Section V

NASA Cultures

Introduction

One of the main conclusions of the Columbia Accident Investigation Board (CAIB) was that "the organizational causes of this accident are rooted in the Space Shuttle Program's history and culture" and that over many years at NASA, "cultural traits and organizational practices detrimental to safety and reliability were allowed to develop . . . ."[1] The idea of organizational culture is therefore a critical issue, though, as La Porte points out in this section, it is a "slippery concept" with a "high degree of operational ambiguity, its use subject to stiff criticism." Although organizational culture may in fact mean many things, all three authors in this section find the concept useful, for lack of a better term, to refer to what La Porte characterizes in the NASA context as "the norms, shared perceptions, work ways, and informal traditions that arise within the operating and overseeing groups closely involved with the systems of hazard." Slippery as it may be as a concept, organizational culture is important to understanding real-world questions, such as those that Vaughan (a sociologist by profession and a staff member of the CAIB) enumerates in her article: How do organizations gradually slide into negative patterns? Why do negative patterns persist? Why do organizations fail to learn from mistakes and accidents? Although human and technical failures are important, she finds their root causes in organizational systems. In order to reduce accidents, therefore, organizational systems and their cultures must be studied and understood.

The first two papers in this section concentrate on organizational culture as it relates to accidents in human spaceflight, here restricted to those in NASA's space program. Vaughan focuses on the Space Shuttle *Challenger* and *Columbia* accidents in 1986 and 2003, respectively, while Brown adds the ground-based Apollo 204 (also known as Apollo 1) fire in 1967. Altogether, 17 astronauts were killed in these accidents, triggering massive criticism, investigations, official reports, and personal and organizational soul-searching. Vaughan finds that, due to overly ambitious goals in an organization strapped for resources, NASA's Apollo-era technical culture was turned into a "culture of production" by the time of the *Challenger* accident, a culture that persisted through *Columbia* and was characterized by "cultural mandates for business-like efficiency, production pressures, allegiance to hierarchy, and rule-following." The result was what she calls "the normalization of deviance"—in other words, over time, that which was deviant or anomalous incrementally became redefined as normal, most notably Solid Rocket Booster (SRB) O-ring behavior in cold weather for *Challenger* and foam hits from the External

1. Columbia Accident Investigation Board, *Report* (Washington, DC: NASA and GPO, August 2003), chap. 8. Chapter 8 was largely written by Diane Vaughan.

Tank (ET) to the wing of the Shuttle in the case of *Columbia*. Lack of communication, which she terms "structural secrecy," within layers of NASA administration compounded the problem.

Vaughan believes that the thesis of "history as cause" in the CAIB report demonstrates how the history of decisions made by politicians and by NASA engineers and managers combined twice to produce disaster. She warns that economic strain and schedule pressure still exist at NASA and that in such circumstances, system effects, including accidents, tend to reproduce. It is important to note that it is not possible to prevent all accidents, but, she concludes, the *Challenger* and *Columbia* accidents, with their long incubation periods, were preventable. In her view, reducing the probability of accidents means changing NASA's culture as well as externally imposed expectations and limitations, a difficult and ongoing process, one in which social scientists must play a role in a systematic way.

Brown, a historian of technology in the Science, Technology and Society program at MIT, takes another approach by analyzing the "disjunctures" in the three fatal NASA accidents. In the case of Apollo 204, the disjuncture is between the engineers designing and managing the spacecraft and the technicians manufacturing it. For the two Shuttle accidents, the disjuncture is between managers controlling the Shuttle program and engineers maintaining and analyzing the spacecraft. By way of explaining these disjunctures, he analyzes the three accident reports and relates their styles and conclusions to the engineering practices of NASA and its contractors. Whereas the Apollo 204 report concluded that poor engineering practice was the sole cause of the fire, the Challenger Commission, by contrast, emphasized secondary causes in addition to the technical O-ring failure, including the decision to launch, schedule pressure, and a weak safety system. As emphasized in Vaughan's paper, the *Columbia* report went even further, pointing (partly at her urging) to equal importance for technical and social causes.

Reading the three accident reports to gain historical insights, Brown finds that they suggest a growing separation between management and engineering over the period under review. They reveal an asymmetry assumed by the accident investigators, in the sense that the technical/engineering causes are to be understood as "context-free and ahistorical activity," while management causes are to be understood in a complex historical and cultural framework. Brown therefore asks two questions: what historical processes caused this separation between management and engineering? And what changes in engineering over the quarter century covered by the accident reports might be important for placing engineering in its own historical and cultural context? In answer to the latter, he enumerates three changes: widespread use of computers, changes in engineering education, and the move away from

systems engineering as an organizing philosophy. During the period 1967 to 2003, modeling, testing, and simulation had changed from hand calibration to computer-based calculations, resulting in loss of transparency. For example, Boeing engineers who used a computer model known as "Crater" to predict the effects of foam impacts on the Shuttle were unaware of its limitations precisely because the process had been computerized; this ignorance greatly affected their ability to make engineering judgments. Over the same period, engineering education, which was moving toward science and away from design, rendered engineering more abstract and less connected to reality. The *Challenger* and *Columbia* reports criticized the lack of engineering design expertise in some of the contractors involved. Finally, whereas systems engineering was the guiding philosophy of the space program at the time of the Apollo 204 fire, Total Quality Management and the "faster, better, cheaper" approach replaced system engineering during the 1990s for senior management, while engineers still used the tools of system management.

La Porte takes a broader view, tackling the issues of high-reliability systems that must operate across decades or generations, as NASA must do in planning and implementing its vision to take humans to the Moon and Mars. Drawing on a variety of empirical studies in the social and management sciences, including nuclear power plant operation and waste disposal, he undertakes this analysis of highly reliable operations that take place over decades, and he assumes high levels of public trust over that time. Such long-term operations also involve issues of institutional constancy. He finds, among other things, that high-reliability organizations (HROs) must have technical competence, stringent quality-assurance measures, flexibility and redundancy in operations, decentralized decision-making, and an unusual willingness to reward the discovery and reporting of error without assigning blame. Maintaining an organizational culture of reliability exhibiting these characteristics is difficult, but important. Nor can HROs become overly obsessed with safety; they must strive equally for high levels of production and safety. If the Shuttle never launches, NASA fails its mission in equal measure as it does when it has accidents. La Porte also emphasizes the importance of external "watchers," including congressional committees and investigating boards, to sustaining high-reliability organizations, a factor also evident in Vaughan's and Brown's analyses of the accident reports.

La Porte notes that, for obvious reasons, maintaining these characteristics over long-term, even trans-generational, efforts is the least-understood process in terms of empirical studies. In an attempt to shed light on this problem, he examines the idea of "institutional constancy" and concludes that in order for such long-term efforts to be successful, an agency such as NASA must demonstrate to the public and to Congress that it can be trusted to keep its word long

into the future, and it must "show the capacity to enact programs that are faithful to the original spirit of its commitments." La Porte discusses the characteristics associated with institutional constancy, summarized in his table 13.2. He, too, calls for further empirical and analytical study, especially to delineate requirements for long-term institutional constancy and trustworthiness.

Implicitly or explicitly, these papers also deal with the question of risk. The Challenger Commission found that its managers and engineers understood risk in very different ways, with the engineers seeing it as quantifiable and the managers as flexible and manageable. The Columbia Accident Investigation Board noted similar differences in the perception of risk. La Porte broaches the question of risk averseness and the public's risk-averse demand for very reliable operations of intrinsically hazardous systems. He suggests research on the conditions under which the public would be willing to accept more risk, given that such operations can never be risk-free. NASA's "Risk and Exploration" symposium, held in late 2004 in the midst of the Hubble Space Telescope controversy and with the Shuttle still grounded, came to a similar conclusion: the public needs to be made aware that accidents are not completely preventable.[2]

Nevertheless, the three views in this section, by a sociologist, a historian, and a political scientist, shed important light on NASA cultures and, if one accepts their arguments, on ways to reduce accidents in what inevitably remains a high-risk endeavor. How to balance risk and exploration is the key question.

2. Steven J. Dick and Keith Cowing, *Risk and Exploration: Earth, Sea and Sky* (Washington, DC: NASA SP-2005-4701, 2005).

Chapter 11

Changing NASA: The Challenges of Organizational System Failures

Diane Vaughan

In both the *Columbia* and *Challenger* accidents, NASA made a gradual slide into disaster. The history of decisions about the risk of Solid Rocket Booster O-ring erosion that led to *Challenger* and the foam debris that resulted in *Columbia* is littered with early warning signs that were misinterpreted. For years preceding both accidents, technical experts defined risk away by repeatedly normalizing technical anomalies that deviated from expected performance. The significance of a long incubation period leading up to an accident is that it provides greater opportunity to intervene and to turn things around, avoiding the harmful outcome. But that did not happen. The Columbia Accident Investigation Board's report concluded that NASA's second Shuttle accident resulted from an organizational system failure, pointing out that the systemic causes of *Challenger* had not been fixed.[1] In fact, both disasters were triggered by NASA's organizational system: a complex constellation of factors including NASA's political/economic environment, organization structure, and layered cultures that affected how people making technical decisions assessed risk. These three aspects of NASA's organizational system interacted, explaining the origins of both accidents.

The amazing similarity and persistence of these systemic flaws over the 17 years separating the two accidents raise several questions: How do organizations gradually slide into negative patterns? Why do negative patterns persist? Why do organizations fail to learn from mistakes and accidents? In this chapter, I examine NASA's experience to consider the challenges of changing NASA's organizational system and to gain some new insight into these questions. My data for this analysis are my *Challenger* research, experience as a researcher and writer on the staff of the Columbia Accident Investigation Board, conversations and meetings with NASA personnel at Headquarters and a NASA "Forty Top Leaders Conference" soon after the CAIB report release, and, finally, a content analysis of the two official accident investigation

1. Columbia Accident Investigation Board, *Report* (Washington, DC: NASA and GPO, August 2003).

reports.[2] Summarizing from my testimony before the CAIB, I begin with a brief comparison of the social causes of *Challenger* and *Columbia* to show the systemic causes of both, how the two accidents were similar and different, and how and why NASA twice made an incremental descent into disaster.[3] I then review the conclusions of the Presidential Commission investigating the *Challenge*r accident and their recommendations for change, the changes NASA made, and why those changes failed to prevent the identical mistake from recurring in *Columbia*.[4] Next, I contrast the Commission's findings with those of the CAIB report and discuss the CAIB's recommendations for changing NASA, the direction NASA is taking in making changes, and the challenges the space agency faces in preventing yet a third Shuttle accident.

Robert Jervis, in *System Effects*, considers how social systems work and why so often they produce unintended consequences.[5] He stresses the importance of dense interconnections and how units and relations with others are strongly influenced by interactions at other places and at earlier periods of time. Thus, disturbing a system produces chains of consequences that extend over time and have multiple effects that cannot be anticipated. I will argue in this chapter for the importance of analyzing and understanding the dynamics of organizational system failures and of connecting strategies for change with the systemic causes of problems. The "usual remedy" in the aftermath of a technological accident is to correct the causes of a technical failure and alter human factors that were responsible so that they, too, can be fixed. However, the root causes of both human and technical failure can be found in organizational systems. Thus, remedies targeting only the technology and individual error are insufficient. Neither complacency, negligence, ignorance, poor training, fatigue, nor carelessness of individuals explains why, in the face of increasing in-flight damage, NASA made flawed decisions, continuing to fly. The lessons to be learned from NASA's experience are, first, in order to reduce the potential for gradual slides and repeating negative patterns, NASA and other organizations dealing with risky technologies must go beyond the search for technical causes and individual error and search the full range of social causes located in the organizational system. Second, designing and implementing solutions that are matched to those causes is a crucial but challenging step in preventing a recurrence.

---

2. Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (Chicago: University of Chicago Press, 1996); Diane Vaughan, "History as Cause: *Columbia* and *Challenger*," chap. 8 in Columbia Accident Investigation Board, *Report*; Presidential Commission on the Space Shuttle *Challenger* Accident, *Report to the President by the Presidential Commission on the Space Shuttle Challenger Accident*, 5 vols. (Washington, DC: GPO, 1986).

3. Vaughan, "History as Cause," pp. 185–204.

4. Presidential Commission on the Space Shuttle *Challenger* Accident, *Report to the President*.

5. Robert Jervis, *System Effects: Complexity in Political and Social Life* (Princeton: Princeton University Press, 1997).

NASA's Slippery Slope: O-Rings, Foam Debris, and Normalizing Deviance

In a press conference a few days after the *Columbia* tragedy, NASA's Space Shuttle Program Manager, Ron Dittemore, held up a large piece of foam approximately the size of the one that fatally struck *Columbia* and discounted it as a probable cause of the accident, saying, "We were comfortable with it." Prior to the *Challenger* accident in 1986, that phrase might have been said about O-ring erosion by the person then occupying Dittemore's position. The O-ring erosion that caused the loss of *Challenger* and the foam debris problem that took *Columbia* out of the sky both had a long history. Neither anomaly was permitted by design specifications, yet NASA managers and engineers accepted the first occurrence, then accepted repeated occurrences, concluding after examining each incident that these deviations from predicted performance were normal and acceptable. In the years preceding NASA's two

This photograph of the Space Shuttle *Challenger* accident on 28 January 1986 was taken by a 70-millimeter tracking camera at site 15, south of Pad 39B, at 11:39:16.061 EST. One of the Solid Rocket Boosters can be seen at the top of the view. *(Image no. STS-51L 10181; Kennedy Space Center alternative photo no. is 108-KSC-86PC-147)*

accidents, managers and engineers had normalized recurring technical anomalies—anomalies that, according to design specifications, were not allowed. How—and why—was the normalization of technical deviations possible?

We must avoid the luxuries of retrospection, when all the flawed decisions of the past are clear and can be directly linked to the harmful outcomes, and instead see the events preceding each accident as did the personnel making risk assessments, as the problems unfolded. As managers and engineers were making decisions, continuing to launch under the circumstances they had made sense to them. The immediate social context of decision-making was an important factor. Although NASA treated the Shuttle as if it were an operational vehicle, it was experimental: alterations of design and unpredictable flight conditions led to anomalies on many parts on every mission. Because having anomalies was normal, neither O-ring erosion nor foam debris was the signal of danger it seemed in retrospect. In both cases, engineering decisions were made incrementally, anomaly by anomaly. Accepting the first deviation set a precedent on which future decisions were based. After inspection and analysis, engineers calculated a safety margin that placed initial damage within a safety margin showing that the design could tolerate even more.

In addition, the pattern of information had an impact on how managers and engineers were defining and redefining risk. As the anomalies began to occur, engineers saw signals of danger that were mixed—an anomalous incident would be followed by a mission with none or a reduced level of damage, so they believed they had fixed the problem and understood the parameters of cause and effect. Or signals were weak—incidents that were outside what had become defined as the acceptable parameters were not alarming because their circumstances were so unprecedented that they were viewed as unlikely to repeat. And finally, signals became routine, occurring so frequently that the repeating pattern became a sign that the machine was operating as predicted. The result was the production of a cultural belief that the problems were not a threat to flight safety, a belief repeatedly reinforced by mission success. Both erosion and foam debris were downgraded in official systems categorizing risk over time, institutionalizing the definition of these problems as low-level problems.

Although these patterns are identical in the two accidents, two differences are noteworthy. First, for O-ring erosion, the first incident of erosion occurred on the second Shuttle flight, which was the beginning of problem normalization; for foam debris, the normalization of the technical deviation began *even before the first Shuttle was launched*. Damage to the thermal-protection system—the thousands of tiles on the orbiter to guard against the heat of reentry—was expected due to the forces at launch and during flight, such that replacement of damaged tiles was defined from the design stage as a maintenance problem that had to be budgeted. Thus, when foam debris damage

was observed on the orbiter tiles after the first Shuttle flight in 1981, it was defined as a maintenance problem, not a flight hazard. This early definition of the foam problem as routine and normal perhaps explains a second difference. Before the *Challenger* disaster, engineering concerns about proceeding with more frequent and serious erosion were marked by a paper trail of memos. The foam debris problem history also had escalations in occurrence but showed no such paper trail, no worried engineers.

