Success, Failure, and NASA Culture

BY DR. STEPHEN B. JOHNSON

When humans first went to space in the 1950s and 1960s, many rockets and satellites failed, leading to the development of processes and technologies to reduce the probability of failure. The extreme harshness of the space environment required novel technologies, but it also drove conservative design to prevent or mitigate failures. In NASA's formative years, these contradictory requirements deeply influenced its organizations and processes. The novelty of NASA's missions, along with the fact that they were generally unique or few of a kind, led to the adoption and refinement of project management and systems engineering to develop and build rockets and spacecraft.

Photo Credit: NASA

Workers study Hubble's main, eight-foot (2.4 m) mirror. The flaw in the Hubble Space Telescope's optics was due in part to reductions in testing to save money.

While Wernher von Braun's experienced rocket team at Marshall Space Flight Center eschewed systems engineering, NASA's other field centers developed that discipline to ensure proper communication and design reviews. In the 1950s and 1960s, the introduction of systems engineering, along with other related innovations such as redundancy and environmental testing, generally reduced system failure rates from around 50 percent to around 5 to 10 percent for robotic spacecraft and better than that for human flight. Von Braun's team seemed anomalous, for it attained very high reliability with its Saturn rockets without systems engineering. However, von Braun's team, which held together for nearly four decades, had learned its trade through three decades of tests and high failure rates from the 1930s in Germany through the 1950s in the United States. Only after the retirement of the German rocket team in the 1970s and the diversification of Marshall beyond rocketry did systems engineering begin to make significant inroads there.

Improvement in system reliability came with increased bureaucracy, as systems engineering put a variety of cross-checks and reviews in place. System dependability improved, but these processes and technologies increased the cost of each vehicle. Eventually, and in response to pressures to decrease costs, engineers and managers cut back on safety and reliability measures. Also, as Henry Petroski explains in *To Engineer Is Human* and *Success Through Failure*, success encourages engineers to reduce performance and safety margins to reduce costs and to create more elegant, optimal designs. Not surprisingly, these cutbacks, exacerbated by overconfidence, lead to failures. Failures in turn lead to increased attention to reliability and safety, pushing the pendulum in the other direction.

We see these pendulum swings in NASA's history. By the 1980s, as NASA faced increasing pressures to reduce costs, many aspects of its bureaucracy, including systems engineering, came under scrutiny. Many outsiders and some insiders began to question the need for all the "red tape." Citing a variety of examples, such as Total Quality Management (TQM) from Japan's automotive manufacturing and the Skunk Works model from Lockheed's aviation organization, critics believed NASA could build and operate its systems more quickly and less expensively by cutting back or changing its management and organization.

Faster, Better, Cheaper

After the *Challenger* accident in 1986, the human flight program was able to reestablish a focus on safety for a number of years. This shifted the cost-cutters' attention to robotic spacecraft programs, however. By the late 1980s, NASA began to experiment with a number of these management ideas, including TQM and reengineering. At the same time, traditional projects came under criticism. For example, the Cassini probe came under fire, parodied as "Battlestar Galactica" because of its size, complexity, and cost, and was frequently cited as an example of what NASA should not do. Failure of the Mars Observer in 1993 demonstrated again that projects managed with traditional methods sometimes failed. The 1990s became the era of "faster, better, cheaper" (FBC) during Dan Goldin's administration. Projects such as Mars Pathfinder, which landed on Mars for significantly lower costs than the 1970s Viking project, were touted as proof that the new methods worked (and hence that the old techniques were unnecessary).

Funding cuts and experiments to reduce the bureaucracy led to occasional success but also to increased failure rates. The flaw in the Hubble Space Telescope's optics was due in part to reductions in testing to save money. A series of failures in Earth-orbiting projects and most prominently in the Mars Polar Lander and Mars Climate Orbiter projects in 1999 led to a rethinking of the FBC strategy. By the early 2000s, the Mars program had retrenched and returned to more conservative and traditional management with significantly more funding than its recent predecessors. Managerial innovations like TQM, reengineering, and FBC were being reconsidered or rejected in favor of a return to classical systems engineering and systems management.

In the 1980s and 1990s, the debates about NASA's organization and its relation to system success or failure had been couched in terms of management methods, in particular systems engineering and management versus a variety of other techniques that usually originated outside the space industry. The loss of *Columbia* in February 2003 changed the debate. What caught the attention of the *Columbia* Accident Investigation Board (CAIB) and others was the resemblance of the decisions and factors leading up to the accident to those behind the *Challenger* accident seventeen years earlier. Ominously, the problems seemed to exist *within* the structures and processes of classical systems engineering and management. These inherent problems posed, and still pose, a much more serious threat to NASA than the attempts to impose new and arguably ill-suited techniques from outside the space industry. Instead of failures to follow rigorous systems engineering methods, as had been the usual earlier diagnosis, the CAIB identified NASA's *culture* as a primary cause of the *Columbia* tragedy.

