National Aeronautics and Space Administration

NASA SAFETY CENTER

SYSTEM FAILURE CASE STUDY

April 2013 *Volume 7 Issue 3*

Through a New Lens

Apollo, Challenger, and Columbia through the Lens of NASA's Safety Culture Five-Factor Model

Ten years after the inflight breakup of Space Shuttle Columbia Space Transportation System Mission (STS-107), the memory of those astronauts—and of Apollo 1 in 1967, and Challenger in 1986—who died in the line of service continues to serve as a reminder to the Agency.

INTRODUCTION

Sifting through the hundreds of documents and studies published since each mishap, a recurrent theme of "safety culture" threads throughout thousands of words: the breakdown of safety culture, sustaining safety culture, changing safety culture… A testament to lessons learned and many mishaps past, the facts and findings of investigators and researchers presented in this publication serve to illustrate five factors underpinning the current safety culture of the seasoned Agency:

- Reporting Culture: reporting concerns without fear of reprisal
- Just Culture: treating eachother fairly
- Flexible Culture: changing and adapting to meet new demands
- Learning Culture: learning from successes and failures
- Engaged Culture: everyone doing their part

More information regard Agency safety culture can be found in the Orientation to NASA Safety Culture, HQ-SMA-ONSC course avaiable through the System for Administration, Training, and Educational Resources for NASA (SATERN).

This examination of failures during the Apollo and Shuttle programs is dedicated to the difficult and groundbreaking work of support personnel, engineers, and astronauts to achieve an incredible record of mission success and scientific achievement. Isolating failures (from the successes of a given program) in case studies sustains vigilance against future recurrence as new generations take over the construction and flight of spacecraft—especially crewed vehicles. Henry Petrosky, author of *To Engineer is Human*, stated, "No one wants to learn by mistakes, but we cannot learn enough from successes to go beyond the state

Apollo 1

Mission AS-204, January 27, 1967

Cabin fire during launch pad test

Remembered:

- Virgil "Gus" Grissom
- Edward H. White
- Roger B. Chaffee

Space Shuttle Challenger

Mission STS-51-L, January 28, 1986

Disintegration during launch after solid rocket booster O-ring seal failed

Remembered:

- Michael J. Smith
- Dick Scobee
- Ronald McNair
- Ellision Onizuka
- Christa McAuliffe
- Gregory Jarvis
- Judith Resnik

Space Shuttle Columbia

Mission STS-107, February 1, 2003

Disintegration during re-entry after foam insulation broke from external tank during launch

Remembered:

- Richard B. Husband
- William C. McCool
- Michael P. Anderson
- Kalpana Chawla
- David M. Brown
- Laurel Clark
- Ilan Ramon

Figure 1. Apollo 1 crew inside capsule. Source: NASA.

of the art.”

Considering past history and—even more importantly—current operations raises questions such as, “In what areas could the Agency do better?” “What is the Agency missing or ignoring in project risk management processes?” and “How can mission success be obtained given cost, schedule, and technical constraints?”

Reporting Culture:

we report our concerns without fear

From 1965 to the 1967 Apollo 1 fire, several reporting systems existed within the program, but there was no central management of the various contractor reports. Open investigations closed, but NASA management could be unaware of status change or how the closure was performed or verified, or whether affected project milestones had in fact been met. The phenomenon where the structure of an organization, and not an individual within the organization, prevents knowledge from reaching individuals who require it, is called “structural secrecy.” The Apollo astronauts lived and slept at the factory, attended design reviews, and communicated with each other; they were aggressive in notifying crew safety issues related to all aspects of flight—guidance, navigation, control, egress, etc.—to design engineers and NASA managers. Some crew suggestions were adopted, but others later deemed critical were dismissed. Behind the conversations between astronauts and engineers was a pitched contest for direct control of spacecraft functions as technology transitioned from stick-and-rudder atmospheric flight to counterintuitive orbital mechanics. In 2012, Apollo 7 astronaut Walter Cunningham said, “People don’t understand the deficiencies of those earlier preparations [to design and build Apollo spacecraft] [or] how we ended up with the fire…crews wanted changes at design review boards, like the hatch (an outward-opening hatch with explosive bolts) that got turned down…I think schedule was number one (priority), weight was pretty important too, but cost was not really a problem in those days…I believe astronaut overconfidence (was involved). We thought we could make up for those deficiencies.”

