National Aeronautics and Space Administration

System Failure Case Studies

NOVEMBER 2006

Volume 1 Issue 1

DEATH ON THE STEPPES

At the dawn of the space age, the largest catastrophe in the history of rocketry occurred in the Soviet Union, killing dozens of people. The incident was kept a secret for decades, but we now know not only that it occurred, but that it was caused by a number of preventable factors: improper safety procedures, flawed design, hazardous chemicals treated with insufficient respect, and a rush to launch that was driven by political pressures and an overconfidence in technical competence by management.

BACKGROUND: A MISSILE RACE

In the late 1950s and early 1960s, the Soviet Union was engaged in a race with the United States of America in building intercontinental ballistic missiles (ICBMs). Early Soviet missiles had many problems, one of which was the use of liquid oxygen as the oxidizer for the fuel. The liquid oxygen required refrigeration at cryogenic temperatures and was difficult to store for the long periods of time necessary for a missile that had to be ready to launch at any time. The Soviets also wanted a system with better guidance, and an infrastructure that was less visible to surveillance from aircraft and satellites.

To address these issues, in 1960, the Soviet leadership initiated the development of a new type of missile that used so-called "storable" propellants, with improved navigation and smaller mobile launch platforms. The propellants chosen for this new missile, designated the R-16, were unsymmetrical di-methyl hydrazine (UDMH) as a fuel and inhibited red fuming nitric acid (IFRNA) as the oxidizer. These are hypergolic propellants, which mean that they self-ignite when they contact each other. While eliminating the problem of unreliable ignitors, new risk was taken on in using chemicals that were both extremely hazardous and highly corrosive.

So important was this project to the Soviet leadership that they put Marshal of Artillery Mitrofan Nedelin himself, the head of the Soviet ballistic missile forces, in charge of it.

The charred remains of the R-16 launch site in Tyuratam.

The R-16 was designed by a man named Mikhail Yangel. Together, the two men were determined to have a test launch of the new system in October of 1960, as a gift to Nikita Kruschev, the Soviet premier, to celebrate the November 7th anniversary of the Bolshevik revolution. Thus, not only was the design and development of the missile rushed, but its flight-development test program was as well.

In October of 1960, a missile disaster in the Soviet Union killed dozens of people.

Proximate Cause:

- Failure in electrical system

Underlying Issues:

- Numerous unauthorized personnel too close to launch pad
- Safety procedures non-existent or ignored
- Poor documentation and design
- Rushed development and design-verification test flight

Marshal Mitrofan Nedelin was in charge of the R-16 project.

What Happened?

Rules Ignored

On the morning of October 21st despite technical problems with the flight control system, the new R-16 rocket was rolled out to the pad at the Soviet missile launch site of Tyura-Tam. Two days later the initial checks had been completed successfully and the rocket was fueled on the launch pad.

Things started to go wrong from the start, beginning with a failure to follow sufficient safety procedures. Though the generals in charge of launch range and safety entreated their boss to leave for safety reasons, Marshal Nedelin insisted on remaining on the launch pad during fueling and testing, as did designer Yangel and a hundred fifty other non-essential personnel under his direction. Nedelin reportedly set up a chair on the pad to observe and direct operations.

"There would be no time for such things in nuclear war."

Problems Arise

In the late afternoon, as the schedule for launch approached, the membranes that prevented propellants from getting into the fuel and oxidizer lines of the 2nd stage were opened in preparation for launch. Following this, a set of explosive pyrotechnic devices on the valves of one of the first-stage engines went off, apparently spontaneously.

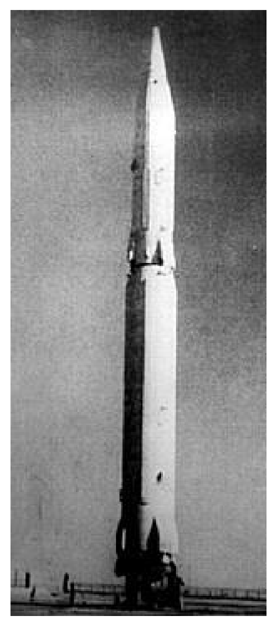
One or both of these events seems to have resulted in the leak in the fuel lines, though accounts differ as to the amount. One unconfirmed report describes buckets of propellant carried from the base of the missile; other, more reliable sources describe drips from lines that were subsequently tightened. Either way, the leak rate seems to have been deemed acceptable for launch, as long as it didn't increase, and the tests continued.