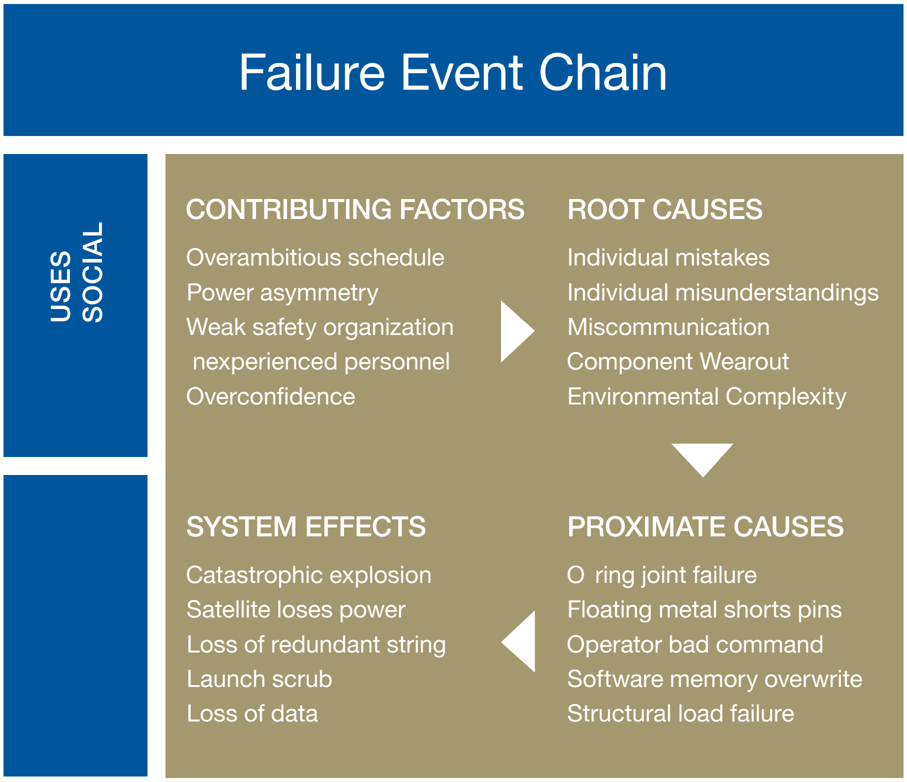
Photo Credit: NASA Kennedy Space Center

The Cassini spacecraft is mated to the launch vehicle adapter in Kennedy Space Center's Payload Hazardous Servicing Facility. Cassini was once frequently cited as an example of what NASA should not do because of its size, complexity, and cost.

The Challenge of Culture

This diagnosis was problematic for NASA for at least two reasons. First, it was not clear what "culture" really meant, as it is a famously holistic and ambiguous term, even for social scientists who use it in their day-to-day work. "Culture" covers a lot a ground, including patterns of human knowledge, beliefs, behaviors, and social forms. Out of the full set of NASA's human knowledge, beliefs, and behaviors, what is it exactly that NASA needed to change? Second, whatever NASA's culture actually is, it is not geared toward soft and squishy concepts about people but rather toward precise, technical assessments of things. Any action to address social issues would be difficult.

NASA's first response to the *Columbia* accident was to determine and fix the technical causes and implement operational procedures to minimize the risks; for instance, ensuring that shuttle missions always had means to inspect the thermal tiles and repair them if necessary. Addressing the cultural issue was more difficult. Knowing that internal



Failure Event Chain

CONTRIBUTING FACTORS

Overambitious schedule
Power asymmetry
Weak safety organization
nexperienced personnel
Overconfidence

ROOT CAUSES

Individual mistakes
Individual misunderstandings
Miscommunication
Component Wearout
Environmental Complexity

SYSTEM EFFECTS

Catastrophic explosion
Satellite loses power
Loss of redundant string
Launch scrub
Loss of data

PROXIMATE CAUSES

O ring joint failure
Floating metal shorts pins
Operator bad command
Software memory overwrite
Structural load failure

expertise was lacking, NASA hired Behavioral Science Technology, Incorporated, (BST) in 2004 to lead the culture-change effort. BST promised to assess NASA's culture through surveys and then implement changes that could be quantitatively measured. This experiment lasted only one year, however, as NASA's executive leadership decided that NASA had the skills to implement cultural change in house.

Another of the CAIB recommendations was to implement an Independent Technical Authority. This was duly accomplished. In February 2006 it was replaced by a new directive to move to a "Process-Based Mission Assurance" system. Behind these changes was the implementation of a renewed and restrengthened matrix management system, where engineers were responsible to the engineering technical authority for the technical effectiveness of their work and to their project management for day-to-day direction. One major goal was to ensure that if engineering opinion was rejected through one line of management, engineers had another line through which to communicate their concerns. Safety reporting systems remained in place and were reemphasized to ensure that safety-related problems could be reported separately from either of the project or engineering management chains. At present, these activities form the bulk of NASA's top-down cultural changes, albeit without the "culture change" label. In addition, educational efforts at NASA's Academy of Program/Project and Engineering Leadership (APPEL) are under way to address some of the cultural issues brought forward by CAIB, as education is a key component of long-term generational change in the workforce.