As a result of the fire, a centralized system collected all failures and assigned them to assessment areas; representatives from all engineering disciplines concerned with failure closeout were involved, and timelines were established to show vehicle and ground support equipment (GSE) closeout effectiveness in support of vehicle milestones and management awareness. Close calls that were not failures were reported as “problems,” and the Problem Reporting And Corrective Action (PRACA) concept was born. Not just safety issues, but Quality Assurance problem reports from inspectors resident at supplier sites entered the system. Real-time displays of open problem data affecting the next launch were maintained at the central point for use by the program manager. Over 50,000 problems were reported by the Apollo program’s end in 1972, but the majority ascribed to design and human error occurred in 1966 before the fire. This reflected tremendous effort to tighten up accountability at all levels targeting zero-defect functioning of spacecraft systems. “Stay vigilant and report everything” became a mantra for crew safety.

Problems continued to crop up and were reported, but control of risks appears to have improved greatly in the months following the fire as design, process, and procedures received laser-like attention.

After the loss of Challenger on mission STS-51L in 1986, Shuttle program manager Arnold Aldrich stated to the Rogers Commission that there had been a lack of problem reporting requirements, inadequate trend analysis, misrepresentation of criticality, and lack of involvement by the line safety organization in critical discussions. The Commission delivered their findings in a chapter titled “The Silent Safety Program” and called for a revival of the Apollo

Figure 2. Post Mercury and Gemini NASA sought to promote greater flight safety awareness with a symbol much like the United States Forest Service’s Smokey Bear. Source: NASA.

PRACA concept. Later research found that in the case of the engineering group directly involved with the failed solid rocket booster O-rings, program safety engineers had been closely involved, directly knowledgeable of the engineering rationale that accepted risk and recommended flight despite incrementally worse erosion, exhaust gas blowby and heat damage to O-ring material. All concerned saw this evolving situation as an acceptable risk, so none reported a safety issue until the famous telephone meeting of NASA Marshall Space Flight Center and Morton Thiokol engineers the evening prior to the STS-51L launch. Even if a mature PRACA system had existed, reporting requires belief and acceptance that a given problem exists.

Just Culture:

we treat each other fairly

In each mishap, evidence shows that excessive risk was secondary to other concerns. After many tries to point out hazards in the Apollo 1 command module, Gus Grissom hung a lemon outside the capsule as a sign of poor quality. Figure 3. indicates a lack of astronaut confidence that the post-fire Apollo culture would find unacceptable.

The telephone meeting between Marshall Space Flight Center NASA engineers and Thiokol engineers on the night before the STS-51L launch was scheduled on short notice to discuss a contractor concern. However, principal engineers and managers each adopted a Flight Readiness Review (FRR) approach during the call. The protocol was not discussed beforehand, but assumed by all who were familiar as FRR participants. Engineering arguments for and against launch were made and a formal, written Thiokol go/no-go recommendation was expected by meeting's end—even though this was the first time in program history that the contractor had expressed such concern. Those present without FRR experience later testified of surprise at the turn of events. Despite weak signals of previous launch damage to the SRB joint seals, the degree of uncertainty was not understood; too little was known about cold weather seal material performance. After the engineering point/counterpoint reached an impasse, Thiokol asked for a brief offline discussion during which managers were asked to "take off [their] engineering hat and put on [their] management hat" to reach a final recommendation. Mulloy had just told the contractors they were imposing new Launch Commit Criteria without sufficient evidence very close to launch, exclaiming, "My God Thiokol, when do you want me to launch, next April?" Seasoned FRR engineers were not surprised by the spirited trading of rationale and counter-argument, but others present said later they felt intimidated. Since July 4, 1982 (when the shuttle was declared operational upon completion of STS-4) the orginazational dynamic had slowly and incrementally shifted from "prove its safe" to "prove its unsafe."