These decisions did not occur in a vacuum. To understand how these two technical anomalies continued to be normalized, we need to grasp the important role that NASA's political and budgetary environment played and how the history of the Space Shuttle program affected the local situation. Decisions made by leaders in the White House and Congress left the space agency constantly strapped for resources to meet its own sometimes overly ambitious goals. The Agency's institutional history was one of competition and scarcity, which created a "trickle-down effect."[6] Thus, the original, pure technical culture of NASA's Apollo era was reshaped into a *culture of production* that existed at the time of *Challenger* and persisted over 50 launches later, for *Columbia*. NASA's original technical culture was reshaped by new cultural mandates for business-like efficiency, production pressures, allegiance to hierarchy, and rule-following.

This culture of production reinforced the decisions to proceed. Meeting deadlines and schedule was important to NASA's scientific launch imperatives and also for securing annual congressional funding. Flight always was halted to permanently correct other problems that were a clear threat to take the Shuttle out of the sky (a cracked fuel duct to the Space Shuttle main engine, for example), but the schedule and resources could not give way for a thorough hazard analysis of ambiguous, low-lying problems that the vehicle seemed to be tolerating. Indeed, the successes of the program led to a belief that NASA's Shuttle was an operational, not an experimental, system, thus affirming that it was safe to fly. Finally, the fact that managers and engineers obeyed the cultural mandates of hierarchy and protocol reinforced the belief that the anomalies were not a threat to flight safety because NASA personnel were convinced, having followed all the rules, that they had done everything possible to assure mission safety.

Both problems had gone on for years. Why had no one recognized what was happening and intervened, halting NASA's two transitions into disaster? The final piece of the organizational system contributing to both accidents was *structural secrecy*. By this I refer to how organization structure concealed the seriousness of the problems from people with responsibility for technical oversight who might have turned the situation around prior to both

6. Diane Vaughan, "The Trickle-Down Effect: Policy Decisions, Risky Work, and the *Challenger* Accident," *California Management Review* 39 (winter 1997): 1–23.

accidents. Organization structure affected not only the flow of information, a chronic problem in all organizations, but also how that information was interpreted. Neither NASA's several safety organizations nor the four-tiered Flight Readiness Review (FRR), a formal, adversarial, open-to-all structure designed to vet all engineering risk assessments prior to launch, called a halt to flying with these anomalies. Top administrators and regulators alike were dependent upon project groups for engineering information and analysis. As managers and engineers reinterpreted warning signs as weak, mixed, and routine signals, normalizing deviance, that diagnosis was what got passed up the hierarchy. Instead of reversing the pattern of flying with erosion and foam debris, Flight Readiness Review ratified it.

The structure of safety regulation also affected understandings about risk. NASA's internal safety system—both times—a) had suffered safety personnel cuts and de-skilling as more oversight responsibility was shifted to contractors in an economy move and b) was dependent upon the parent organization for authority and funding, so it had no ability to independently run tests that might challenge existing assessments. NASA's external safety panel had the advantage of independence but was handicapped by inspection at infrequent intervals. Unless NASA engineers defined something as a serious problem, it was not brought to the attention of safety personnel. As a result of structural secrecy, the cultural belief that it was safe to fly with these two anomalies prevailed throughout the Agency in the years prior to each of NASA's tragedies.

TWO ACCIDENTS: THE REPRODUCTION OF SYSTEM EFFECTS

I have shown how the organizational system worked in the years preceding both accidents to normalize the technical anomalies: the immediate context of decision-making—patterns of information; the context of multiple problems; mixed, weak, and routine signals—the culture of production, and structural secrecy all interacted in complex ways to neutralize and normalize risk and keep NASA proceeding with missions. To show how NASA's organizational system affected the crucial decisions made immediately before both accidents, I now revisit the unprecedented circumstances that created yet new signals of potential danger: an emergency teleconference held on the eve of the 1986 *Challenger* launch, when worried engineers recommended not launching in unprecedented cold temperatures predicted for the next day, and the events at NASA after the 2003 *Columbia* foam debris strike, when engineers again expressed concerns for flight safety. I selectively use examples of these incidents to show similarities and differences, recognizing that doing so greatly simplifies enormously complicated interactions.[7] An initial difference

7. For details, see Vaughan, *Challenger Launch Decision*, chap. 8; and CAIB, *Report*, chap. 6.

that mattered was the window of opportunity for decision and number of people involved. The *Challenger* teleconference was held prelaunch, involved 34 people in three locations, consuming several hours of one day, the proceedings unknown to others at NASA. *Columbia*'s discussion was postlaunch, with a window of 16 days before reentry, and videos of the foam debris strike were widely circulated, involving people throughout the Agency. They can be called crisis situations only in retrospect because at the time these events were unfolding, many participants did not define it as a crisis situation, which was, in fact, one of the problems.

In both scenarios, people facing unprecedented situations came to the table with a cultural belief in the risk acceptability of O-ring erosion and foam debris based on years of engineering analysis and flight experience. Thus, both the history of decision-making and the history of political and budgetary decisions by elites had system effects. As these selected examples show, the mandates of the culture of production for efficiency, schedule, hierarchy, and protocol infiltrated the proceedings. Also, structural secrecy acted as before, feeding into the tragic outcomes.

- Schedule pressure showed when *Challenger*'s Solid Rocket Booster Project Manager and *Columbia*'s Mission Management Team (MMT) Head, responsible for both schedule and safety, were confronted with engineering concerns. Both managers repeated that preexisting definition of risk, sending to others a message about the desired result. Schedule pressure on managers' thinking also showed when engineers proposed a temperature criterion for *Challenger* that would jeopardize the launch schedule for all launches, and for *Columbia* when obtaining satellite imagery would require the orbiter to change its flight orientation, thus prolonging the mission and likely jeopardizing the timing of an important future launch. Believing the safety of the mission was not a factor, both managers focused on future flights, making decisions that minimized the risk of delay.

- In both cases, hierarchy and protocol dominated; deference to engineering expertise was missing. In the *Challenger* teleconference, unprecedented and therefore open to innovation, participants automatically conformed to formal, prelaunch, hierarchical Flight Readiness Review procedures, placing engineers in a secondary role. The postlaunch *Columbia* Mission Management Team operation, intentionally decentralized to amass information quickly, also operated in a hierarchical, centralized manner that reduced engineering input. Further, engineering attempts to get satellite imagery were blocked for not having followed appropriate protocol. In both cases, norms requiring quanti-

tative data were pushed, rendering engineering concerns insufficient; they were asked to prove that it was unsafe to fly, a reverse of the normal situation, which was to prove it was safe to fly. Engineers animated by concern took the issue to a certain level, then, discouraged and intimidated by management response, fell silent. A difference for *Columbia*: the rule on rule-following was inoperative for management, whose definition of risk was influenced by an "informal chain of command"—one influential person's opinion, not hard data.

- Organization structure created structural secrecy, as people structurally peripheral to the technical issue, either by location or expertise or rank, had information but did not feel empowered to speak up. Thus, critical input was lost to the decision-making. The weakened safety system was silent. No safety representative was told of the *Challenger* teleconference. Present at the *Columbia* MMT meeting but weak in authority, safety personnel interjected no cautions or adversarial challenges; information dependence and organizational dependence gave them no recourse but to follow the management lead.

This overview shows these accidents as the unanticipated consequences of system effects, the causes located in the dynamic connection between three layers of NASA's organizational system:

1) Interaction and the Normalization of Deviance: A history of decision-making in which, incrementally, meanings developed in which the unacceptable became acceptable. The first decisions became a basis for subsequent ones in which technical anomalies—signals of danger—were normalized, creating a cultural belief in the safety of foam and O-ring anomalies.

2) The Culture of Production: History was important in a second way. Historic external political and budgetary decisions had system effects, trickling down through the organization, converting NASA's original, pure technical culture into a culture of production that merged bureaucratic, technical, and cost/schedule/efficiency mandates that, in turn, reinforced decisions to continue flying with flaws.

3) Structural Secrecy: These same external forces affected NASA's organization structure and the structure of the safety system, which in turn affected the interpretation of the problem, so that the seriousness of these two anomalies was, in effect, unknown to those in a position to intervene. Instead, before the crisis events immediately preceding

> the accidents, a consensus about these anomalies existed, including among agents of social control—top administrators and safety personnel—who failed to intervene to reverse the trend.

With these systemic social causes in mind, I now turn to the problem of repeating negative patterns and learning from mistake by considering the "Findings" and "Recommendations" of the report of the Presidential Commission on the Space Shuttle *Challenger* Accident, NASA's changes in response, and why the changes NASA implemented failed to prevent a second tragedy.[8]

The Presidential Commission: Connecting Causes and Strategies for Control

Published in June 1986, the Presidential Commission's report followed the traditional accident investigation format of prioritizing the technical causes of the accident and identifying human factors as "contributing causes," meaning that they were of lesser, not equal, importance. NASA's organizational system was not attributed causal significance. However, the report was pathbreaking in the amount of its coverage of human factors, going well beyond the usual focus on individual incompetence, poor training, negligence, mistake, and physical or mental impairment.

Chapters 5 and 6 examine decisions about the O-ring problems, adhering to the traditional human factors/individual failure model. Chapter 5, "The Contributing Cause of the Accident," examines the controversial eve-of-the-launch teleconference. A "flawed decision making process" is cited as the primary causal agent. Managerial failures dominate the empirical "Findings": the teleconference was not managed so that the outcome reflected the opposition of many contractor engineers and some of NASA's engineers; managers in charge had a tendency to solve problems internally, not forwarding them to all hierarchical levels; the contractor reversed its first recommendation for delay "at the urging of Marshall [Space Flight Center] . . . to accommodate a major customer."[9]

Chapter 6, "An Accident Rooted in History," chronicled the history of O-ring decision-making in the years preceding the teleconference. Again, the empirical Findings located cause in individual failures.[10] Inadequate testing was done; neither the contractor nor NASA understood why the O-ring anomalies were happening; escalated risk-taking was endemic, apparently "because they got away with it the last time"; in a thorough review at Headquarters in 1985, information "was sufficiently detailed to require corrective action prior

8. Presidential Commission on the Space Shuttle *Challenger* Accident, *Report to the President*.
9. Ibid., p. 104.
10. Ibid., p. 148.

to the next flight"; managers and engineers failed to carefully analyze flight history, so data were not available on the eve of *Challenger*'s launch to properly evaluate the risks.[11] The system failure cited was in the anomaly tracking system, which permitted flight to continue despite erosion, with no record of waivers or launch constraints, and paid attention only to anomalies "outside the data base."

Both chapters described decision-making, focusing on interaction, but did not explain why decisions were made as they were. Chapter 7, "The Silent Safety Program," turned to organizational matters, initially addressing them in the traditional accident investigation frame. The Commission noted the failures: "lack of problem reporting requirements, inadequate trend analysis, misrepresentation of criticality and lack of involvement in critical discussions."[12] For example, they found so many problems listed on NASA's Critical Items List that the number reduced the seriousness of each. Acknowledging that top administrators were unaware of the seriousness of the O-ring problems, the Commission labeled the problem a "communication failure," thus deflecting attention from organization structure as a cause of the problems. In evaluating NASA's several safety offices and panels, however, the Commission made a break with the human factors approach by addressing the structure of regulatory relations. The Commission found that in-house safety programs were dependent upon the parent organization for funding, personnel, and authority. This dependence showed when NASA reduced the safety workforce even as the flight rate increased. In another economy move, NASA had increased reliance upon contractors, relegating many NASA technical experts to safety oversight of contractor activities, becoming dependent on contractors rather than retaining safety control in-house.

In chapter 8, "Pressures on the System," the Commission took an unprecedented step by examining schedule pressure and its effects on the NASA organization. However, this pressure, according to the report, was NASA-initiated, with no reference to external demands or restrictions on the Agency that might have contributed to it. The fault rested with NASA's own leaders. "NASA began a planned acceleration of the Space Shuttle launch schedule . . . . In establishing the schedule, NASA had not provided adequate resources for its attainment. As a result, the capabilities of the system were strained . . . ."[13] The system being analyzed is the flight production system: all the processes that must be engaged and completed in order to launch a mission. The report states that NASA declared the Shuttle "operational" after the fourth experimental flight even though the Agency was not prepared to meet the demands of an

11. Ibid., p. 148.
12. Ibid., p. 152.
13. Ibid., p. 164.

operational schedule. This belief in operational capability, according to the Commission, was reinforced by NASA's history of 24 launches without a failure prior to *Challenger* and to NASA's legendary "can-do" attitude, in which the space agency always rose to the challenge, draining resources away from safety-essential functions to do it.[14]

Next consider the fit between the Commission's "Findings," above, and their "Recommendations" for change, summarized as follows.[15] Many of the changes, if properly implemented, would reduce structural secrecy. The Commission mandated a review of Shuttle Management Structure because Project Managers felt more accountable to their Center administration than the Shuttle Program Director, thus vital information bypassed Headquarters. The Commission targeted "poor communications" by mandating that NASA eliminate the tendency of managers not to report upward, "whether by changes of personnel, organization, indoctrination or all three"; develop rules regarding launch constraints; and record Flight Readiness Reviews and Mission Management Team Meetings. Astronauts were to be brought into management to instill a keen awareness of risk and safety.[16]

Centralizing safety oversight, a new Shuttle Safety Panel would report to the Shuttle Program Manager. It would attend to Shuttle operations, rules and requirements associated with launch decisions, flight readiness, and risk management. Also, an independent Office of Safety, Reliability and Quality Assurance would be established, headed by an Associate NASA Administrator, with direct authority over all safety bodies throughout the Agency, and reporting to the NASA Administrator. With designated funding to give it independence, SR&QA would direct reporting and documentation of problems and trends affecting flight safety. Last, but by no means least, to deal with schedule pressures, the Commission recommended that NASA establish a flight rate that was consistent with its resources.

These were the official lessons to be learned from *Challenger.* The Commission's "Findings" and "Recommendations," in contrast to those later forthcoming from the CAIB, were few and very general, leaving NASA considerable leeway in how to implement them. How did the space agency respond? At the interaction level, NASA addressed the flawed decision-making by following traditional paths of changing policies, procedures, and processes that would increase the probability that signals of danger would be recognized. NASA used the opportunity to make changes to "scrub the system totally." The Agency rebaselined the Failure Modes Effects Analysis. All problems tracked by the Critical Items List were reviewed, engineering

14. Ibid., pp. 171–177.
15. Ibid., pp. 198–201.
16. Ibid., p. 200.

fixes implemented when possible, and the list reduced. NASA established Data Systems and Trend Analysis, recording all anomalies so that problems could be tracked over time. Rules were changed for Flight Readiness Review so that engineers, formerly included only in the lower-level reviews, could participate in the entire process. Astronauts were extensively incorporated into management, including participation in the final prelaunch Flight Readiness Review and signing the authorization for the final mission "go."

At the organizational level, NASA made several structural changes, centralizing control of operations and safety.[17] NASA shifted control for the Space Shuttle program from Johnson Space Center in Houston to NASA Headquarters in an attempt to replicate the management structure at the time of Apollo, thus striving to restore communication to a former level of excellence. NASA also initiated the recommended Headquarters Office of Safety, Reliability and Quality Assurance (renamed as Safety and Mission Assurance), but instead of the direct authority over all safety operations, as the Commission recommended, each of the Centers had its own safety organization, reporting to the Center Director.[18] Finally, NASA repeatedly acknowledged in press conferences that the Space Shuttle was and always would be treated as an experimental, not operational, vehicle and vowed that henceforth, safety would take priority over schedule in launch decisions. One step taken to achieve this outcome was to have an astronaut attending Flight Readiness Reviews and participating in decisions about Shuttle readiness for flight; another was an effort to bring resources and goals into alignment.