However, because of the leak, repairs had to be made to replace the blown pyrotechnics on the valves and the automatic control system used to operate them. According to some reports, requests were made to drain the rocket first, though there was no established procedure to do so, but Nedelin refused, saying that there would be "no time for such things in a nuclear war". At this point, it was getting late, so plans for the launch were put off until the following day as technicians worked through the night. During this time, more common sense safety procedures were violated, such as soldering on a fully fueled rocket. While it's not clear that this act of cutting corners directly contributed to the ultimate disaster, it is indicative of the work environment that set the stage for what was to follow.

The engineer who had [the only schematic diagram of the rocket's electrical system] wasn't allowed on the pad.

A Rush to Launch

On October 24th, a group of high government officials had arrived to view the launch, and a viewing stand had been set up for them several hundred meters from the pad. Nedelin was under pressure from Moscow to launch on time and reportedly had at least two conversations with Premier Khrushchev, who was apparently impatient with the seeming lack of progress. A few days before, Khrushchev had made a speech to the United Nations about the might of the Soviet armed forces, in which he claimed that rockets were being produced "like sausages from a machine."



The R-16 had been leaking propellant.

When another thirty-minute delay was announced, Nedelin insisted on going back to the pad himself and sitting just a few meters away to oversee things, stating "What's there to be afraid of? Am I not an officer?" His presence would have put more pressure on the technicians and probably was not necessary because it is unlikely that he would have been familiar with the details of the operation.

Time was beginning to run out due to the repairs needed to fix the previous day's membrane breach. Under pressure from their superiors, frantic technicians were running tests quickly and simultaneously. According to some reports, a "rough draft" schematic diagram (the only one in existence) of the rocket's electrical system may have been unavailable because, ironically, the engineer who had it wasn't allowed on the pad.

A Deadly Inferno

There was an automatic control system for sending signals to important components of the missile such as the fuel membrane pyrotechnics. During testing, the automatic control system had cycled through its settings so that it was no longer in a condition for launch. As the countdown continued, a technician sent a command to reset it to its launch condition. When this happened, a spurious signal was apparently sent to open the propellant line valves of the second-stage engines.

The propellants self-ignited and exploded the rocket's first stage engine, engulfing dozens in an inferno of toxic fumes.

Upon mixing, the propellants self-ignited and the engines lit, quickly burning through the top of the first stage, which then exploded. This created a fire at the pad of some 3000 degrees Fahrenheit and spewed toxic gases and flaming propellant all around. A movie camera that had been set up to record the launch instead captured the disaster.

The lucky ones were killed instantly, but many others burned and fell off the pad, still in flames, attempting to escape the blaze. Many people were reportedly trapped by a fence, unable to escape the oncoming wave of burning propellants. Others suffocated from the toxic acidic fumes. At least seventy-four people died that day, according to sources, including Marshal Nedelin, and approximately fifty more died later of their injuries. There has never been a more devastating disaster in rocketry, before or since.

THERE HAS NEVER BEEN A MORE DEVASTATING DISASTER IN ROCKETRY, BEFORE OR SINCE.

Proximate Cause

According to published reports, the proximate cause of the explosion was likely a failed "block" in the electrical system that was supposed to prevent signals from reaching operational portions of the rocket during testing. This failure allowed the activating signal to be sent to the second stage.

Underlying Issues

While the explosion was caused by the failure of the electrical inhibitor, this resulted in disaster because of poor design, a rush in development and testing, and a disregard for common-sense safety procedures. In terms of design, there were inadequate fail-safes built into the vehicle, and there were no established provision to safely detank it of its hazardous propellants if trouble arose.

The poor design was probably a consequence of the R-16's rushed development, and the rushed testing led to further mistakes. Both of these were driven by the political pressure of a nation at war and the project leadership's pursuit of prestige.

The destruction of the launch pad and the setback to the program would have been bad enough, but the unnecessary loss of life was a tragedy. There was no excuse for the excess of non-essential personnel located at the launch pad in such close proximity to a fully-fueled missile with technical issues still in resolution.