Figure 3. The Apollo 1 crew parody portrait. Source: NASA

Regardless, most NASA personnel were sure that Thiokol would stick with its initial recommendation: do not launch below 53 degrees Fahrenheit. However, Thiokol managers decided they did not have enough strong evidence to stay with their recommendation and dropped them completely, testifying later this was not due to NASA intimidation. Yet, the option of testing for more knowledge was not even entertained. NASA Solid Rocket Motor Manager Larry Wear summed up the unusual decision in a 1992 interview, "Once you've accepted an anomaly or something less than perfect…you can't go back….where do you draw the line?…I can imagine what the Program would have said if we—we being me, Larry Mulloy, Thiokol, or anyone in between—if we had stood up one day and said, 'We're not going to fly anymore because we are seeing erosion on our seal.' They would have all looked back in the book and said, 'Wait a minute. You've seen that before and told us that was OK. And you saw it before that, and you said that was OK. Now, what are you? Are you a wimp? Are you a liar? What are you?'"

In 2003, on Day Two after STS-107 launch video indicated that foam had struck Columbia's left wing, Intercenter Photo Working Group engineers believed the orbiter may have been damaged and requested on-orbit imagery to assess the situation further. The hastily formed NASA Debris Management Team supported the request, but NASA and United Space Alliance managers who had officially shared their views that the strike posed a lower level of concern at first delayed and ultimately canceled a request to the USAF for imagery on Day Seven. The Columbia Accident Investigation Board (CAIB) report later addressed the issue:

> "The organizational structure and hierarchy blocked effective communication of technical problems. Signals were overlooked, people were silenced, and useful information and dissenting views on technical issues did not surface at higher levels. What was communicated to parts of the organization was that O-ring (a type of seal on the Space Shuttle Solid Rocket Booster relevant to the Challenger disaster) erosion and foam debris (relevant to the Columbia disaster) were not problems."

In a just culture, recurring willful intent to violate rules and/or the complacency to allow known violations to occur and reoccur requires accountability proportional to the violation.

Figure 4. Shuttle Flight Readiness Review. Source: NASA

Unintentional slips or decisions made with good intent that prove devastating are addessed though training or non-punitive communication.

Utmost importance must be placed on encouraging and rewarding those reporting unsafe behavior or previously unseen hazards instead of perpetuating a shortsighted "shoot the messenger" environment. Furthermore, a just culture assures that those reporting do not receive reprisals by those who may have been consciously negligent.

Flexible Culture:
we change to meet new demands

Evidence from the Apollo 1 investigation suggests that negative outcomes occurred when too much flexibility to create or modify design and procedures overran safety considerations. Operational test procedures were changed on the fly verbally, but not always in writing, because there was no policy in place to complete writing a test procedure before implementing it. No vibration tests were done on a flight-configured command module to accomodate schedule. At no point had the command module design been confirmed to be under configuration control. After the fire, crew safety-driven design changes and rules governing quality, reliability, and integration increased, but all involved understood the rationale behind stiffer standards and tight process control. The resulting Block II vehicle was much more reliable and served each crew well.

