


Some Safety Lessons Learned

BY BRYAN O'CONNOR

The proximate causes of an accident and the changes needed to avoid repetition are usually clearer and more readily dealt with than the associated root causes. As a team of engineers, we usually find a way to modify the design, change the software, or develop an operational workaround that adequately mitigates the proximate and near-proximate causes of our mishaps. But root causes are different kinds of problems.



Lightning strikes near a silhouetted mobile launch tower about 36.5 seconds after the 1969 liftoff of Apollo 12, which was also struck during its ascent. This event led to updated weather criteria for governing launch decisions, but a rationale for the update was not recorded.

Root causes tend to be related to the broader, sometimes squishier aspects of what we do: such things as the what-versus-how of our procedures and requirements and the appropriate volume and frequency of organizational communications up and down and left and right. Sometimes they involve organizational and authority relationships, the effectiveness of checks and balances, and other cultural aspects of program and operational management.

The *Columbia* Accident Investigation Board (CAIB) report recommendations and associated internal studies resulted in two very challenging sets of activities: the first technical, the second managerial. Efforts dealing with the proximate (technical) causal factors were tough because the physics and engineering and production processes related to external tank insulation in the ascent environment are very complex. As for the managerial changes, they too were difficult, but probably for very different reasons.

The CAIB report listed a number of organizational/cultural findings and recommendations, but that section did not include the kind of factual basis that characterized the technical parts of the report. Of seven volumes of factual information in the CAIB final report, none pertained to the root causes of the mishap; they were all about the technical failure itself. The relatively limited summary of organizational and cultural material in volume one was all we had, leaving much to the NASA team to determine for itself. By itself, this should not have been a problem for us. After all, any mishap board is advisory, and the ultimate findings often come from Agency follow-up. In this case though, the high visibility of the CAIB investigation, along with the public statements by the board about lack of engineering curiosity and authority

imbalances between the institution and the program, made it very difficult for the Agency to modify, let alone disagree with, their specific recommendations.

On top of that, we asked another external group (the Covey Stafford team) to oversee our return-to-flight activities and told them they should evaluate our efforts relative to the “intent” of the CAIB. We asked the Covey Stafford management team to interpret the intent of the CAIB’s three management recommendations. Unfortunately, the CAIB members they consulted, the Covey Stafford management team members, and our own NASA leaders could not agree on intent. The result was several false starts, uneven application of the new governance model, and residual issues and misunderstandings that persist to this day.

Having said that, I believe NASA’s governance model and safety culture in general are as good today as they have been for a long time. In retrospect, though, I think it was a shame to waste so much time and effort getting to this point.

A Recipe for Safety

So what are the best ways to make the inherently risky activity of human space flight as safe as possible? My recipe for flight safety goes like this:

- 1 part shared values
- 1 part organizational structure
- 1 part requirements
- 2 parts risk management
- A pinch of luck



CAIB Photo by Rick Stiles 2003

A CAIB reconstruction team member examines debris with a video microscope. The CAIB report included technical and managerial recommendations, both difficult to put into practice for different reasons.

The value of luck goes without saying and, although some environments seem to be more conducive to good or bad luck than others, luck generally is not something you can do much about. I'll look briefly at the other ingredients.

Shared Values

An organization whose core values include teamwork, integrity, excellence, and, of course, commitment to safety is likely going to have a good mission success and safety record. Alcoa and DuPont are two well-known organizations whose strong core values are reflected in excellent safety records. Closely related to teamwork and commitment to safety is accountability. Everyone in NASA is responsible for safety, although the degree of individual accountability varies in accordance with this formula:

$$\text{Accountability} = \text{responsibility} \times \text{authority} \times \text{capability}$$

A given individual's level of formal responsibility and authority may vary from project to project. Their capability—the relevant knowledge and experience they have—will also vary from situation to situation. But none of those factors—responsibility, authority, or capability—is ever zero, so no one can entirely lack accountability, regardless of how far they are from the prime decision makers. At the very least, every person is accountable for his or her own safety. Those with programmatic and technical authority and capability find themselves more or less accountable for the safety of the mission.