Is there still a need for "culture change" at NASA? I believe the answer remains "yes." The reinvigorated matrix structure is a move in the right direction, multiplying communication channels and delineating responsibilities for technical excellence. APPEL's new and updated engineering and management curriculum, if properly focused, is also a significant step. However, the core issues that relate NASA's "culture" to improvements in system dependability and safety have so far, in my opinion, only been marginally addressed. If the CAIB had any message for NASA regarding culture, it is that something in NASA's social organization and processes leads to technical failure of systems. To directly address the CAIB's concern, we must determine the connection between culture and failure.

To make this connection, we need to understand the nature of faults and failures. Failure is generally the outcome of a chain of events that are made more likely by various contributing factors. Failure investigations start from the end of the failure process: the final failure effects, which can include complete system loss, like the Space Shuttle *Columbia* burning up in the atmosphere, or can be more benign, such as the scrub of a launch. The proximate causes are generally the technical items that malfunctioned and led to the failure effects: O-ring failure of the *Challenger* accident, or the foam that fell off the external tank and hit *Columbia*'s wing during ascent. But proximate causes have their genesis in root causes, such as human-induced errors in the application of the foam to the external tank in the *Columbia* case, the decision to launch *Challenger* on a morning when the temperature was lower than rated environmental limits, or human error in creating the shuttle's original, flawed Solid Rocket Booster segment-joint design. Finally, there are contributing factors, such as pressures to launch the shuttle on an accelerated schedule, pressures to lower costs, or use of a teleconference instead of a face-to-face meeting contributing to miscommunication.

Frequently, we find that the failure effects and the proximate causes are technical, but the root causes and contributing factors are social or psychological. Successes and failures clearly have technical causes, but a system's reliability strongly depends on human processes used to develop it, the decisions of the funders, managers, and engineers who collectively determine the level of risk. In the terms of an old cliché, "we have met the enemy, and they are us!" We humans make mistakes, either individual cognitive or physical mistakes, or as groups through lack of communication or miscommunication.

Although the statistics have not been studied fully, my sense, from experience in the field and discussions with other experienced engineers, is that 80 to 95 percent of failures are ultimately due to human error or miscommunication. Most of these are quite simple, which makes them appear all the more ridiculous when the investigation gets to the root cause and finds, for example, that it is due to a missed conversion factor of English to metric units, a simple error in a weld, a reversed sign in an equation, or one person not knowing that another person had a piece of information needed to make a proper decision. The mundane nature of the causes is precisely what makes them so hard to catch. We constantly carry out simple daily tasks and communications. Thousands of such tasks and communications happen every day on a project, and any one of them can be the cause of tomorrow's dramatic failure.

FREQUENTLY, WE FIND THAT THE FAILURE EFFECTS AND THE PROXIMATE CAUSES ARE TECHNICAL, BUT THE ROOT CAUSES AND CONTRIBUTING FACTORS ARE SOCIAL OR PSYCHOLOGICAL.

Systems management and systems engineering reduce failure rates by providing formal cross-checks that find and fix most potential mission-ending faults. Skunk-works approaches can succeed through the extraordinary hard work of a cadre of experienced personnel, but over the long run, they are not repeatable. That is because we humans are unable to maintain our focus for long periods. Eventually we become lax and forget some key detail or skip a critical process because "we know" that we have done the right things and don't need to double-check. Systems management and systems engineering cannot guarantee absolute success either, but history shows that they do significantly reduce project failure rates. This should be no surprise, because that is what they were created to do.

How can NASA make progress directly addressing the CAIB recommendations? The first step is recognizing that technical failures have individual and social causes. Evidence for this is overwhelming, and we do not need to look further for some elusive "cultural issue." The second step is to take action. While there is no single solution to this problem, there are many ways we can improve. We can perform research to better understand how humans make mistakes and what circumstances increase our "natural error rates." We can use this research to change the environment in which we operate and communicate, and we can educate ourselves to reduce the probability of making individual mistakes or miscommunicating with others. We can improve the relationships between engineering, operations, and safety organizations, and we can create design and operational engineering disciplines to better engineer our systems to tolerate the inevitable failures.

Above all, NASA needs to make tackling the individual and social causes of failure a priority. It should put a plan in place to start the research and to plan, coordinate, and assess organizational and educational innovations specifically targeted to improve dependability. Individual education, organizational change, and technical improvements will all be part of this plan. All these methods, and the efforts of all of us, will be needed to tackle this, one of NASA's most difficult and deep-seated issues. ●

STEPHEN B. JOHNSON is a health management systems engineer for the Advanced Sensors and System Health Management Branch at Marshall Space Flight Center and an associate research professor with the Institute for Science, Space, and Security Centers at the University of Colorado at Colorado Springs. He is the author of *The United States Air Force and the Culture of Innovation, 1945–1965* and *The Secret of Apollo: Systems Management in American and European Space Programs.*