The vastly more complex shuttle produced a four-layer, rule-driven engineering culture that drove design and review processes to accommodate the production of flights in an "operational" environment. In both the Challenger and Columbia mishaps, an Acceptable Risk process allowed successive review panels to approve launches despite the lack of solid test data (accepting unprecedented cold temperature versus Solid Rocket Booster O-ring integrity) or counter to design specifications (accepting External Tank foam shedding in multiple launches). Contrary to findings of the Presidential Commission on the Challenger mishap, later research showed that no NASA or contractor engineer or manager concealed key information from managers or bypassed any rule; instead, rules were scrupulously followed and risk acceptance was documented. But the multilevel structure of reviews, coupled with an imperative to resolve problems to an acceptable risk level and fly, masked real uncertainty that engineers still faced in understanding the behavior of the Solid Rocket Booster (SRB) joint and External Tank foam system. Inflexible rules demanded decisions on problems at each review level, and the lack of perceived flexibility to test the design and fix flaws demanded problems be sketched in successively lesser detail and more certainty when presented to the next higher level. When each joint erosion or foam shedding event was accepted and the next mission flew successfully, mission success seemed to affirm each previous "go" review decision. By January 1986 and again in January 2003, engineers and managers behaved as if the SRB joint and external tank (ET) foam systems were understood when in fact they were not. Too few data points and lack of instrumentation needed for dedicated testing meant that SRB joint issues and foam loss events—judged later as glaring precursors—were weak and confusing signals at the time and considered insufficient in building a strong "no-go, ground the Shuttle" engineering argument against the success of past launches. NASA Solid Rocket Booster Manager Larry Mulloy testified, "We were absolutely relentless and Machiavellian about following through on all the required procedures at Level III…with all procedural systems in place, we had a failure."

> "The salient environmental condition was NASA's institutional history of competition and scarcity. We want to know how it affected decision making. Official launch decisions accepting more and more risk were products of the production culture in the SRB work group, the culture of production, and structural secrecy. What is important about these three elements is that each, taken alone, is insufficient as an explanation. Combined, they constitute a nascent theory of the normalization of deviance in organizations."
>
> —Diane Vaughan, The Challenger Launch Decision

> "One of the biggest problems we have at NASA sometimes is our can-do attitude. We're known for it. It's one of our greatest assets and it's also one of our greatest liabilities. The secret is knowing when can-do is too much and is pushing too hard."
>
> —Bob Crippen, Message to Shuttle Workforce, May 22, 2009

Learning Culture:
we learn from successes and mistakes

What did the Apollo Program learn from the Apollo 1 fire? Ironically perhaps, since the exact cause of the fire could not be identified but many other problems were found, there was a strong "zero-defect" motivation vertically and horizontally to improve every engineering and management domain with minimal schedule impact. At the spacecraft hardware level, a re-designed Command Module benefited from adoption of many previously identified hazard barriers and controls. Post-mishap, the Apollo Program welcomed a new focus on quality, reliability and maintainability, and system safety engineering. Safety and mission assurance specialists joined

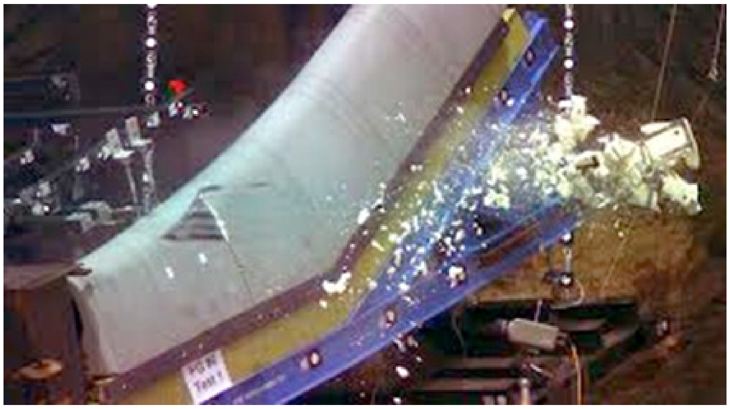

Figure 5. Foam debris test performed after Columbia mishap. Source: NASA.

the team in those areas for the first time. Above all, better planning and communication drove rigorous component-level and end-to-end testing. A high pressure, 100% pure oxygen atmosphere was used during the fatal test because it was accepted as necessary to achieve scaled pressures between orbit and the sea-level test pad for the capsule (a techinque stemming from high-performance aircraft test history). Actual risk exposure within the capsule was not understood. Historians credit the program's technical success after the fire to use of first-order data from well-designed tests. Apollo work involved engineers at every NASA Center and many aerospace companies. This created a a synergistic effect that transcended the program and changed aspects of NASA activities for decades after the program ended.