Each of these changes addressed causes identified in the report, so why did the negative pattern repeat, producing the *Columbia* accident? First, the Commission did not identify all the social causes of the accident. From our post-*Columbia* position of hindsight, we can see that the Commission did not target NASA's institutional environment as a cause. The powerful actors whose actions precipitated "Pressures on the System" by their policy and budgetary decisions do not become part of the contributing-cause scenario. NASA is obliged to bring resources and goals into alignment, although resources are determined externally. NASA took the blame for safety cuts, which were attributed to NASA's own "perception that less safety, reliability and quality assurance activity would be required during 'routine' Shuttle operations."[19] The external budgetary actions that forced NASA leaders to impose such efficiencies were not mentioned. Most of the Commission's recommended changes aimed at the organization itself, in particular, changing interactions

17. CAIB, *Report*, p. 101.

18. Ibid.

19. Presidential Commission on the Space Shuttle *Challenger* Accident, *Report to the President*, p. 160.

structure. The Commission did not name culture as a culprit, although production pressure is the subject of an entire chapter. Also, NASA's historic "can-do" attitude (a cultural attribute) is not made part of the "Findings" and "Recommendations." Thus, NASA was not sensitized to possible flaws in the culture or that action needed to be taken. The Commission did deal with the problem of structural secrecy; however, in keeping with the human factors approach, the report ultimately places responsibility for "communication failures" not with organization structure, but with the individual middle managers responsible for key decisions and inadequate rules and procedures. The obstacles to communication caused by hierarchy and consequent power that managers wielded over engineers, stifling their input in crucial decisions, are not mentioned. These obstacles originate in organization structure but become part of the culture.

Second, consider NASA's response to these "Recommendations" and the challenges they faced. Although NASA's own leaders played a role in determining goals and how to achieve them, the institutional environment was not in their control. NASA remained essentially powerless as a government agency dependent upon political winds and budgetary decisions made elsewhere. Thus, NASA had little recourse but to try to achieve its ambitious goals—necessary politically to keep the Agency a national budgetary priority—with limited resources. The intra-organizational changes that NASA did control were reviewed in the CAIB report.[20] It found that many of NASA's initial changes were good. However, a critical one—the structural changes to centralize safety—was not enacted as the Commission had outlined. NASA's new Headquarters Office of Safety, Reliability and Quality Assurance did not have direct authority, as the Commission mandated; further, the various Center safety offices in its domain remained dependent because their funds came from the activities that they were overseeing.[21]

The CAIB also found that other changes—positive changes—were undone by subsequent events stemming from political and budgetary decisions made by the White House and Congress. The new, externally imposed goal of the International Space Station (ISS) forced the Agency to mind the schedule and perpetuated an operational mode. As a consequence, the culture of production was unchanged; the organization structure became more complex. This structural complexity created poor systems integration; communication paths were not clear. Also, the initial surge in post-*Challenger* funding was followed by cuts, such that the new NASA Administrator, Daniel Golden, introduced new efficiencies and smaller programs with the slogan "faster, better, cheaper." As a result of the squeeze, the initial increase in NASA safety

20. CAIB, *Report*.
21. Ibid., pp. 101, 178–179.

personnel was followed by a repeat of pre-accident economy moves that again cut safety staff and placed even more responsibility for safety with contractors. The accumulation of successful missions (defined as flights returned without accident) also reproduced the belief in an operational system, thus legitimating these cuts: Fewer resources needed to be dedicated to safety. The loss of people and subsequent transfer of safety responsibilities to contractors resulted in a deterioration of post-*Challenger* trend analyses and other NASA safety oversight capabilities.

NASA took the report's mandate to make changes as an opportunity to make others it deemed necessary, so the number of changes actually made is impossible to know and assess, much less report in a chapter of this length. The extent to which additional changes might have become part of the problem rather than contributing to the solution is also unknown. Be aware, however, that we are assessing these changes from the position of post-*Columbia* hindsight, tending to identify all the negatives associated with the harmful outcome.[22] The positive effects, the mistakes avoided by post-*Challenger* changes,

The 13-member Columbia Accident Investigation Board poses for a group photo taken in the CAIB boardroom. The official STS-107 insignia hangs on the wall in the center of the boardroom. From left to right, seated, are Board members G. Scott Hubbard, Dr. James N. Hallock, Dr. Sally Ride, Chairman Admiral Hal Gehman (ret.), Steven Wallace, Dr. John Logsdon, and Dr. Sheila Widnall. Standing, from left to right, are Dr. Douglas D. Osheroff, Major General John Barry, Rear Admiral Stephen Turcotte, Brigadier General Duane Deal, Major General Kenneth W. Hess, and Roger E. Tetrault. *(CAIB photo by Rick Stiles, 2003)*

22. William H. Starbuck, "Executives' Perceptual Filters: What They Notice and How They Make Sense," in *The Executive Effect*, ed. Donald C. Hambrick (Greenwich, CT: JAI, 1988).

tend to be lost in the wake of *Columbia*. However, we do know that increasing system complexity increases the probability of mistake, and some changes did produced unanticipated consequences. One example was NASA's inability to monitor reductions in personnel during a relocation of Boeing, a major contractor, which turned out to negatively affect the technical analysis Boeing prepared for NASA decision-making about the foam problem.[23] Finally, NASA believed that the very fact that many changes had been made had so changed the Agency that it was completely different from the NASA that produced the *Challenger* accident. Prior to the CAIB report release, despite the harsh revelations about organizational flaws echoing *Challenger* that the CAIB investigation frequently released to the press, many at NASA believed no parallels existed between *Columbia* and *Challenger.*[24]

The CAIB: Connecting Causes with Strategies for Control

Published in August 2003, the Columbia Accident Investigation Board report presented an "expanded causal model" that was a complete break with accident investigation tradition. Turning from the usual accident investigation focus on technical causes and human factors, the CAIB fully embraced an organizational systems approach and was replete with social science concepts. Further, it made the social causes equal in importance to the technical causes, in contrast to the Commission's relegation of nontechnical causes to "contributing causes." Part 1 of the CAIB report, "The Accident," addressed the technical causes; part 2, "Why the Accident Occurred," examined the social causes; part 3 discussed the future of spaceflight and recommendations for change.

In the executive summary, the CAIB report articulated both a "technical cause statement" and an "organizational cause statement." On the latter, the Board stated that it "places as much weight on these causal factors as on the more easily understood and corrected physical cause of the accident."[25] With the exception of the "informal chain of command" operating "outside the organization's rules," this organizational cause statement applied equally to *Challenger*:

> The organizational causes of this accident are rooted in the Space Shuttle Program's history and culture, including the

23. CAIB, *Report*.

24. Michael Cabbage and William Harwood, *CommCheck . . . The Final Flight of Shuttle Columbia* (New York: Free Press, 2004), p. 203.

25. CAIB, *Report*, p. 9.

> original compromises that were required to gain approval for the Shuttle, subsequent years of resource constraints, fluctuating priorities, schedule pressures, mischaracterization of the Shuttle as operational rather than developmental, and lack of an agreed national vision for human space flight. Cultural traits and organizational practices detrimental to safety were allowed to develop, including reliance on past success as a substitute for sound engineering practices (such as testing to understand why systems were not performing in accordance with requirements); organizational barriers that prevented effective communication of critical safety information and stifled professional differences of opinion; lack of integrated management across program elements; and the evolution of an informal chain of command and decision-making processes that operated outside the organization's rules.[26]

The part 2 chapters described system effects. In contrast to the Commission's report, the CAIB explained NASA actions as caused by social factors. Chapter 5, "From *Columbia* to *Challenger*," began part 2 with an analysis of NASA's institutional environment. Tracking historic decisions by leaders in NASA's political and budgetary environment and the effect of policy decisions on the Agency after the first accident, it showed how NASA's external environment caused internal problems by shaping organization culture: the persistence of NASA's legendary can-do attitude, excessive allegiance to bureaucratic proceduralism and hierarchy due to increased contracting out, and the squeeze produced by "an agency trying to do too much with too little" as funding dropped so that downsizing and sticking to the schedule became the means to all ends.[27] The political environment continued to produce pressures for the Shuttle to operate like an operational system, and NASA accommodated. Chapter 6, "Decision Making at NASA," chronicled the history of decision-making on the foam problem, showing how the weak, mixed, and routine signals behind the normalization of deviance prior to *Challenger* also precipitated NASA's second gradual slide into disaster. Chapter 6 presented evidence that schedule pressure directly impacted management decision-making about the *Columbia* foam debris hit. Also, it showed how NASA's bureaucratic culture, hierarchical structure, and power differences created missing signals, so that the depth of engineer concerns and logic of their request for imagery were not admitted to poststrike deliberations.

26. Ibid.
27. Ibid., pp. 101–120.

Chapter 7, "The Accident's Organizational Causes," stepped back from the reconstruction of the decision history to examine how the organizational context affected the decisions traced in chapter 6. The chapter set forth an analysis of NASA's organizational culture and structure. The focal point was the "broken safety culture" that resulted from a weakened safety structure that, in turn, caused decision-makers to "miss the signals the foam was sending."[28] Organization structure, not communication failure, was responsible for problems with conveying and interpreting information. Systems integration and strong independent NASA safety systems were absent. Incorporating the social science literature from organization theory, theories of risk, and accidents, this chapter surveyed alternative models of organizations that did risky work, posing some safety structures that NASA might consider as models for revamping the Agency. Then, in the conclusion, it connected these organizational factors with the trajectory of decision-making after the *Columbia* foam strike. Chapter 8, "History as Cause: *Columbia* and *Challenger*," compared the two accidents. By showing the repeating patterns, it established the second accident as an organizational system failure, making obvious the causal links within and between the three preceding chapters. It demonstrated that the causes of *Challenger* had not been fixed. By bringing forward the thesis of "history" as cause, it showed how both the history of decision-making by political elites and the history of decision-making by NASA engineers and managers had twice combined to produce a gradual slide into disaster.

Now consider the fit between the Board's expanded causal model and its "Findings" and its "Recommendations." Empirically, the CAIB found the same problems as did the Presidential Commission and in fact recognized that in the report: schedule pressure; dependent and understaffed safety agents; communication problems stemming from hierarchy, power differences, and structural arrangements; poor systems integration and a weakened safety system; overburdened problem-reporting mechanisms that muted signals of potential danger; a can-do attitude that translated into an unfounded belief in the safety system; a success-based belief in an operational system; and bureaucratic rule-following that took precedence over deference to the expertise of engineers.[29] The data interpretation and causal analysis differed, however, because the CAIB report integrated social science analysis and concepts throughout part 2: culture, institutional failure, organizational system, history as cause, structure, the normalization of deviance, and the causal linkages between the three empirical chapters. Thus, the CAIB targeted for change each of the three layers of NASA's organizational system. A second difference

28. Ibid., p. 164.
29. Ibid., p. 100.

was that the number of findings and recommendations was greater and each was more detailed and specific than those of the Commission. A few of those illustrative of the organization system approach to change follow.

Chapter 5, "From *Challenger* to *Columbia*," tracing historic decisions by leaders, included neither findings nor recommendations about NASA's external environment. However, in contrast to the Commission's report, the CAIB specifically implicated decision leaders by the data in chapter 5, and in the introduction to part 2, the CAIB report stated that the Agency

> accepted the bargain to operate and maintain the vehicle in the safest possible way. The Board is not convinced that NASA has completely lived up to the bargain, or that Congress and the Administration have provided the funding and support necessary for NASA to do so. This situation needs to be addressed—if the nation intends to keep conducting human space flight, it needs to live up to its part of the bargain.[30]

Policy and budgetary decisions by leaders again show up in the "Findings" and "Recommendations" in chapters 6 and 7. Chapter 6, "Decision Making at NASA," makes three Recommendations, primary among them the adoption of "a Shuttle flight schedule that is consistent with available resources."[31] Also, it advocated training the Mission Management Team, which did not operate in a decentralized mode or innovate, instead adhering to an ill-advised protocol in dealing with the foam strike. As Weick found with forest-fire fighters in a crisis, the failure "to drop their tools," which they were trained to always carry, resulted in death for most.[32] The CAIB recommendation was to train NASA managers to "drop their tools," responding innovatively rather than bureaucratically to uncertain flight conditions and to decentralize by interacting across levels of hierarchy and organizational boundaries.[33]

Chapter 7, "The Accident's Organizational Causes," asserts the important causal role of a broken safety culture and NASA's cultural "blind spot" that kept them from getting the signals the foam was sending. The "Recommendations" advocated changes in the structure of NASA's safety system: the broken safety culture was to be fixed by changing the safety structure. The Commission charged NASA to create an "independent Technical Engineering Authority" with complete authority over technical issues, its independence guaranteed by funding directly from NASA Headquarters, with no responsibility for sched-

30. CAIB, *Report*, p. 97.

31. Ibid., p. 139.

32. Karl E. Weick, "The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster," *Administrative Science Quarterly* 38 (1993): 628–652.

33. CAIB, *Report*, p. 172.

ule or program cost.[34] After *Challenger*, cost, schedule, and safety were all the domain of a single office. Second, NASA Headquarters' Office of Safety and Mission Assurance would have direct authority and be independently resourced. Finally, to assure that problems on one part of the Shuttle (e.g., the foam debris from the External Tank) took into account ramifications for other parts (e.g., foam hitting the orbiter wing), the Space Shuttle Integration Office would be reorganized to include the orbiter, previously not included.

Chapter 8, "History as Cause," presented general principles for making changes, rather than concrete recommendations. These principles incorporate the three layers of NASA's organizational system and the relationship between them. First, decision-making patterns that normalize deviance should be altered by "strategies that increase the clarity, strength, and presence of signals that challenge assumptions about risk," which include empowering engineers, changing managerial practices, and strengthening the safety system.[35] Second, this chapter reiterates the accountability at higher levels, stating, "The White House and Congress must recognize the role of their decisions in this accident and take responsibility for safety in the future."[36] Later and more specifically, "Leaders create culture. It is their responsibility to change it . . . . The past decisions of national leaders—the White House, Congress, and NASA Headquarters—set the *Columbia* accident in motion by creating resource and schedule strains that compromised the principles of a high-risk technology organization."[37] Third, at the organizational level, culture and structure are both targets for change. Understanding culture should be an ongoing research-based project. Necessary changes to organization structure must be carefully considered because of the law of unintended consequences: change and increased complexity produce mistake; changing structure can change culture in unpredictable ways.

The report made it imperative that NASA respond to many of these recommendations prior to the Return to Flight Evaluation in 2005.[38] Although change is still under way at NASA, it is appropriate to examine the direction NASA is taking and the obstacles the Agency is encountering as it goes about implementing change.

Signals of Danger and the Normalization of Deviance

Because the Space Shuttle is and always will be an experimental vehicle, technical problems will proliferate. In such a setting, categorizing risk will

34. Ibid., p. 193.
35. Ibid., p. 203.
36. Ibid., p. 196.
37. Ibid., p. 203.
38. Prior to the resumption of Shuttle launches, progress on these changes was monitored and approved by a NASA-appointed board, the Covey-Stafford Board, and also by the U.S. Congress House Committee on Science, which has official oversight responsibilities for the space agency.

always be difficult, especially with low-lying, ambiguous problems, like foam debris and O-ring erosion, where the threat to flight safety is not readily apparent and mission success constitutes definitive evidence: calculations and lab experiments are approximations, but flight outcome is considered the final test of engineering predictions. The decision problem is not only how to categorize the many elements and variations in risk, but how to make salient early warning signs about low-lying problems that, by definition, will be seen against a backdrop of more serious problems.

The new NASA Engineering and Safety Center (NESC), created after the *Columbia* accident, is to be a safety resource for engineering decisions throughout the Agency. NESC will review recurring anomalies that engineering had determined do not affect flight safety to see if those decisions were correct.[39] Going back to the start of the Shuttle program, NESC will create a common database, looking for missed signals, reviewing problem dispositions, and taking further investigative and corrective action when deemed necessary. However, as we have seen from *Columbia* and *Challenger,* what happens at the level of everyday interaction, interpretation, and decision-making does not occur in a vacuum, but in an organizational system in which other factors affect problem definition, corrective actions, and problem dispositions.