Problem Resolution

Even long after the end of the Cold War, much of the history of the Soviet missile program remains shrouded in mystery, but we do know that nothing remotely like the events at Tyura-Tam ever occurred again. Given the large numbers of missiles that the Soviets developed and tested, it seems clear that many lessons were learned from the Nedelin Disaster.

Doubtless they introduced much more stringent procedures regarding who was allowed on the pad and in dangerous areas in general, most likely to ensure that the orders of those responsible for safety would be obeyed, even by their superiors, would have been put in place.

Site 41, a memorial to those killed in the disaster stands at the test launch site.

Valuable lessons almost certainly were also incorporated in future missile designs. In fact, the descendants of those early vehicles, today's Russian space launchers, are considered quite safe and reliable; the U.S. space program has relied on them to keep the International Space Station supplied during the stand-down of the Space Shuttle before NASA returned to flight.

Applicability To NASA

The Nedelin Disaster is a cautionary tale against rushing design or development of a complex system with high energy content. It is critical to ensure that systems safety engineering is an integral part of the design process and the program life-cycle and to conduct extensive prototype/development testing prior to full scale flight hardware.

The applicability to NASA of this disaster lies in the preventable factors identified as contributing causes to the accident. Specifically, improper safety procedures, flawed design, hazardous chemicals treatment, and hastened launch decisions represent critical activities that require sound processes, policies, and decision-making for successful program execution.

In turn, the tragic events at Tyura-Tam are a powerful reminder of our need to follow through on our processes including adherence to and oversight of safety procedures, reviewing these procedures and the system design to ensure adequate depths of redundancy and safety are incorporated (i.e. detanking activities on the launch pad).

It is always instructive to go back and consider and discuss the mistakes people can make under the pressure of schedules. Although it might be comforting to think that we would never make such errors in judgment again, it would be foolish to think ourselves immune. NASA must continue to emphasize the importance of reading, discussing, and thinking about complex system failures and lessons learned, not only in the case of the Nedelin Disaster, but within each NASA Center and across the Agency.

The internalization of these lessons learned must then guide the design, development, and operation of complex systems. For example, as NASA staff and contractors in supporting complex missions develop System Safety Program Plans, Safety Data Packages, Safety Assessment Reports (SAR), etc., it is critical that we are implementing and monitoring these plans and processes to ensure quality system safety design reviews, thorough I&T activities (at NASA Centers and launch ranges), consistent pre/post-launch operations, and continually meeting NPR 8715.3 for safety requirements traceability. Finally, it is equally important to disperse these lessons learned and associated systems safety data into the hands of decision-makers early and often to ensure mission success through sound program execution and oversight.

Questions for Discussion

- How did errors that didn't necessarily cause the disaster heighten its consequences?
- Which problems would have been easiest to prevent? Which ones hardest?
- What lessons here apply best to projects you work on?
- What should the role in authority of the safety engineer be in supporting hazardous operations?

References:

Marshal Mitrofan Nedelin. Site 41 Memorial. [Online image] Available http://www.aerospaceweb.org/question/spacecraft/q0179.shtml, June 6, 2004.

"Nedelin Disaster." Aerospace.org. <http://www.aerospaceweb.org/question/spacecraft/q0179.shtml>.

R-16. [Online image] Available http://www.globalsecurity.org/wmd/world/russia/r-16.htm, April 28, 2005.

"Rockets: R-16 Family: Nedelin Disaster." RussianSpaceWeb.com. <http://www.russianspaceweb.com/r16_disaster.html>.

Siddiqi, Asif. "Challenge to Apollo: The Soviet Union and the Space Race, 1945-1974." NASA SP-2000-4408. (2000)

Siddiqi, Asif. "Mourning Star." Quest Magazine. Winter 1994.

Site 41. [Online image] Available http://www.videocosmos.com/images/plesetsk-80/nedelin-60.jpg.

Zak, Anatoly. R-16 Explosion. [Online image] Available http://www.russianspaceweb.com/r16_disaster.html, 2001.

Prepared by the

OFFICE OF SAFETY & MISSION ASSURANCE

RAD

Knowledge ▪ Understanding ▪ Visibility

Review and Assessment Division

Director: John Castellano (Acting) john.p.castellano@nasa.gov
Executive Editor: Steve Wander stephen.m.wander@nasa.gov

To view this document online and/or to read about other System Failure Case Studies go to http://nsc.nasa.gov/SFCS