What did the Shuttle program learn from the Challenger mishap? Most of the recommendations of the Presidential Commission and the House Committee investigations were adopted. The troublesome SRB joint design was improved, management structure was studied and astronauts were added to the review process. All critical waivers were canceled and revalidation was required. A new independent safety organization was chartered and funded for oversight. Improved Shuttle landing gear and airfield aids were developed. Crew escape options were developed, but unfortunately they did not cover the first minutes after launch to suborbital glide altitude, or vehicle structural failure in any case. Maintenance activity planning was increased.

But in 2003, the CAIB reported that the Space Shuttle Program had not learned several lessons from Challenger, including continuing to treat the vehicles as operational, not as research and test vehicles—despite advice from the Aerospace Safety Advisory Panel in 1985 and from the Shuttle Independent Assessment Team (SIAT) in 1999. Acceptance of risk as normal despite uncertain data and contrary evidence continued with External Tank foam loss events, as mentioned in the CAIB report:

> "Cultural beliefs about the low risk O-rings and foam debris posed, backed by years of Flight Readiness Review decisions and successful missions, provided a frame of reference against which the engineering analyses were judged… NASA's culture of bureaucratic accountability emphasized chain of command, procedure, following the rules, and going by the book. While the rules were essential for coordination, they had an unintended but negative effect. Allegiance to hierarchy and procedure had replaced deference to NASA engineers' technical expertise."
>
> "Many accident investigations make the same mistake in defining causes. They identify the widget that broke or malfunctioned, then locate the person most closely connected with the technical failure: the engineer who miscalculated an analysis, the operator who missed signals or pulled the wrong switches, the supervisor who failed to listen, or the manager who made bad decisions. When causal chains are limited to technical flaws and individual failures, the ensuing responses aimed at preventing a similar event in the future are equally limited: they aim to fix the technical problem and replace or retrain the individual responsible. Such corrections lead to a misguided and potentially disastrous belief that the underlying problem has been solved…NASA's initial briefings to the Board on its safety programs espoused a risk-averse philosophy that empowered any employee to stop an operation at the mere glimmer of a problem. Unfortunately, NASA's views of its safety culture in those briefings did not reflect reality."

Engaged Culture: everyone does their part

Gene Kranz, Flight Director during Gemini and Apollo missions, called a meeting of his branch and flight control team on the Monday morning following the Apollo I disaster. He made the following address

> "Spaceflight will never tolerate carelessness, incapacity, and neglect. Somewhere, somehow, we screwed up. It could have been in design, build, or test. Whatever it was, we should have caught it. We were too gung ho about the schedule and we locked out all of the problems we saw each day in our work. Every element of the program was in trouble and so were we. The simulators were not working, Mission Control was behind in virtually every area, and the flight and test procedures changed daily. Nothing we did had any shelf life. Not one of us stood up and said, 'Dammit, stop!' I don't know what Thompson's committee will find as the cause, but I know what I find. We are the cause! We were not ready! We did not do our job. We were rolling the dice, hoping that things would come together by launch day, when in our hearts we knew it would take a miracle. We were pushing the schedule and betting that the Cape would slip before we did. From this day forward, Flight Control will be known by two words: 'Tough and Competent.' Tough means we are forever accountable for what we do or what we fail to do. We will never again compromise our responsibilities. Every time we walk into Mission Control we will know what we stand for. Competent means we will never take anything for granted. We will never be found short in our knowledge and in our skills."

According to Weick and Sutcliffe in *Managing the Unexpected*, "The common content thread in cultures that strive to be mindful, informed, and safe is that they all focus on wariness." It is incumbent on all NASA personnel to be wary about safety of flight hazards to crews, ground crews, the public, and valuable flight and ground systems.