The Culture of Production: NASA's Political/Economic Environment

NASA remains a politically vulnerable agency, dependent on the White House and Congress for its share of the budget and approval of its goals. After *Columbia*, the Bush administration supported the continuation of the Space Shuttle program and supplied the vision for NASA's future that the CAIB report concluded was missing: the space program would return to exploration of Mars. However, the funds to make the changes required for the Shuttle to return to flight and simultaneously accomplish this new goal were insufficient. Thus, NASA, following the CAIB prescription, attempted to align goals and resources by phasing out the Hubble telescope program and, eventually, planning to phase out the Shuttle itself. Further, during the standdown from launch while changes are implemented, the International Space Station is still operating and remains dependent upon the Shuttle to ferry astronaut crews, materials, and experiments back and forth in space. Thus, both economic strain and schedule pressure still persist at NASA. How the conflict between NASA's goals and the constraints upon achieving them will unfold is still unknown, but one lesson from *Challenger* is that system effects tend to reproduce. The Board mandated independence and resources for the safety system, but when

39. Frank Morring, Jr., "Anomaly Analysis: NASA's Engineering and Safety Center Checks Recurring Shuttle Glitches," *Aviation Week & Space Technology* (2 August 2004): 53.

goals, schedule, efficiency, and safety conflicted post-*Challenger*, NASA goals were reined in, but the safety system also was compromised.

The Organization: NASA Structure and Culture

In the months preceding the report release, the Board kept the public and NASA informed of some of the recommended changes so that NASA could get a head start on changes required for Return to Flight. With the press announcement that the CAIB would recommend a new safety center, and pressed to get the Shuttle flying again, NASA rushed ahead to begin designing a center despite having no details about what it should entail. When the report was published, NASA discovered that the planned NASA Engineering and Safety Center (NESC) it had designed and begun to implement was not the Independent Technical Authority that the Board recommended. Converting to the CAIB-recommended structure was resisted internally at NASA, in large part because the proposed structure a) did not fit with insiders' ideas about how things should work and where accountability should lie and b) was difficult to integrate into existing operations and structures. NESC is in operation, as described above, but NASA is now working on a separate organization, the Independent Technical Authority, as outlined by the CAIB.

Whereas CAIB recommendations for changing structure were specific, CAIB directions for changing culture were vague. The CAIB was clear about implicating NASA leaders, making them responsible for changing culture. What was the role of NASA leaders in cultural change, and how should that change be achieved? The report's one clear instruction for making internal change was for correcting the broken safety culture by changing the structure of the safety system. From my participation in meetings at NASA, it was clear that NASA leaders did not understand how to go about changing culture. To these leaders, who were trained in engineering and accustomed to human factors analysis, changing culture seemed "fuzzy." Many NASA personnel believed that the report's conclusion about Agencywide cultural failures wrongly indicted parts of NASA that were working well. More fundamentally, they had a problem translating the contents of the report to identify what changes were necessary and what actions they implied. Each of the three causal chapters contained explicit information about where necessary cultural changes were needed:

1) Chapter 5 shows actions by leaders in OMB, Congress, the White House, and NASA made cost and schedule a part of the organization culture, competing with safety and technical and scientific innovation as goals.

2) Chapter 6 shows how the technical anomaly became normalized, experience with the foam debris problem leading to a cultural belief that foam was not a threat to flight safety.

3) Chapter 7 points out a gap; administrators' belief in NASA's strong "safety culture" was contradicted by the way the organization actually operated in this accident. Layers of structure, hierarchy, protocol, power differences, and an informal chain of command in combination stifled engineering opinion and actions, impeding information gathering and exchange, showing a culture where deference to engineering technical expertise was missing. The belief that operations were safe led NASA to buy as much safety as they felt they needed; cutbacks were made in safety personnel accordingly.

So changes that targeted the cause of NASA's cultural problems had to be three-pronged. But how to do it? NASA's approach was this: On 16 December 2003, NASA Headquarters posted a Request for Proposals on its Web site for a cultural analysis to be followed by the implementation of activities that would eliminate cultural problems identified as detrimental to safety. Verifying the CAIB's conclusions about NASA's deadline-oriented culture, proposals first were due 6 January; then the deadline was extended by a meager 10 days. Ironically, the CAIB mandate to achieve cultural change itself produced the very production pressure about which the report had complained. Although the study was to last three years, NASA required data on cultural change in six months (just in time for the originally scheduled date of the Return to Flight Evaluation, later deferred several times), then annually.

The bidders were corporate contractors with whom NASA frequently worked. Details are not available at this writing, but the awardee conducted a "cultural analysis" survey to gather data on the extent and location of cultural problems in the Agency. The ability of a survey to tap into cultural problems is questionable because it asks insiders, who can be blinded to certain aspects of their culture. A better assessment results when insider information is complemented by outside observers who become temporary members, spending sufficient time there to be able to identify cultural patterns, examine records, and interview asking open-ended questions. A further problem is implied in the initial response rate of 40 percent, indicating that insider viewpoints tapped will not capture Agencywide cultural patterns. Further, this survey was to be followed by plans to train and retrain managers to listen and decentralize and to encourage engineers to speak up. Thus, the Agency response would be at the interactional level only, leaving other aspects of culture identified in the CAIB report—such as goals; schedule pressures; power distribution across the hierarchy and between administrators, managers, and engineers—unaddressed. The agency that had always been expected to do too much with too little was still struggling with that all-too-familiar situation.

Conclusion: Lessons Learned

The dilemmas of slippery slopes, repeating negative patterns, and learning from mistake are not uniquely NASA's. We have evidence that slippery slopes are frequent patterns in manmade disasters.[40] We also know that slippery slopes with harmful outcomes occur in other kinds of organizations where producing and using risky technology is not the goal: think of the incursion of drug use into professional athletics, U.S. military abuse of prisoners in Iraq, and Enron—to name some sensational cases in which incrementalism, commitment, feedback, cultural persistence, and structural secrecy seem to have created an organizational "blind spot" that allowed actors to see their actions as acceptable and conforming, perpetuating a collective incremental descent into poor judgment. Knowing the conditions that cause organizations to make a gradual downward slide, whether the manmade disasters that result are technical, political, financial, public relations, moral, or other, does give us some insight into how it happens that may be helpful to other managers hoping to avoid these problems.

In contradiction to the apparent suddenness of their surprising and sometimes devastating public outcomes, mistakes can have a long incubation period. How do early warning signs of a wrong direction become normalized? A first decision, once taken and met by either success or no obvious failure (which also can be a success!), sets a precedent upon which future decisions are based. The first decision may be defined as entirely within the logic of daily operations because it conforms with ongoing activities, cultural norms, and goals. Or, if initially viewed as deviant, the positive outcome may neutralize perceptions of risk and harm; thus, what was originally defined as deviant becomes normal and acceptable as decisions that build upon the precedent accumulate. Patterns of information bury early warning signs amidst subsequent indicators that all is well. As decisions and their positive result become public to others in the organization, those making decisions become committed to their chosen line of action, so reversing direction—even in the face of contradictory information—becomes more difficult.

The accumulating actions assume a taken-for-granted quality, becoming cultural understandings, such that newcomers may take over from others without questioning the status quo; or, if objecting because they have fresh eyes that view the course of actions as deviant, they may acquiesce and participate upon learning the decision logic and that "this is the way we do it here." Cultural beliefs persist because people tend to make the problematic nonprob-

40. Barry M. Turner, *Man-made Disasters* (London: Wykeham, 1978); Scott A. Snook, *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq* (Princeton: Princeton University Press, 2000).

lematic by defining a situation in a way that makes sense of it in cultural terms. NASA's gradual slides continued because 1) the decisions made conformed to the mandates of the dominating culture of production and 2) because organization structure impeded the ability of those with regulatory responsibilities—top administrators, safety representatives—to critically question and intervene.

Why do negative patterns repeat? Was it true, as the press concluded after *Columbia*, that the lessons of *Challenger* weren't learned? When we examined the lessons of *Challenger* identified in the "Findings" and "Recommendations" of the Commission's 1986 report, they located cause primarily in individual mistakes, misjudgments, flawed analysis, flawed decision-making, and communication failures. The findings about schedule pressures and safety structure were attributed also to flawed decision-making, not by middle managers but by NASA leaders. In response, the Commission recommended adjusting decision-making processes, creating structural change in safety systems, and bringing goals and resources into alignment. NASA acted on each of those recommendations; thus, we could say that the lessons were learned. The *Columbia* accident and the CAIB report that followed taught different lessons, however. They showed that an organizational system failure, not individual failure, was behind both accidents, causing the negative pattern to repeat. So, in retrospect, we must conclude that from *Challenger* NASA learned incomplete lessons. Thus, they did not connect their strategies for control with the full social causes of the first accident.

Events since *Columbia* teach an additional lesson: we see just how hard it is to learn and implement the lessons of an organization system failure, even when the CAIB Report pointed them out. Further, there are practical problems. NASA leaders had difficulty integrating new structures with existing parts of the operation; cultural change and how to go about it eluded them. Some of the CAIB recommendations for change were puzzling to NASA personnel because they had seen their system working well under most circumstances. Further, understanding how social circumstances affect individual actions is not easy to grasp, especially in an American ethos in which both success and failure are seen as the result of individual action.[41] Finally, negative patterns can repeat because making changes has system effects that can produce unintended consequences. Changing structure can increase complexity and, therefore, the probability of mistake; it can change culture in unpredictable ways.[42]

41. After a presentation in which I translated the cultural change implications of the CAIB report to a group of administrators at NASA Headquarters, giving examples of how to go about it, two administrators approached me. Drawing parallels between the personalities of a *Columbia* engineer and a *Challenger* engineer who both acted aggressively to avert an accident but, faced with management opposition, backed off, the administrators wanted to know why replacing these individuals was not the solution.

42. Charles B. Perrow, *Normal Accidents* (New York: Basic Books, 1994); Diane Vaughan, "The Dark Side of Organizations: Mistake, Misconduct, and Disaster," *Annual Review of Sociology* 25

continued on the next page

Even when the lessons are learned, negative patterns can still repeat. The process and mechanisms behind the normalization of deviance make incremental change hard to detect until it's too late. Change occurs gradually, the signs of a new and possibly harmful direction occurring one at a time, injected into daily routines that obfuscate the developing pattern. Moreover, external forces are often beyond a single organization's ability to control. Cultures of production, whether production of police statistics, war, profits, or timely Shuttle launches, are a product of larger historical, cultural, political, ideological, and economic institutions that produce them. Making organizational change that contradicts them is difficult to implement but, in the face of continuing and consistent institutional forces, even more difficult to sustain as time passes. The extent to which an organization can resist these conditions is likely to vary as its status and power vary. Although compared to some, NASA seems a powerful government agency, its share of the federal budget is small compared to other agencies. In the aftermath of both accidents, NASA changes were undermined by subsequent events, many of which they could not control. Political and budgetary decisions of elites created new goals, resulting in new structures, making the system more complex; by not giving sufficient support, they reproduced a culture dominated by schedule pressures, deadlines, resource scarcity, bureaucratic protocols, and power differences that made it difficult to create and sustain a different kind of NASA where negative patterns do not repeat. It may be argued that under the circumstances, NASA's Space Shuttle program has had a remarkable safety record.

But even when everything possible is done, we cannot have mistake-free organizations because system effects will produce unanticipated consequences. Because the Shuttle is unprecedented and flight conditions unpredictable, NASA will always have many postflight anomalies to deal with, and low-lying problems with hard-to-decipher, uncertain outcomes like O-ring erosion and foam debris will always be a challenge. Part of the remedy is to increase the power and effectiveness of the safety system, but the critical piece to this puzzle is changing the culture of production. For *Columbia*, as for *Challenger*, resources—both time and money—were not available for thorough hazard analysis to fully explore why these two technical problems were occurring and the implications of continuing to fly with flaws. The reason they were not thoroughly analyzed and fixed was that the level of risk assigned to these problems was low. The definition of risk precluded the dedication of time and money to problems that had no clear potential for high costs. Further, all contingencies can never be predicted; most people don't understand how social

continued from the previous page
(1999): 271–305; Diane Vaughan, "Organisational Rituals of Risk and Error," in *Organisational Encounters with Risk*, ed. Bridget M. Hutter and Michael K. Power (Cambridge: Cambridge University Press, 2005).

context affects individual action and so cannot create strategies of control that connect with the social causes of a problem; organizational changes that correct one problem may, in fact, have a dark side, creating unpredictable others; and external environments are difficult to control.

Jervis describes the unintended consequences and harmful outcomes that result from complex interactions in social systems.[43] When complex, interactive technical systems, like the Space Shuttle, are run by complex organizations, like NASA, the probability of accidents is increased. Thus, system effects force us to recognize that it is not possible to prevent all accidents. However, it is important to remember that both of NASA's accidents had a long incubation period, and thus *were preventable*. By addressing the social causes of gradual slides and repeating negative patterns, organizations *can reduce the probability* that mistakes and accidents will occur. To do so, connecting strategies for correcting organizational problems with their social causes is crucial. Social scientists can play a significant role. First, we have research showing the problem of the slippery slope is perhaps more frequent than we now imagine, but less is known about cases where this pattern, once begun, is reversed.[44] Building a research base about organizations that make effective cultural change and reverse downward slides is an important step. Further, by their writing, analysis, and consulting, social scientists can 1) teach organizations about the social sources of their problems, 2) advise on strategies that will address those social causes, and 3) explore the system effects of planned changes, helping to forestall unintended consequences.[45]

---

43. Robert Jervis, *System Effects: Complexity in Political and Social Life* (Princeton: Princeton University Press, 1997).

44. Turner, *Man-made Disasters*; David Miller, *The Icarus Paradox: How Exceptional Companies Bring About Their Own Downfall* (New York: Harper, 1990), but see Rosabeth Moss Kanter, *Confidence: How Winning Streaks and Losing Streaks Begin and End* (New York: Simon & Schuster, 2004).

45. See, e.g., Rosabeth Moss Kanter, *The Changemasters* (New York: Simon & Schuster, 1983), and *Confidence: How Winning Streaks and Losing Streaks Begin and End* (New York: Simon & Schuster, 2004); Karlene H. Roberts, "Managing High Reliability Organizations," *California Management Review* 32, no. 4 (1990): 101–114; Karl E. Weick, Kathleen Sutcliffe, and David Obstfeld, "Organizing for High Reliability," *Research in Organizational Behavior* 21 (1990): 81–123; Todd R. La Porte and Richard Consolini, "Working in Practice but not in Theory: Theoretical Challenges of High-Reliability Organizations," *Journal of Public Administration Research and Theory* 1 (1991): 19–47; Diane Vaughan, "The Trickle-Down Effect: Policy Decisions, Risky Work, and the *Challenger* Accident," *California Management Review* 39 (winter 1997): 1–23; Lee Clarke, *Mission Improbable: Using Fantasy Documents to Tame Disaster* (Chicago: University of Chicago Press: 1999); Anita L. Tucker and Amy C. Edmondson, "Why Hospitals Don't Learn from Failures: Organizational and Psychological Dynamics that Inhibit System Change," *California Management Review* 45 (winter 2003): 55–72; Karen Marais, Nicolas Dulac, and Nancy Leveson, "Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems," (unpublished manuscript, Massachusetts Institute of Technology, 2004); Amy C. Edmondson, Michael Roberto, and Richard Bohmer, *The Columbia's Last Flight* (multimedia business case, Harvard Business School, 2005).

Second, NASA's problem of the cultural blind spot shows that insiders are unable to identify the characteristics of their own workplace structure and culture that might be causing problems. This suggests that rather than waiting until after a gradual slide into disaster or repeat of a negative pattern to expose the dark side of culture and structure, organizations would benefit from ongoing cultural analysis by ethnographically trained sociologists and anthropologists giving regular feedback, annually replaced by others to avoid seduction by the cultural ethos and assure fresh insights. Bear in mind this additional obstacle: the other facet of NASA's cultural blind spot was that the Agency's success-based belief in its own goodness was so great that it developed a pattern of disregarding the advice of outside experts.[46] To the extent that the CAIB report's embrace of an organizational system approach becomes a model for other accident investigation reports, other organizations may become increasingly aware of the social origins of mistakes and of the need to stay in touch with how their own organizational system is working.