Organizational Structure

A key aim of NASA's recent governance changes has been to establish an independent technical authority and ensure that technical concerns that arise at any level will be addressed. The check-and-balance model we have chosen means that the programmatic and agency strategic leadership decide on programmatic and performance parameters, and the institution uses years of lessons learned to decide which technical requirements apply. The program needs institutional (independent technical authority) approval for relief from technical requirements but works as necessary within the programmatic chain of command for relief from cost, schedule, and performance requirements. This is the model we believe the CAIB intended.

Requirements

Good requirements are nothing more than lessons learned. To be effective, though, they must come with enough context and background to explain why they exist. Without an understanding of the underlying reasons for a requirement, decision makers are more likely to make the wrong choices. An example of the problem is the 1987 Atlas Centaur 67 lightning strike that destroyed an Atlas 2 and its FleetSatCom payload. A lack of rationale—of context—for the weather criteria governing launch decisions was a factor in a faulty decision and the loss of the mission.

Risk Management

Much of what we do at NASA is not conducive to simple requirements compliance. The nature of our missions means that our performance margins are often very low, and we often find ourselves accepting "residual" safety risks in order to accomplish the mission. If we were to design a human space

flight vehicle that fully met all our standards and requirements for human rating, it likely would be too heavy to fly. So some number of waivers for our technical requirements and less than fully controlled hazards are inevitable. Bad experiences from the past (notably *Challenger* and *Columbia*) tell us that we are capable of fooling ourselves when we fail to apply technical rigor and process discipline in our risk management processes.

Learning from Experience

No matter how dedicated we are to safety, accidents happen. When they do, they give us an opportunity—though often a painful one—for learning that can prevent problems in the future. We also need to be careful not to derive the wrong lessons from experience. Specifically, we don't want to "learn" from a string of successes that a particular kind of mission is inherently safe and we no longer need to look so carefully at risks.

There are, broadly speaking, two modes of learning and behavior that help organizations prevent mishaps. One is incident recovery: the intense, focused period of analysis and action that follows an accident and takes steps to avoid a recurrence. The other is complacency avoidance: countering the tendency to assume that recent success promises future safety.

Learning from Incident Recovery

A serious mishap galvanizes an organization. Experts minutely study the evidence to uncover the proximate causes of the accident. This type of work, though reactive, is engineering in every sense of the word. NASA engineers know how to investigate failures and, in the wake of a major mishap, motivating them to do it well is not an issue. If anything, we have to tell our investigators to back off and take a breath once in a while.

Fighting Complacency

After the mishap investigation and the return to flight, the team focuses again on the mission, and the challenge for the leadership team shifts from recovery to fighting complacency. Countering complacency is arguably harder than recovering from a mishap. We have to find creative ways to counteract the common psychological tendency to assume that a string of successes means that we have somehow reached a state of engineering and operational perfection—and, therefore, immunity from failure. One way I have found useful to get our team back to the proper state of humility and respect for risk is to occasionally revisit accident case studies. This does two things. It reminds us that other people who thought they were paying sufficient attention to safety have been surprised by failure; the case study serves as a vivid reminder of the fact that most past accidents almost always happened during a period of complacency. It also gives them a challenging and—we hope—relevant technical problem-solving session. These two things can go a long way toward reviving the critical recovery mind-set. They, along with the safety factors I mentioned above—shared values of teamwork, integrity, and commitment to safety, and requirements that make clear *why* they are important—are crucial weapons in our fight against complacency. ●



BRYAN O'CONNOR is a former Marine Corps test pilot and aeronautical engineer. He served at NASA as a Space Shuttle commander and program director and is currently serving as the Agency's Chief of Safety and Mission Assurance.