Apollo and Shuttle program personnel engaged in dramatic fashion to do their respective parts after the Apollo fire, Challenger explosion, and Columbia inflight breakup. Management freedom to place safety ahead of cost and scheduling following Columbia allowed a safe flyout of the remaining Shuttle mission. This route was required to restore technical margins of safety, quality, and reliability. CAIB chairman Admiral Harold Gehman in a 2005 speech summed up the degree-of-freedom dilemma existing before the Columbia mishap:

> "…the program manager has four areas to trade. The first one is money. Obviously, he can go get more money if he falls behind schedule. If he runs into technical difficulties or something goes wrong, he can go ask for more money (Editor's note: this happened throughout Apollo). The second one is quantity…The third one is performance margin. If you are in trouble with your program, and it isn't working, you shave the performance. You shave the safety margin… The fourth one is time. If you are out of money, and you're running into technical problems, or you need more time to solve a margin problem, you spread the program out, take more time. These are the four things that a program manager has.
>
> If you are a program manager for the shuttle, the option of quantity is eliminated. There are only four shuttles. You're not going to buy any more. What you got is what you got. If money is being held constant, which it is…then if you run into some kind of problem with your program, you can only trade time and margin. If somebody is making you stick to a rigid time schedule (Editor's note: so the International Space Station could be 'Core Complete' by February 2004), then you've only got one thing left, and that's margin. By margin, I mean either…making something 1.5 times stronger than it needs to be instead of 1.7 times stronger than it needs to be—or testing it twice instead of five times. That's what I mean by margin…"
>
> "We actually found the PowerPoint viewgraphs that were briefed to NASA leadership when the program for good, solid engineering reasons began to slip…One, work over the Christmas holidays. Two, add a third shift at the Kennedy Shuttle turnaround facility. Three, do safety checks in parallel rather than sequentially. Four, reduce structural inspection requirements. Five, defer requirements and apply the reserve, and six, reduce testing scope…they're going to cut corners. He's only got four choices, right? There is no more money. There are no more shuttles…So the only choice he has is margin."

After Apollo 1, money and schedule were added. After Columbia, money and schedule were added. Degrees of program management freedom enabled a large enough technical margin to gain mission success.

The physics of reaching low Earth orbit remain merciless, but history speaks to those who listen. The five factors of NASA Safety Culture can help all NASA employees interpret weak and mixed signals and reach sound decisions in the face of uncertainty. Our commitment to these principles is vital as NASA and commercial companies seek to work both independently and in concert to launch Earth science missions, to resupply and re-crew the International Space Station. Try looking at your own project or organization and asking, "How are we behaving with respect to the Five Factors of NASA Safety Culture?"

REFERENCES

"Apollo Astronauts Discussing The Apollo 1 Fire - Part 2." http://www.youtube.com/watch?v=zm_j0cw1zCw, accessed March 11, 2013.

Gray, Mike. *Angle of Attack*. Norton, 1992

Apollo Experience Report, Problem Reporting and Corrective Action System, NASA, Feb 1974.

CAIB Report, Volume 1 Chapter 8, 2003.

Ethical Challenges for Organizations: Lessons Learned from the USS COLE and Columbia Tragedies. ADM Harold W. Gehman, Jr. USN (ret), 2005.

Burgess, Colin, Kate Doolan, Bert Vis. *Fallen Astronauts: Heroes Who Died Reachning for the Moon*. Bison, 2003.

Mindell, David. *Digital Apollo: Human and Machine in Spaceflight* MIT Press, 2008.

NASA Report to the President: Actions to Implement the Recommendations of the Presidential Commission on the Space Shuttle Challenger Accident, 1986.

Rogers Commission Report, GPO, 1986.

Vaughan, Diane. *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. University of Chicago Press, 1996.

Weick, Karl E., Kathleen M. Sutcliffe. *Managing the Unexpected: Assuring High Performance Technology in an Age of Complexity*. Jossey-Bass, 2001.

NSC
NASA SAFETY CENTER

Responsible NASA Official: Steve Lilley steve.k.lilley@nasa.gov
Thanks to Dr. Tim Barth, Dr. Tracy Dillinger, Dr. Barbara Kanki, Donna Blankmann-Alexander, and Larry Ross for their insightful peer reviews.