46. CAIB, *Report*, chap. 5.

Chapter 12

Accidents, Engineering, and History at NASA, 1967–2003

Alexander Brown

Section 203(a)(3) of the National Aeronautics and Space Act directs NASA to "provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof."[1] To fulfill that mandate, NASA Administrator T. Keith Glennan instituted the NASA History Office in 1959.[2] The office has stayed open ever since, collecting archival materials for NASA staff and outside researchers, writing history, and commissioning a wide range of works on NASA's history. Over the last decade, the budget of NASA's history office has remained constant at around $335,000 per annum, although funds allocated to the history office from project offices vary from year to year. Even assuming such a level over the lifetime of the office, and not adjusting for inflation, NASA's commitment to telling its own history has cost the organization at least $15 million. But this figure is dwarfed by three official histories of NASA not commissioned by the history office. In 1967, 1986, and 2003, NASA spent $31 million, $75 million, and $152.4 million to produce multivolume accounts of fatal accidents in the manned space program.[3] These three accident reports examined the fatal fire in Apollo 204 (Apollo 1) in 1967, the explosion of the Solid Rocket Booster in STS-51L (*Challenger*) in 1986, and the destruction of the orbiter in STS-107 (*Columbia*).

Fatal accidents in publicly funded systems catch particular media and public attention.[4] Governments become compelled to conduct wide-ranging

1. John M. Logsdon et al., eds., *Exploring the Unknown: Selected Documents in the History of the U.S. Civil Space Program*, vol. 1, *Organizing for Exploration* (Washington, DC: NASA SP-4407, 1995), p. 337.

2. Roger D. Launius, "NASA History and the Challenge of Keeping the Contemporary Past," *Public Historian* 21, no. 3 (summer 1993): p. 63.

3. For Apollo 1, see Ivan D. Ertel and Roland Newkirk, with Courtney G. Brooks, *The Apollo Spacecraft: A Chronology*, vol. 4 (Washington, DC: NASA SP-4009, 1978); for *Challenger*, see Frank Oliveri, "NASA gets $50 million for Shuttle Investigation," *Florida Today* (21 February 2004); for *Columbia*, see Paul Recer, "NASA: Columbia Cleanup costs near $400M," *Newsday* (11 September 2003).

4. Thomas White, Jr., "Establishment of Blame as a Framework for Sensemaking in the Space Policy Subsystem: A Study of the Apollo 1 and Challenger Accidents" (Ph.D. diss., Virginia Polytechnic

continued on the next page

investigations to reassure the public of the safety of the system and the integrity of the funding process. Accidents at NASA are particularly public and so demand an investigation process that is accountable not only to the Congress but also to the American people. NASA accident investigation boards are forced to draw connections between national politics and engineering design and operations. The process of writing a final report also forces an accident investigation body to tell one coherent story about the accident—how the accident happened, what and who was at fault, and how steps can be taken to ensure the accident cannot happen again.

But as Peter Galison has observed in his study of aircraft accidents in the 1980s, accident reports are inherently unstable. They are multicausal in their historical explanations, and yet embedded in the very process of investigation is a drive for a single point of culpability upon which to base moral responsibility and recommendations for corrective action. Accident reports, then, are always ambiguous about the appropriate explanatory scale, so that it is never clear which is the right scale for analysis—whether the small scale or the large scale, the inflexible O-ring or the schedule pressure imposed on NASA by the White House and Congress.[5]

Galison is certainly correct to assert that reports show an explanatory tension, but this instability between frames of analysis is not just a function of the particular genre of accident reports. Engineering has changed such that there is now a social and epistemological gap between the management of engineering and engineering practice. The analytical tension in the investigation reports mirrors the real gap between engineers and managers at NASA. Furthermore, the reports are analytically asymmetrical, treating engineering as a context-free activity while explaining management in a sophisticated historical and cultural framework.

These gaps are not just a phenomenon inherent to accident reports, but the outcome of a set of historical and historiographical changes. The Apollo 204 accident shows the disjuncture between the engineers designing and managing the project and the technicians manufacturing the spacecraft. The *Challenger* and *Columbia* accidents show that disjuncture has shifted to the gap between managers controlling the project and engineers maintaining and analyzing the spacecraft. Similarly, since the 1980s, the organizational theory and organizational communications communities have joined the aeronautical engineering community in paying significant scholarly attention to

---

continued from the previous page

Institute and State University, 2000). White's thesis analyzes the ways in which blame was allocated in these two accidents but also makes it very clear that public and political concern and outrage were extremely high in both cases.

5. Peter Galison, "An Accident of History," in *Atmospheric Flight in the Twentieth Century*, ed. Peter Galison and Alex Roland (Dordrecht, Netherlands: Kluwer Academic Publishers, 2000), pp. 3–43.

accidents at NASA. Their engagement has shifted attention to the historical and organizational context of management decision-making surrounding the accidents. No historians of engineering and technology have matched this contextualization of management with a history of the engineering involved in the accidents or an attempt to integrate the two.

This paper will briefly lay out the accidents and discuss the findings of their investigative bodies. The changing historiographical styles, frameworks, and conclusions of the reports will be analyzed. These changes will be linked to changes in the practice of engineering by NASA and its contractors. Finally, some suggestions will be made for future research into accidents and changes in engineering.

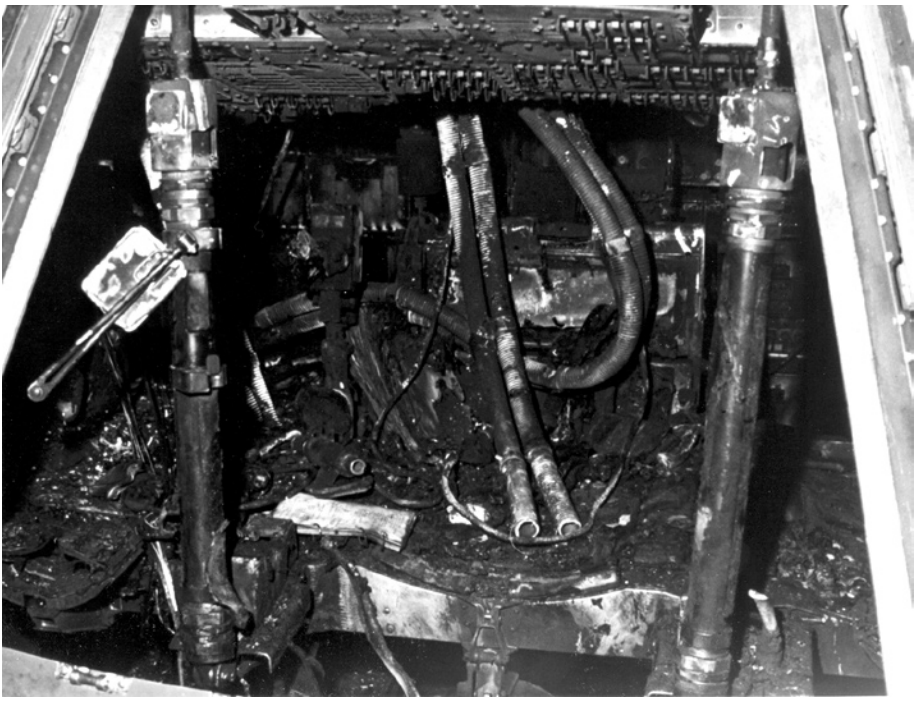
APOLLO 204

On 27 January 1967, Spacecraft 012, assigned to the Apollo 204 mission, was undergoing a Plugs-Out Integrated Test on Pad 34 at Kennedy Space Center in Florida. The internal power systems of the newly delivered Command and Service Module were being tested, and so the crew cabin was pressurized to 16 pounds per square inch (psi) of pure oxygen. There were three astronauts on board: Gus Grissom, Ed White, and Roger Chaffee. At around 6:31 p.m. EST, the crew reported a fire in the spacecraft. Less than 20 seconds later, the spacecraft heatshield had ruptured and flame had burst into the service tower. The crew in the Command and Service Module (CSM) level of the support tower immediately evacuated the area but quickly returned with what firefighting and protective gear they could find. However, they were unable to extinguish the fire immediately or remove the crew from the cabin. Meanwhile, the crew had attempted to remove the middle hatch of the spacecraft but had been overcome before doing so. Firefighting crews and medical support arrived approximately 20 minutes later.

NASA Deputy Administrator Robert Seamans had already considered the possibility of an accident in the manned spaceflight program, after Neil Armstrong and Dave Scott in Gemini VIII had lost control of their capsule after docking with an Agena booster.[6] In the aftermath of Gemini VIII, he developed a set of procedures to be followed should an accident ever occur. On the evening of 28 January, he followed those procedures and immediately convened an accident review board.[7] The board convened at Kennedy Space Center in Florida and was

6. Robert C. Seamans, *Aiming at Targets* (Washington, DC: NASA SP-4106, 1996), pp. 135–136; Barton C. Hacker and James M. Grimwood, *On the Shoulders of Titans: A History of Project Gemini* (Washington, DC: NASA SP-4203, 1977), pp. 308–319.

7. Apollo 204 Review Board, appendix a-G, "Board Minutes," in *Report of Apollo 204 Review Board to the Administrator, National Aeronautics and Space Administration* (Washington, DC: GPO, 1967), pp. 1-5–1-6.



The mission officially designated Apollo/Saturn 204 is more commonly known as Apollo 1. This close-up view of the interior of the Command Module shows the effects of the intense heat of the flash fire that killed the prime crew during a routine training exercise. While they were strapped into their seats inside the Command Module atop the giant Saturn V Moon rocket, a faulty electrical switch created a spark that ignited the pure-oxygen environment. The speed and intensity of the fire quickly exhausted the oxygen supply inside the crew cabin. Unable to deploy the hatch due to its cumbersome design and the lack of breathable oxygen, the crew lost consciousness and perished. They were astronauts Virgil I. "Gus" Grissom (the second American to fly into space), Edward H. White II (the first American to "walk" in space), and Roger B. Chaffee (a "rookie" on his first space mission). *(JSC image no. S-67-21294, 28 January 1968)*

chaired by Floyd "Tommy" Thompson, Director of NASA's Langley Research Center.[8] The board was made up of three senior NASA engineers, a chemist from the Bureau of Mines, an Air Force officer from the Inspector General's office, NASA Langley's general counsel, and an astronaut.[9]

On 5 April 1967, the Apollo 204 Review Board presented its report to NASA Administrator James Webb. They concluded that the fire was caused

8. James R. Hansen, *Engineer in Charge: A History of the Langley Aeronautical Laboratory, 1917–1958* (Washington, DC: NASA SP-4305, 1987), pp. 387–391.

9. Apollo 204 Review Board, appendix a-G, "Board Minutes," pp. 2-1–2-17.

by an unknown source of electrical arc, probably malfunctioning wire insulation around the environmental control unit on the floor of the spacecraft, although the cause would never be definitively known. The spark then ignited nylon netting, Velcro strips, and other combustible materials inside the spacecraft. These materials would have been removed before spaceflight, but under test conditions were not seen as hazardous. The coolant inside the spacecraft, water-glycol, was flammable and left a flammable residue in the cabin after evaporation. As the pipes melted, coolant leaked and ignited, further fueling the fire. The fire was rendered particularly dangerous by the high-pressure, pure-oxygen environment inside the spacecraft during the test. The crew was unable to use the inward-opening inner hatch under the pressurized conditions. The Board determined that the crew had died from asphyxiation caused by fumes from the fire.[10]

The Board told a story of engineering failure, identifying six conditions that led to the fire, and provided recommendations to fix the engineering problems they identified. These conditions were a sealed cabin with a pressurized atmosphere, extensive distribution of flammable materials in the cabin, vulnerable wiring carrying spacecraft power, vulnerable plumbing containing combustible and corrosive coolant, inadequate escape provisions, and an inadequate provision for rescue or medical assistance.[11]

After the Board made their engineering recommendations, they spoke briefly about the larger circumstance surrounding the accident:

> Having identified the condition that led to the disaster, the Board addressed itself to the question of how these conditions came to exist. Careful consideration of this question leads the Board to the conclusion that in its devotion to the many difficult problems of space travel, the Apollo team failed to give adequate attention to certain mundane but equally vital questions of crew safety. The Board's investigation revealed many deficiencies in design and engineering, manufacture and quality control. When these deficiencies are corrected the overall reliability of the Apollo Program will be increased greatly.[12]

On 27 February 1967, the Senate Committee on Aeronautical and Space Sciences started to hold hearings on the Apollo 204 fire, and on 11 April, the House Committee on Science and Astronautics started to hold hearings into the Apollo 204 fire.

10. Ibid., pp. 5-1–5-12.
11. Ibid., p. 5-12.
12. Ibid., p. 5-12.

On the first day of the hearings before the Senate, NASA Administrator James Webb, Deputy Administrator Seamans, and Associate Administrator George Mueller were sandbagged by the Democratic Senator from Minnesota, Walter Mondale. Mondale asked them about a report that Apollo Program Director Major General Sam Phillips had prepared in 1965 after visiting North American Aviation (NAA), manufacturers of the spacecraft.[13] Mueller first denied any knowledge of the report, arguing that Phillips had prepared many reports on many NASA contractors. Webb then argued that he was not going to release the report for reasons of commercial confidentiality, as it contained details of contract negotiations between NASA and NAA.[14] Senators Brooke, Percy, and, in particular, Mondale became highly critical of NASA's unwillingness, as they saw it, to be accountable to elected officials.[15]

The Phillips report was damning. Phillips had written:

> I am definitely not satisfied with the progress and outlook of either program and am convinced that the right actions now can result in substantial improvement of position in both programs in the relatively near future.
>
> Even with due consideration of hopeful signs, I could not find a substantive basis for confidence in future performance. I believe that a task group drawn from NAA at large could rather quickly verify the substance of our conclusions, and might be useful to you in setting the course for improvements.[16]

Phillips recommended that NAA thoroughly revise (and in many cases implement) systems management and engineering procedures. He called for them to implement a program management system and to significantly improve their manufacturing and quality control.[17]

The House hearing subcommittee was chaired by Representative Olin Teague of Texas, a long-term supporter of the space program. The hearings were contentious—with a Republican from Illinois, Donald Rumsfeld, taking particular aim at NASA senior officials Webb, Seamans, and Faget. Rumsfeld took objection to the constitution of the Board, arguing that it

13. Senate Committee on Aeronautical and Space Sciences, *Apollo Accident*, Hearing, 90th Cong., 1st sess., 7 February 1967, pp. 125–127.

14. Ibid., pp. 131–132.

15. Ibid., pp. 217, 331–332; Senate Committee on Aeronautical and Space Sciences, *Apollo 204 Accident. Report of the Committee on Aeronautical and Space Sciences, United States Senate, with Additional Views* (Washington, DC: GPO, 1968), pp. 13–16.

16. Samuel Phillips, cover letter to Lee Atwood, in "NASA Review Team Report," 1965.

17. Ibid., pp. 1–20.

was made of people responsible for the areas of work whose failure they were investigating. NASA was, in effect, investigating itself. Rumsfeld was also concerned about the narrow focus of the Board's report, suggesting that they had defined their terms very specifically to avoid investigating larger problems within NASA management. Finally, he wanted to know why NASA did not have a separate and independent safety organization.[18] Webb and Seamans gave fairly weak responses to Rumsfeld's questions and were only saved by Teague's interruptions.

But the worst was still to come for NASA. It was revealed that in the initial awarding of the CSM contract to NAA, NAA had scored lower in the technical assessment than Martin. The Congressmen used this revelation to imply some sort of improper relationship between NASA and NAA.[19] In the final days of the House hearing, Thomas Baron, a quality-assurance inspector from NAA, presented to the Committee a detailed report of deficiencies, official malfeasances, and general complaints about the standard of workmanship and care at NAA.[20] While the Baron report was eventually proved to be largely personal grievances and unproven accounts of interactions between workers at NAA, it all contributed to a larger picture of poor management and workmanship at NAA and poor supervision at NASA.

