer demand shifted focus away from thoroughness (understanding actual system margins versus increased pressure) to efficiency (satisfying demands with the existing system). NTSB characterized the incident as a tragic example of an organizational failure to recognize latent hazards.

NASA is vulnerable to latent hazards such as those leading to the San Bruno explosion. To some degree, the 2010 National Academies' assessment of NASA's basic research capabilities detailed large backlogs of deferred maintenance at NASA research centers. Years of bare subsistence research funding without sustaining infrastructure or procuring new instruments had left laboratory capabilities diminished compared to modern university and corporate laboratories. The study found that systems designed for planned maintenance are instead being run to failure. Separately, on construction and demolition projects, latent high-energy hazards such as buried conduits are struck inadvertently. Lack of accurate drawings along with failure to verify a circuit as de-energized contributed to a near-fatal electric shock at a NASA Center demolition site.

Questions for Discussion

- What steps are we taking to ensure that our current systems are free of latent flaws that might cause future malfunctions?
- What can we do to ensure that our own integrity management programs are truly effective—that they do not simply offer a false sense of safety?
- What contingencies and backup plans related to your project might you have possibly overlooked?

To carry forward the NASA tradition of leadership in exploration and scientific endeavors, we must feed our motivation to discover and act on those latent conditions—known and unknown, sometimes in combination—that lead to errors and unsafe situations; this is a learning culture that we are trying to further foster within NASA.

REFERENCES

Fagan, Kevin et al. "It looks like a war zone." SFGate.com. 11 Sept. 2010. < <http://goo.gl/Qeyk6>>.

La Ganga, Maria L. "U.S. official chastises PG&E over San Bruno blast probe." Los Angeles Times. 9 June 2011. < <http://goo.gl/Ql9mT>>

National Transportation Safety Board. Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire Accident Report. U.S. Government, 30 August 2011.

Sumwalt, Robert J. Investigating and Preventing organizational Accidents. National Transportation Safety Board. 25 Jan 2011 < <http://goo.gl/Glal6>>

Upton, John. "San Bruno Disaster Could Cost PG&E \$763 Million." The Bay Citizen. 18 Feb 2011. < <http://goo.gl/Ll5gx>>

Worth, Katie. "One year after San Bruno blast: Explosion the culmination of PG&E failures." San Francisco Examiner. 7 Sept. 2011. < <http://goo.gl/SIvsU>>

SYSTEM FAILURE CASE STUDIES



Responsible NASA Official: Steve Lilley steve.k.lilley@nasa.gov
Thanks to Stephen Klejst for an insightful peer review.

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. Visit nsc.nasa.gov/SFCS to read this and other case studies online or to subscribe to the Monthly Safety e-Message.