Although the Apollo 204 Board did not blame any individuals for the fire, there were consequences. Joseph Shea, manager of the Apollo Spacecraft Program Office, and Harrison Storms, NAA's vice president in charge of the Space and Information Division, were both moved out of their positions.[21] Deputy Administrator Seamans also resigned soon after the investigation had concluded, his personal relationship with James Webb having deteriorated dramatically over the fire.[22]

CHALLENGER

On 28 January 1986, the Space Shuttle *Challenger* launched from Kennedy Space Center on mission 51-L. There were seven astronauts on board: Dick Scobee, Michael Smith, Ellison Onizuka, Judith Resnik, Ronald McNair, Christa McAuliffe, and Gregory Jarvis. Their mission was to deploy and

18. House Committee on Science and Astronautics, *Investigation into Apollo 204 Accident*, Hearings before the Subcommittee on NASA Oversight, 90th Cong., 1st sess., 10 April 1967, pp. 10–14.

19. Ertel and Newkirk, *The Apollo Spacecraft: A Chronology*, vol. 4, entry for 11 May 1967.

20. Thomas Ronald Baron, "An Apollo Report," in House Committee on Science and Astronautics, *Investigation into Apollo 204 Accident*, pp. 483–500.

21. Ertel and Newkirk, *The Apollo Spacecraft: A Chronology*, vol. 4, entry for 7 April 1967; Mike Gray, *Angle of Attack: Harrison Storms and the Race to the Moon*, 1st ed. (New York: W. W. Norton, 1992), pp. 254–255.

22. Seamans, *Aiming at Targets*, pp. 145–147.

recover a satellite in orbit and to conduct flight-dynamics experiments.[23] Christa McAuliffe, a teacher from New Hampshire, was to conduct a science lesson in orbit.[24] The 28th of January was a very cold morning. The temperature at Kennedy Space Center in Florida had dropped below freezing overnight, and ice teams had been sent out three times to examine potential damage. Parts of the Space Shuttle, including the Solid Rocket Boosters, were still below freezing point at launch. The ambient air temperature was 36°F, 15 degrees lower than any previous flight.[25]

Less than a second after launch, at 11:38 a.m. EST, a puff of gray smoke emerged from the right Solid Rocket Booster (SRB). Over the next 2 seconds, eight more puffs of smoke, blacker and more dense, emerged from the same place on the SRB. Thirty-seven seconds after launch, the Shuttle experienced a 27-second period of severe wind shear, stronger than any other Shuttle launch had experienced. Fifty-eight seconds after launch, a small flame appeared on the aft field joint of the right SRB. Over the next 14 seconds, the flame grew rapidly, burning through the lower strut holding the SRB to the External Tank. Seventy-two seconds after launch, the strut burned through and the right SRB rotated around the upper strut, crashing into the External Tank. The tank collapsed, venting the hydrogen fuel into the atmosphere. The fuel immediately ignited, and the entire Shuttle flew into the fireball. The orbiter entered the fireball, broke up under severe aerodynamic load, and fell back into the Atlantic Ocean. There were no survivors.[26]

On 3 February 1986, President Ronald Reagan appointed the Presidential Commission on the Space Shuttle *Challenger* Accident.[27] The Commission was chaired by William Rogers, Secretary of State under Richard Nixon and an attorney by training and experience. The Commission included two astronauts, a test pilot, two physicists, another attorney, three engineers, a senior Air Force officer, an aerospace journalist, and an astronomer. Another engineer was executive director. The Commission conducted public and private hearings over the early part of 1986 and presented its report to President Reagan on 6 June 1986.

Like the Apollo 204 Review Board, the Commission understood its objectives to be investigating the accident and providing a series of rec-

23. Presidential Commission on the Space Shuttle *Challenger* Accident, *Report to the President*, 5 vols. (Washington, DC: GPO, 1986), p. 16; "John F. Kennedy Space Center—51-L Shuttle Mission," *http://www-pao.ksc.nasa.gov/kscpao/shuttle/missions/51-l/mission-51-l.html*.

24. For Christa McAuliffe's official NASA biography, see *http://www.jsc.nasa.gov/Bios/htmlbios/mcauliffe.html*.

25. Presidential Commission on the Space Shuttle *Challenger* Accident, *Report to the President*, vol. 1, pp. 16–21.

26. Ibid., pp. 20–21.

27. Ibid., pp. 212–213.

The STS-51L crew members. In the back row, from left to right: mission specialist Ellison S. Onizuka, Teacher in Space participant Sharon Christa McAuliffe, payload specialist Greg Jarvis, and mission specialist Judy Resnik. In the front row, from left to right: pilot Mike Smith, commander Dick Scobee, and mission specialist Ron McNair. *(JSC image no. S85-44253,15 November 1985)*

ommendations for a return to safe flight.[28] And like the Apollo Board, the Commission examined the physical causes of the accident but was also critical of NASA and its contractors as organizations:

> The genesis of the Challenger accident—the failure of the joint of the right Solid Rocket Motor—began with decisions made in the design of the joint and in the failure by both Thiokol (manufacturer of the Solid Rocket Motors) and NASA's Solid Rocket Booster project office to understand and respond to facts obtained during testing.[29]

28. Ibid., p. 1.
29. Ibid., p. 166.

The Commission determined that a combustion gas leak through the aft field joint on the right Solid Rocket Motor caused the flame plume. The field joint was designed to be sealed by O-rings. On STS-51L, the O-rings failed to work because ambient temperature was too cold and the O-rings lost resilience and hence their ability to seal quickly.[30] The Commission's report took aim at poor management decisions, arguing that schedule- and cost-conscious managers misunderstood and overruled the safety judgments of engineers. They concluded that flaws existed in NASA's decision-making process and that these flaws had caused NASA to decide to launch STS-51L when there was reason to believe that launching would be risky and potentially catastrophic. NASA's safety system was indicted as silent and ineffective in the face of increasing pressure on the launch schedule. Finally, the Commission suggested that these flaws were rooted in the history of the Space Shuttle program and the history of NASA.[31]

Commissioner Richard Feynman went further in appendix F to the report. This appendix contained Feynman's personal observations from his service on the Commission and particularly addressed the difference he had observed between NASA and Thiokol engineers and managers. Feynman observed that managers and engineers tended to calculate risk in very different ways—managers determining risk from a number of qualitative factors, whereas engineers calculated risk quantitatively, using standard statistical methods. He also observed that these two methods tended to produce widely divergent results. Managers generally understood risks to be orders of magnitude less than engineers.[32] Feynman was highly critical of this gap, arguing that there were only two ways to understand it. The first was dishonesty on the part of managers, designed to ensure a continuous flow of funding for the Shuttle. The second was an incredible lack of communication between engineers and managers.[33] He argued that to ensure safe operation of the Shuttle, NASA managers needed to understand the realities of risk involved in flying high-performance vehicles like the Shuttle. After all, he concluded, "for a successful technology, reality must take precedence over public relations, for Nature cannot be fooled."[34]

30. Ibid., chaps. 3, 4.

31. Ibid. Chapter 5 discusses management decisions; chapter 6, the historical background of the accident; and chapter 7, NASA's safety program.

32. Richard Phillips Feynman and Ralph Leighton, *What Do You Care What Other People Think? Further Adventures of a Curious Character*, 1st ed. (New York: Norton, 1988), pp. 179–184. This volume also contains a version of appendix F edited for clarity, pp. 220–237. For the original version, see Presidential Commission on the Space Shuttle *Challenger* Accident, *Report to the President*, pp. F-1–F-5.

33. Feynman and Leighton, *What Do You Care What Other People Think?* pp. 236–237.

34. Presidential Commission on the Space Shuttle *Challenger* Accident, *Report to the President*, p. F-5.

The Commission's report echoed Feynman's findings, even though he felt upset that his opinions had not been adequately incorporated into the final document.[35] The report suggested that NASA management and NASA engineers saw the material world in very different ways—the engineers understanding risk as quantifiable and determined by the material world, whilst managers understood risk as flexible and manageable in commercial and political contexts. The cause of the accident, the report concluded, was the failure of communication between these two perspectives. The ultimate expression of this philosophy was the statement by Jerald Mason of Morton Thiokol telling Robert Lund, vice-president of engineering, "You've got to put on your management hat, not your engineering hat" in order to determine whether the *Challenger* would launch the next day despite engineers' concerns over the safety of the Solid Rocket Motor.[36] In its final recommendations, the Commission wanted design changes to the Solid Rocket Motor, reform of the Shuttle program management structure, and the establishment of a Shuttle Safety Panel and an independent Office of Safety, Reliability and Quality Assurance.

The House Committee on Science and Technology started holding hearings on the *Challenger* accident on 10 June 1986. As in Apollo 204, from which the Committee drew its precedent, hearings were delayed until the Commission report was published. The Committee conducted 10 days of hearings, questioning senior NASA and Morton Thiokol officials, as well as members of the Commission, astronauts, and Morton Thiokol engineers.[37] While the Committee endorsed the findings of the Commission, their report went further:

> The Committee feels that the underlying problem which led to the Challenger accident was not poor communication or inadequate procedures as implied by the Rogers Commission conclusion. Rather the fundamental problem was poor technical decision-making over a period of several years by top NASA and contractor personnel, who failed to act decisively to solve the increasingly serious anomalies in the Solid Rocket Booster joints.[38]

Neither the Commission nor the Committee explicitly laid blame at the feet of any individuals. However, their criticisms of management at NASA's

35. Feynman and Leighton, *What Do You Care What Other People Think?* pp. 199–205.

36. Presidential Commission on the Space Shuttle *Challenger* Accident, *Report to the President*, p. 94.

37. House Committee on Science and Technology, *Investigation of the Challenger Accident: Report of the Committee on Science and Technology, House of Representatives*, 99th Cong., 2nd sess., 1986, pp. 37–38.

38. Ibid., p. 5.

Marshall Space Flight Center and at Morton Thiokol were duly noted by those organizations. Most of Morton Thiokol management involved in the launch decision were reassigned, retired, or resigned, including Jerald Mason and Robert Lund. At NASA, Associate Administrator for Space Flight Jesse Moore resigned, while MSC Director William Lucas and booster project manager Lawrence Mulloy both retired early.[39]

COLUMBIA

On 16 January 2003, the Space Shuttle *Columbia* launched from Kennedy Space Center on mission 107. There were seven astronauts on board: Rick Husband, William McCool, Michael Anderson, David Brown, Kalpana Chawla, Laurel Clark, and Ilan Ramon. Fifty-seven seconds after launch, at around 10:40 a.m. EST, the *Columbia* entered a period of unusually strong wind shear, which created a low-frequency oscillation in the liquid oxygen in the External Tank.[40] At 81.7 seconds after launch, at least three pieces of Thermal Protection System foam detached from the left bipod ramp of the External Tank and fell backwards at between 416 and 573 miles per hour, smashing through the leading edge of the left wing of the orbiter. The largest piece of foam was around 2 feet long and 1 foot wide. The launch was otherwise without incident, and *Columbia* arrived in orbit by 11:39 a.m. EST.

On 23 January, Mission Control e-mailed commander Husband and pilot McCool to inform them of the foam strike, informing them that some foam had hit the orbiter but reassuring them that "we have seen this phenomenon on several other flights and there is absolutely no concern for entry."[41]

On 1 February 2003, after a successful 17-day mission, the orbiter reentered the Earth's atmosphere for a landing at Kennedy Space Center. As the orbiter reentered, superheated air penetrated the left wing through the foam strike in the leading edge and started to melt away the wing from the inside. At around 9:00 a.m. EST, the orbiter broke up under severe aerodynamic load and disintegrated over the Southwest of the United States. There were no survivors.

Around 10:00 a.m. on 1 February 2003, NASA Administrator Sean O'Keefe declared a Shuttle Contingency and, acting under procedures set in place after the *Challenger* accident, established the International Space Station

39. Claus Jensen, *No Downlink: A Dramatic Narrative About the Challenger Accident and Our Time*, 1st ed. (New York: Farrar, Straus and Giroux, 1996), pp. 354–355; Richard S. Lewis, *Challenger: The Final Voyage* (New York: Columbia University Press, 1988), pp. 222–223.

40. Columbia Accident Investigation Board, *Report*, vol. 1 (Washington, DC: NASA and GPO, 2003), pp. 33–34.

41. Ibid., p. 159.

and Space Shuttle Mishap Interagency Board.[42] O'Keefe named Admiral Harold Gehman as Chair of the Board. Gehman was retired from the Navy and had recently headed the investigation into the terrorist attack on the USS *Cole*.[43] Ex officio, there were immediately seven Board members: four military officers with responsibilities for safety in their home services, a Federal Aviation Administration representative, a Department of Transportation representative, and a NASA Center Director. O'Keefe soon thereafter named both NASA's Chief Engineer and the counsel to Glenn Research Center to the Board. Over the next six weeks, five more members were appointed to the renamed Columbia Accident Investigation Board. They included an aeronautical engineer and former Air Force Secretary, a physicist, a former astronaut and *Challenger* Commission member, a space policy expert, and the retired CEO of a major defense contractor.[44] Over the first six months of 2003, the Board held hearings and conducted investigations into the *Columbia* accident and, on 26 August 2003, released its report.

The CAIB report identified the physical cause of the accident as the foam strike on the left wing leading edge. But unlike the Apollo 204 Board, which briefly mentioned organizational and other factors, or the *Challenger* Commission, which described these factors as contributory, the CAIB emphasized that factors other than the proximate physical cause were as, if not more, important in understanding the *Columbia* accident:

> 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. The Board did not want to make these errors. A central piece of our expanded cause model involves NASA as an organizational whole.

42. Ibid., pp. 231–232.
43. William Langewiesche, "Columbia's Last Flight," *Atlantic Monthly* (November 2003): 65–66.
44. CAIB, *Report*, p. 232.

> The organizational causes of this accident are rooted in the Space Shuttle Program's history and culture, including the original compromises that were required to gain approval for the Shuttle Program, subsequent years of resource constraints, fluctuating priorities, schedule pressures, mischaracterizations of the Shuttle as operational rather than developmental, and lack of an agreed national vision. Cultural traits and organizational practices detrimental to safety and reliability were allowed to develop, including: reliance on past success as a substitute for sound engineering practices (such as testing to understand why systems were not performing in accordance with requirements/specifications); organizational barriers which prevented effective communication of critical safety information and stifled professional differences of opinion; lack of integrated management across program elements; and the evolution of an informal chain of command and decision-making processes that operated outside the organization's rules.
>
> In the Board's view, NASA's organizational culture and structure had as much to do with this accident as the External Tank foam.[45]

Seventeen years after *Challenger*, the Board concluded that many of the findings of the *Challenger* Commission were still applicable to the Space Shuttle program in the early 21st century. They were critical of the similarities between the *Challenger* and *Columbia* accidents, noting in the *Columbia* accident flawed decision-making processes, a silent safety program, and schedule pressure. The Board also observed that the causes of these failures were rooted in NASA's history and culture; the history of the Space Shuttle program had been a history of the normalization of deviance. Increasingly large engineering problems that had not caused catastrophic failures had been incorporated into NASA's experience base instead of raising safety concerns. NASA had come to rely on past success (or lack of past catastrophe) rather than rigorous testing and analysis. NASA's safety system was still silent. Decision-making was still flawed, with managers and engineers still unable to communicate effectively about risk.

The Commission recommended design changes to the Thermal Protection System on the External Tank, reform of the Space Shuttle Integration Office, training for the Mission Management Team, the establishment of an indepen-

45. Ibid., p. 177.

dent Technical Engineering Authority with safety responsibilities, and rendering the NASA Office of Safety and Mission Assurance independent and with total oversight of the Space Shuttle program safety organization.[46]

READING ACCIDENT REPORTS AS HISTORY

The Apollo 204 report is almost exclusively devoted to an analysis of the engineering problems that the Board argued caused the fire. It divides its analysis into two parts, parts IV and V of the report.[47] Part IV, "History of the Accident," provides a chronology of the accident from August 1964 until 28 January 1967. The sections discussing the fabrication, delivery, and inspection of the CSM spacecraft, which cover the period from August 1964 until December 1966, take up less than 10 percent of the report. The remainder of the history of the accident is a detailed chronology of the Plugs-Out Integrated Test of CSM 012, starting around 5 hours and 30 minutes before the accident. Part V, "Investigation and Analysis," has four sections: "Inspection and Disassembly," "Chronology," "Data Analyses," and "Cause of the Fire." Both the "Inspection and Disassembly" and "Chronology" sections are strictly narrative. "Data Analyses" discusses analyses of spacecraft telemetry data and crew voice transmissions from less than a minute before the accident, while the "Causes of the Fire" section notes deficiencies in electrical equipment and wiring insulation, the effects of electrical arcs on wiring and coolant on other equipment, and the effects of a cabin environment of pure oxygen under pressure. The sole mention of other, larger contributory factors is the final paragraph, noting that these engineering problems came about through deficiencies in design and manufacturing.[48]

But none of the political circumstances surrounding the Apollo program—its iconic status as the martyred President Kennedy's legacy, as a visible symbol of American technical prowess, as a marker of position in the Cold War—were identified as contributory. Nor was NASA's organizational structure or its culture. No individuals were identified as bearing particular responsibility for the accident. The report makes clear that poor engineering practice, whether design, management, or operation, was to blame.

The report of the Presidential Commission on the Space Shuttle *Challenger* Accident is a striking contrast to the Apollo 204 report. Even superficially, the reports are dissimilar. The Apollo 204 report looks like a report—it is

46. Ibid., chap. 11.

47. Parts I, II, and III describe the Board's legal authority, the biographies of its members, and the proceedings of the Board.

48. Apollo 204 Review Board, *Report to the Administrator, National Aeronautics and Space Administration* (Washington, DC: GPO, 1967), pp. 5–12.

monochromatic, printed in standard Government Printing Office format, and appears very similar to a multitude of other NASA reports. The report on the *Challenger* accident looks more like a magazine or coffee table book. It has large sections of color photographs used as visual evidence by the Commission, was printed on glossy paper, and was written in a narrative form familiar to readers of nonfiction. It opens with a preface and an introduction, outlining the task of the Commission and contextualizing the development of the Space Shuttle. The report goes on to outline the events of 28 January 1986 and from there leads into its analysis of the physical cause of the accident in a chapter simply titled "The Cause of the Accident."[49] The remainder of the report analyzes the series of events that contributed to the accident: the chain of decisions that led to the decision to launch, the history of design problems with the O-ring system, the political and organizational pressures to launch, and the failure of the safety system.[50] In seeking to understand the contributory causes of the accidents, the Commission's report does not explicitly draw on any theoretical work. The report's footnotes are to transcripts of Commission hearings or to original NASA and Morton Thiokol documents, rather than any other writings on accidents or safety.

The Presidential Commission was clear that there were physical causes for the accident—in this case, the failure of the O-rings to seal correctly. But unlike the Apollo 204 Review Board, the Commission saw secondary contributing causes. These secondary causes were the flawed launch decision, political pressures on the launch schedule, and a silent safety system. The 1967-model report, setting out an understanding of engineering failures to be fixed with engineering solutions, was changed into a critique of both engineering and management with separate solutions for each area of endeavor.

The report of the Columbia Accident Investigation Board (CAIB) was even more like a magazine. Unlike the Apollo 204 and *Challenger* reports, the CAIB report has its own logo and its own page headers and footers. The report contains sidebars to provide contextual or background material and is illustrated with images of the *Columbia* in preparation and in flight and images of the *Columbia* crew both before and during the 107 mission.

Like the *Challenger* report, the CAIB report devotes only one chapter, chapter 3, to the proximate physical cause of the accident—the separation of Thermal Protection System (TPS) foam from the External Tank and its subsequent impact on the leading edge of the orbiter. But the report has four chapters, chapters 5 to 8, discussing the context of the decision-making that led to the breakup of the orbiter on reentry. Chapter 3 discusses the engineering

49. Presidential Commission on the Space Shuttle *Challenger* Accident, *Report to the President*, vol. 1, chap. 4.

50. Ibid., chaps. 5 through 8, respectively.

analyses the Board performed, the history of External Tank design decisions, and the conclusions to be drawn from these, but it does so without using any theory, simply presenting this engineering section as needing no context or justification. It is only where the Board starts to examine the decision-making of NASA engineers and managers that led to the *Columbia* disaster that more sophisticated explanatory frameworks are needed. The Board drew on a variety of theoretical perspectives, considering Charles Perrow's theory of normal accidents and the work of both Scott Sagan and Todd La Porte on high-reliability theory.[51]

Perhaps most interestingly, the CAIB report drew heavily on the work of Diane Vaughan. Vaughan's 1996 book, *The Challenger Launch Decision*, set out a sociological explanation for the flawed decision, arguing that, far from the managerial misconduct identified by the *Challenger* report, the accident can best be understood in terms of the normalization of deviance, the culture of production at NASA and Morton Thiokol, and structural secrecy.[52] Vaughan argued:

> This book explicates the sociology of mistake. It shows how mistake, mishap and disaster are socially organized and systematically produced by social structures. No extraordinary actions by individuals explain what happened: no intentional managerial wrongdoing, no rule violations, no conspiracy. The cause of disaster was a mistake embedded in the banality of organizational life.[53]

This perspective informed chapter 8 of the CAIB report, where the Board drew explicit links between the *Challenger* and *Columbia* accidents, applying the components of Vaughan's analysis to *Columbia*. The Board concluded:

> First, the history of engineering decisions on foam and O-ring incidents had identical trajectories that "normalized" these anomalies, so that flying with these flaws became routine and acceptable. Second, NASA history had an effect. In response to White House and Congressional mandates, NASA leaders took actions that created systemic organizational flaws at the time of Challenger that were also present for Columbia.[54]

51. CAIB, *Report*, p. 180.

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

53. Ibid., p. xiv.

54. CAIB, *Report*, p. 195.

Unlike the *Challenger* report, the CAIB report gives equal weight to the organizational causes of the accident, arguing that while mistakes were made, the organizational structure of NASA was more to blame that any individual failings.

The three reports suggest a story of growing separation of management and engineering. As Peter Galison has suggested, this may simply be a result of the instability between frames of analysis: the desire both to localize and to diffuse the locus of causation, to find a single physical cause, and to explain the accident in terms of larger organizational and cultural problems.[55] But it is interesting to note that these two activities are not only juxtaposed as possible sources of accidents, but also understood and analyzed in different ways. There has been a growing sophistication in the ways that decision-making and its contexts have been understood. There is a transition from Apollo 204's one-paragraph analysis of larger causes, to *Challenger*'s inclusion of organizational and political factors as contributory, to *Columbia*'s equal pairing of technical and social causes. There is a corresponding increase in the contextualization of these social elements of the analysis, from rudimentary mentions in Apollo 204 to a full examination and consideration of sociological and organizational theory literature in *Columbia*.

But there is an interesting asymmetry in these reports as well. As analyses of decision-making and its historical and cultural contexts have grown ever more sophisticated in these accident reports, the discussions of physical causes have remained remarkably similar. In each accident report, a number of possible causes are considered and eliminated before attention is turned to the actual cause. In each of the sections of the reports dealing with physical cause, there is little or no contextualization of engineering and design decision-making and no attempt to locate the discussion in a body of literature. This separates the physical and technical causes of accidents from their contexts and sets up the two activities—engineering and decision-making about engineering—as two quite different activities, to be understood and analyzed in different terms. In this formulation, engineering seems to be understood on its own terms, as a context-free and ahistorical activity, whereas management decision-making is understood as contingent and located within a complex historical and cultural framework.

This asymmetry immediately opens two questions. First, what historical processes caused the separation of engineering and management in the manned space program from 1967 to the present day? Second, what changes in engineering over the same period can be seen in the three accident reports and might provide the basis for understanding engineering in its own historical and cultural context? The disciplines of the history of technology and the history of science provide some directions to go look for answers to these questions.

55. Galison, "An Accident of History," p. 4.

Engineering accidents can be understood in a similar way to scientific controversies. A scientific controversy is resolved when the winners declare that their account is true and opponents are no longer taken seriously by the relevant scientific community.[56] Just as scientific controversies open up the inner workings of a laboratory or research group, so accidents open up the internal practices and politics of engineering. But accidents also provide a way to examine how engineers go about activities other than design and innovation. Most studies of engineers and engineering focus on design because it is the most creative and innovative element of the engineer's craft.[57] However, the vast majority of time spent by engineers is taken up with the development and operation of technologies rather than their design. Accident investigations take a comprehensive look at the design, manufacture, and operation of the broken artifact or system and so provide a way to look at engineering work at the routine, everyday level, as well as at the creative design level. The process of investigating an accident results in the extensive description of these everyday routines, routines that are often seen as so mundane as to leave little trace in the documentary record of the project. Thus, if these NASA accident reports are examined as a historian might examine them, they can trace changes in both design and routine engineering.

By treating accidents and their investigations as windows into engineering at NASA, there are at least three aspects of engineering at NASA that have changed since the 1960s—the widespread use of computers in engineering, the emergence of astronautical engineering as a new discipline, and a move away from systems engineering as an organizing philosophy for large projects.

Computing

Since the 1960s, computers have become ubiquitous, and there is a growing literature that points to the ways in which interaction with computers reshapes

56. This particular interpretation of scientific controversy is taken from the works of Bruno Latour and Wiebe Bijker in particular. See Bruno Latour, *Science in Action: How to Follow Scientists and Engineers through Society* (Cambridge, MA: Harvard University Press, 1987); Bruno Latour and Steve Woolgar, *Laboratory Life: The Construction of Scientific Facts* (Princeton, NJ: Princeton University Press, 1986); Wiebe E. Bijker, Thomas Parke Hughes, and T. J. Pinch, *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge, MA: MIT Press, 1987).

57. This point was well made by John Staudenmaier in his surveys of the field of history of technology. See John M. Staudenmaier, *Technology's Storytellers: Reweaving the Human Fabric* (Cambridge, MA: Society for the History of Technology and the MIT Press, 1985); John M. Staudenmaier, "Recent Trends in the History of Technology," *American Historical Review* 95, no. 3 (1990). For examples of this focus on design to the exclusion of other aspects of engineering, see, for example, Walter G. Vincenti, *What Engineers Know and How They Know It: Analytical Studies from Aeronautical History*, Johns Hopkins Studies in the History of Technology (Baltimore: Johns Hopkins, 1990); Henry Petroski, *To Engineer Is Human: The Role of Failure in Successful Design* (New York: St. Martin's Press, 1985).

the ways people live and work.[58] Just like scientists, the engineering profession has adopted computing extensively, with almost all elements of engineering activity now mediated through computers—design, simulation modeling, communications, logistics, financial management, and administration.[59] Over the period 1967–2003, modeling, testing, and simulation moved from being largely hand-calibrated to being almost exclusively computer-mediated.[60] The Columbia Accident Investigation Board report shows, however, that this process involved the loss of much of the transparency of older techniques.

A brief history of the modeling tool Crater illustrates this process well. Crater was originally built in 1966 by Allen Richardson at Rockwell. It was designed in conjunction with NASA engineers to predict the effects of hypervelocity impacts on multilayer surfaces like those of the Apollo CSM. Crater was a curve fit from a data set generated in part from Gemini experience and in part from testing performed by General Motors and NASA on aluminum honeycomb materials. Crater could predict threshold velocities and penetration damage but was complex to use; the number and complexity of calculations needed to derive a result made it time-consuming and prone to error. Crater was validated using small pieces of foam and ice on single tiles. During the process of turning empirical data into a predictive equation, the limitations and contingencies of these initial data sets were lost.[61] Furthermore, the process of computerization of Crater rendered the uncertainties inherent in the tool even more invisible, and the specific mode of computerization, a plug-in-the-numbers spreadsheet, gave a false sense of clarity and certainty to the results. Thus, an engineer unaware of the history of the tool and its limita-

58. See Sherry Turkle, *The Second Self: Computers and the Human Spirit* (New York: Simon & Schuster, 1984); and Sherry Turkle, *Life on the Screen: Identity in the Age of the Internet* (New York: Simon & Schuster, 1995), for an examination of how interaction through the mediation of computers changes identity. More specifically, Dominique Vinck and Eric Blanco, *Everyday Engineering: An Ethnography of Design and Innovation*, *Inside Technology* (Cambridge, MA: MIT Press, 2003), and Susan Leigh Star, *The Cultures of Computing* (Oxford, U.K., and Cambridge, MA: Blackwell Publishers, 1995), start to address how engineering and scientific work has changed.

59. For a general overview of computing since World War II, see Paul E. Ceruzzi, *A History of Modern Computing*, 2nd ed. (Cambridge, MA: MIT Press, 2003). Paul E. Ceruzzi, *Beyond the Limits: Flight Enters the Computer Age* (Cambridge, MA: MIT Press, 1989), provides a good outline of the introduction of computers into aerospace, although the focus of the work is on-board computers rather than ground equipment or design tools. Gary Lee Downey, *The Machine in Me: An Anthropologist Sits among Computer Engineers* (New York: Routledge, 1998), and Louis L. Bucciarelli, *Designing Engineers*, *Inside Technology* (Cambridge, MA: MIT Press, 1994), both provide ethnographies of engineering that discuss the effects of the ubiquity of computers in the workplace.

60. For a good overview of this topic, see Sergio Sismondo and Snait Gissis, "Practices of Modelling and Simulation," *Special Issue of Science in Context* 12 (1999). George E. Smith, "The Dangers of Cad," *Mechanical Engineering* (February 1986), gives an early warning of the dangers of increasingly closed simulation tools.

61. Allen Richardson interview, by A. Brown, 15 February 2005.

tions, as was the Boeing engineer who did the *Columbia* analysis, could not know that the predictive powers of Crater were unknown outside a limited range of values. The piece of foam that fell from *Columbia*'s external tank was 640 times larger than Crater's valid range. The Crater model predicted that the foam strike would have broken entirely through the Thermal Protection System of the Shuttle and exposed the aluminum wing structure.[62] But because the engineers were aware that there were limitations to the tool, but not aware of how to correct or modify the model, they dismissed their results as too conservative and not predictive of a problem.

This example shows that the Boeing engineers were working in a mode of engineering where their relationships to the materials and objects that they build and study were profoundly mediated through a computer and profoundly dependent on the uncritical acceptance of the findings and assumptions of previous generations of engineers. In January 2003, Boeing engineers and NASA's Debris Assessment Team had no choice but to accept the results of their Crater analysis. Their reliance on a computer model, with the inherent lack of access to the mechanics of the model, let alone the assumptions and uncertainties underlying it, had profoundly affected their ability to make engineering judgments. A similar story can be told about the External Tank bolt catchers—their safety margin, flagged by the Board as dangerously low and a possible source of disaster, was computed using ancient data sets whose origins and limitations had been obscured by computerization.[63]

Engineering Education

There is a growing trend in the history of science to look towards pedagogy as a lens through which to understand how science and scientists come to be.[64] David Kaiser writes, "Scientists are not born, they are made. The ways in which this happens bears the marks of time and place."[65] This observation holds equally true for engineers. Engineering education has changed since Apollo 1. In the late 1960s, engineering schools started to move towards

62. CAIB, *Report*, pp. 144–145.

63. Ibid., pp. 86–88.

64. David Kaiser, *Pedagogy and the Practice of Science: Historical and Contemporary Perspectives* (Cambridge, MA: MIT Press, 2005), is a collection of essays examining science pedagogy over a variety of disciplines, places, and times. Andrew Warwick, *Masters of Theory: Cambridge and the Rise of Mathematical Physics* (Chicago: The University of Chicago Press, 2003), a study of mathematical training in 19th-century Cambridge and its relationship to 19th-century physics in Britain, is perhaps the most sustained development of the argument for the value of the study of pedagogy. Sharon Traweek, *Beamtimes and Lifetimes: The World of High Energy Physicists* (Cambridge, MA: Harvard University Press, 1988), examines contemporary Japanese physicists and identifies education as critical in the formation of a distinctively Japanese way of doing physics.

65. Kaiser, *Pedagogy and the Practice of Science,* p. 1.

engineering science and away from engineering design as a model for the discipline.[66] Engineering students were required to take classes in physics, math, and chemistry to give them a thorough grounding in the physical sciences before going on to engineering classes. The ongoing effects of the National Defense Education Act of 1958 meant changes towards more easily teachable and assessable modes of learning as educators struggled to manage massive expansions in class sizes.[67] The combination of these two trends meant that for many freshmen and sophomores in the 1970s, engineering meant doing physics and math problem sets rather than sketching, building, and working with their hands.[68] This mode of learning fit well with the growing presence of computers in education, providing students with the mathematical tools needed to build and use their own software. As computers became ubiquitous, so engineering schools brought computing into engineering education.

These changes served to both render engineering more abstract and arcane, less connected to its objects of study, and to make it more automated. Both the *Challenger* and *Columbia* reports are critical of the relationships between NASA and its contractors, and particularly critical of the lack of engineering design and development capacity amongst some of the contractors.[69] Embodying engineering judgment in computer programs can devalue that judgment when embodied in engineers, leading to downgrading of the institutional value placed on engineers as employees. This leaves engineers and their skills more vulnerable to privatization and commodification and hence leads to the downgrading of the engineering design capacity of commercial organizations.

The new discipline of astronautics or astronautical engineering was also emerging over this period, intertwined with the development of NASA as an

66. Rosalind H. Williams, *Retooling: A Historian Confronts Technological Change* (Cambridge, MA: MIT Press, 2002), pp. 40–42.

67. Barbara Barksdale Clowse, *Brainpower for the Cold War: The Sputnik Crisis and National Defense Education Act of 1958* (Westport, CT: Greenwood Press, 1981), examines the initial responses to the Sputnik crisis. David Kaiser, "Scientific Manpower, Cold War Requisitions, and the Production of American Physicists after World War II," *Historical Studies in the Physical and Biological Sciences* 33 (fall 2002), looks specifically at the relationship between Cold War geopolitics and changing styles of science and education during this period.

68. Both Kathryn Henderson, *On Line and on Paper: Visual Representations, Visual Culture, and Computer Graphics in Design Engineering, Inside Technology* (Cambridge, MA: MIT Press, 1999), and Eugene S. Ferguson, *Engineering and the Mind's Eye* (Cambridge, MA: MIT Press, 1992), examine the changes in engineering brought about by changes in the ways in which students learn to interact with the material world. Ferguson discusses the loss of a visual intuitiveness amongst young engineers brought about by a move to a more analytic style of engineering in the 1960s and 1970s. Henderson looks at the ways in which engineering knowledge and practices are transformed when computer visualization tools are introduced into the workshop and drafting room.

69. Presidential Commission on the Space Shuttle *Challenger* Accident, *Report to the President*, pp. 194–195; CAIB, *Report*, pp. 110–118.

engineering science and away from engineering design as a model for the discipline.[66] Engineering students were required to take classes in physics, math, and chemistry to give them a thorough grounding in the physical sciences before going on to engineering classes. The ongoing effects of the National Defense Education Act of 1958 meant changes towards more easily teachable and assessable modes of learning as educators struggled to manage massive expansions in class sizes.[67] The combination of these two trends meant that for many freshmen and sophomores in the 1970s, engineering meant doing physics and math problem sets rather than sketching, building, and working with their hands.[68] This mode of learning fit well with the growing presence of computers in education, providing students with the mathematical tools needed to build and use their own software. As computers became ubiquitous, so engineering schools brought computing into engineering education.

These changes served to both render engineering more abstract and arcane, less connected to its objects of study, and to make it more automated. Both the *Challenger* and *Columbia* reports are critical of the relationships between NASA and its contractors, and particularly critical of the lack of engineering design and development capacity amongst some of the contractors.[69] Embodying engineering judgment in computer programs can devalue that judgment when embodied in engineers, leading to downgrading of the institutional value placed on engineers as employees. This leaves engineers and their skills more vulnerable to privatization and commodification and hence leads to the downgrading of the engineering design capacity of commercial organizations.

The new discipline of astronautics or astronautical engineering was also emerging over this period, intertwined with the development of NASA as an

66. Rosalind H. Williams, *Retooling: A Historian Confronts Technological Change* (Cambridge, MA: MIT Press, 2002), pp. 40–42.

67. Barbara Barksdale Clowse, *Brainpower for the Cold War: The Sputnik Crisis and National Defense Education Act of 1958* (Westport, CT: Greenwood Press, 1981), examines the initial responses to the Sputnik crisis. David Kaiser, "Scientific Manpower, Cold War Requisitions, and the Production of American Physicists after World War II," *Historical Studies in the Physical and Biological Sciences* 33 (fall 2002), looks specifically at the relationship between Cold War geopolitics and changing styles of science and education during this period.

68. Both Kathryn Henderson, *On Line and on Paper: Visual Representations, Visual Culture, and Computer Graphics in Design Engineering, Inside Technology* (Cambridge, MA: MIT Press, 1999), and Eugene S. Ferguson, *Engineering and the Mind's Eye* (Cambridge, MA: MIT Press, 1992), examine the changes in engineering brought about by changes in the ways in which students learn to interact with the material world. Ferguson discusses the loss of a visual intuitiveness amongst young engineers brought about by a move to a more analytic style of engineering in the 1960s and 1970s. Henderson looks at the ways in which engineering knowledge and practices are transformed when computer visualization tools are introduced into the workshop and drafting room.

69. Presidential Commission on the Space Shuttle *Challenger* Accident, *Report to the President*, pp. 194–195; CAIB, *Report*, pp. 110–118.

organization.[70] The new discipline drew heavily on the principles of aeronautical engineering but taught students how to apply these principles in higher stress environments—at higher temperatures and pressures, with higher aerodynamic loads, in high-radiation environments, using finer tolerance manufacturing, and with larger and more complex vehicle systems. The new discipline of astronautical engineering had to learn how to manage problems with testing the massive vehicles it built. In many cases, it was physically impossible to adequately test astronautical hardware, and so new methods of producing knowledge about complex systems like computer modeling and simulation were developed. The Apollo 204 report illustrates the engineering challenges that accompanied the transition from designing and developing craft to operate within the atmosphere to craft designed to operate in the space environment. As the report makes clear, the levels of both precision and complexity needed to build a spacecraft grew dramatically, perhaps beyond the capacity of North American Aviation engineers to keep up. As astronautics developed, engineering scale, engineering knowledge, and engineering management changed.

The Systems Approach

Systems engineering as a philosophy emerged from the complex military defense projects of the 1950s. It can be best described as a "set of organizational structures and processes to rapidly produce a novel but dependable technological artifact within a predictable budget."[71] Systems engineering was one element in a long history of the application of scientific and engineering principles to complex commercial or organizational problems, a history that started with Taylorism and scientific management in the late 19th century.[72] Systems engineering involved the use of engineering ideas to organize large engineering projects—most profoundly, systems engineering defines project

70. W. Henry Lambright, *Powering Apollo: James E. Webb of NASA* (Baltimore: John Hopkins, 1995); W. Henry Lambright, Edwin A. Bock, and Inter-university Case Program, *Launching NASA's Sustaining University Program* (Syracuse, NY: Inter-university Case Program, 1969); Howard E. McCurdy, *Inside NASA: High Technology and Organizational Change in the U.S. Space Program* (Baltimore: Johns Hopkins, 1993).

71. Stephen B. Johnson, *The Secret of Apollo: Systems Management in American and European Space Programs* (Baltimore: Johns Hopkins, 2002), p. 17.

72. See James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, MA: Harvard University Press, 1986), and JoAnne Yates, *Control through Communication: The Rise of System in American Management* (Baltimore: Johns Hopkins, 1989), for a brief introduction to the literature on system and scientific management. Robert Kanigel, *The One Best Way: Frederick Winslow Taylor and the Enigma of Efficiency* (New York: Viking, 1997), and Hugh G. J. Aitken, *Scientific Management in Action: Taylorism at Watertown Arsenal, 1908–1915* (Princeton, NJ: Princeton University Press, 1985), both provide excellent introductions to Taylor and scientific management.

management as an engineering problem best solved by engineers and engineering practice. In this philosophy, management becomes a subset of engineering practice. The large SAGE (Semi-Automatic Ground Environment) air defense and Atlas missile projects trained a generation of engineers how to apply systems engineering ideas to complex research, development, and manufacturing projects.[73] Systems management experts from the Air Force and the aerospace industry were brought into NASA to manage the Apollo program as it grew in the 1960s.[74] The Apollo 204 accident marks the moment of transition into a full acceptance of systems engineering as the guiding philosophy of the space program, whereas throughout the early part of the 1960s, there was tension between the aircraft manufacturers and the missile-program-trained NASA engineering managers. Indeed, the most common historiographical interpretation of the larger significance of Apollo 204 is simply that—the fire forced NASA and its contractors to find new ways of managing the complexity of the Apollo program, and systems management was the new way.[75]

The manned spaceflight community within NASA made the transition from research and development to being primarily an operational organization in the 1980s and 1990s, as the focus of the U.S. manned spaceflight program moved from exploration to ready access to low-Earth orbit. Systems engineering as an overarching philosophy for the management of complexity was replaced with new approaches drawn from both the business and government worlds. This does not mean that the tools that collectively made up systems engineering—configuration control boards, integrated management

73. Agatha C. Hughes and Thomas Parke Hughes, *Systems, Experts, and Computers: The Systems Approach in Management and Engineering, World War II and After, Dibner Institute Studies in the History of Science and Technology* (Cambridge, MA: MIT Press, 2000); Thomas Parke Hughes, *Rescuing Prometheus*, 1st ed. (New York: Pantheon Books, 1998); and Kent C. Redmond and Thomas M. Smith, *From Whirlwind to Mitre: The R&D Story of the SAGE Air Defense Computer* (Cambridge, MA: MIT Press, 2000), all discuss the origins of systems management in the ballistic missile and air defense programs of the 1950s.

74. Johnson's *The Secret of Apollo: Systems Management in American and European Space Programs* is by far the most comprehensive examination of the rise of systems management in the U.S. space program. See also Arnold S. Levine, *Managing NASA in the Apollo Era* (Washington, DC: NASA SP-4102, 1982); John M. Logsdon, *Managing the Moon Program: Lessons Learned from Project Apollo: Proceedings of an Oral History Workshop* (Washington, DC: NASA SP-4514, 1999).

75. For examples of this type of interpretation, see Andrew Chaikin and Tom Hanks, *A Man on the Moon: The Voyages of the Apollo Astronauts* (New York: Penguin Books, 1998), chap. 1; Charles A. Murray and Catherine Bly Cox, *Apollo, the Race to the Moon* (New York: Simon & Schuster, 1989), chaps. 15–16; William E. Burrows, *This New Ocean: The Story of the Space Age*, 1st ed. (New York: Random House, 1998), pp. 406–415. Astronaut and flight controller biographies make a similar point. See, for example, Frank Borman and Robert J. Serling, *Countdown: An Autobiography*, 1st ed. (New York: W. Morrow, 1988), chap. 9; Michael Collins, *Carrying the Fire: An Astronaut's Journeys* (New York: Farrar, 1974), pp. 269–275; Christopher C. Kraft, *Flight: My Life in Mission Control* (New York: Dutton, 2001), pp. 269–278; Gene Kranz, *Failure Is Not an Option: Mission Control from Mercury to Apollo 13 and Beyond* (New York: Simon & Schuster, 2000), pp. 208–214.

systems, resident program offices at contractors—ceased to be used, but rather that the philosophy that a collection of these tools was the best way to manage a program was replaced by other ways of thinking.[76]

Total Quality Management, reengineering, and "faster, better, cheaper" took the place of systems engineering in the 1990s, part of a larger cultural trend in the United States that valorized the business approach to organization and emphasized the merits of private free-enterprise solutions to problems previously thought the realm of government.[77] The idea of using scientific and engineering principles to solve business and organizational challenges was replaced by the application of business and commercially derived management philosophy to an engineering organization.

Changes in engineering practice over the 1970s, 1980s, and 1990s meant that engineers in the manned space program were working in the increasingly mediated environment of computer-based engineering whilst working on technological systems that were becoming increasingly complex, difficult to test, and designed to operate at an increasingly high performance envelope. Margins for error grew ever smaller, whilst the computer-based tools being used to manage that margin grew increasingly less transparent. At the same time, the shared organizational philosophy of systems engineering was being abandoned by senior management in favor of more commercially oriented ideas, while engineers still used the tools of systems management.

FURTHER RESEARCH

There are several areas that call for further research in order to put together a picture of changes in engineering in the U.S. manned space program. The first area is studies of engineering in practice in the late 20th century. Although the genre of engineering ethnographies is growing, it is still small. Some of these studies examine the impact of computers in the engineering workplace, but none do so in the context of aeronautics or astronautics. Howard McCurdy's work on NASA culture provides an excellent base to work from but focuses on organizational change rather than engineering change from the 1970s onwards.[78] Furthermore, the field needs not just in-depth studies of engineering practice, but broad-scope surveys comparable to Sylvia Fries's *NASA Engineers in the Age of Apollo*.[79] We do not yet know

76. See CAIB, *Report*, pp. 105–110.

77. Howard E. McCurdy, *Faster, Better, Cheaper: Low-Cost Innovation in the U.S. Space Program* (Baltimore: Johns Hopkins, 2001).

78. McCurdy, *Inside NASA: High Technology and Organizational Change in the U.S. Space Program*; McCurdy, *Faster, Better, Cheaper: Low-Cost Innovation in the U.S. Space Program*.

79. Sylvia Doughty Fries, *NASA Engineers and the Age of Apollo* (Washington, DC: NASA SP-4104, 1992).

enough about the educational and demographic characteristics of NASA engineers from the 1970s onwards.

There is a need for a body of literature on the recent institutional and cultural history of engineering comparable to the literature on the rise of the engineering profession in the later half of the 19th century. We know much about the ways in which engineers developed a clearly articulated professional identity, created a standardized curriculum and accreditation process, and made themselves middle-class in the late 19th century.[80] We know much about the engineering triumphs of the early 20th century and the involvement of engineers in the winning of World War II and the Cold War, both as producers of military technology but also as the creators of the consumer society.[81] But we know little about how engineers have responded to changing economic and cultural circumstances since the 1960s.

We need more nuanced histories of the NASA of the 1970s, 1980s, and 1990s. Reflecting the ongoing cultural legacy of the Apollo program, much of the literature on the U.S. manned spaceflight program focuses on the triumphs of the 1960s. Those histories that do attempt to cover the entire history of the program tend to fall into a declensionist mode of writing, discussing NASA's decline and fall from Apollo. A more nuanced understanding of the legacy of the Apollo program, including a more realistic assessment of the relative safety of Apollo and Shuttle missions, might serve to provide a new framework in which to understand the history of NASA over this period.

80. For example, see Edwin T. Layton, *The Revolt of the Engineers: Social Responsibility and the American Engineering Profession* (Cleveland: Press of Case Western Reserve University, 1971); George S. Emmerson, *Engineering Education: A Social History* (New York: David & Charles; Crane, 1973); David F. Noble, *America by Design: Science, Technology, and the Rise of Corporate Capitalism*, 1st ed. (New York: Knopf, 1977); Brendan Patrick Foley, "Fighting Engineers: The U.S. Navy and Mechanical Engineering, 1840–1905" (Ph.D. thesis, MIT, June 2003).

81. See Thomas Parke Hughes, *American Genesis: A Century of Invention and Technological Enthusiasm, 1870–1970* (New York: Penguin Books, 1990); David A. Hounshell, *From the American System to Mass Production, 1800–1932: The Development of Manufacturing Technology in the United States* (Baltimore: Johns Hopkins, 1984); Terry S. Reynolds, *The Engineer in America: A Historical Anthology from Technology and Culture* (Chicago: University of Chicago Press, 1991).

Chapter 13

Institutional Issues for Continued Space Exploration: High-Reliability Systems Across Many Operational Generations—Requisites for Public Credibility[1]

Todd R. La Porte

Highlighting critical issues arising from the evolution of a large government enterprise is both important and occasionally painful and sometimes provides a basis for exciting next steps. Calling out critical technical issues from past developments inspires engineers and makes visible to policymakers likely requests for program funding to address them. A "critical issues" focus also holds the promise of exploring other sorts of issues: those that arise in deploying technologies.[2] These are particularly interesting when they entail large-scale organizations that are judged to be highly hazardous.

This paper highlights the challenges and issues involved when we wish large, technically rooted organizations to operate *far more* effectively, with *much less* error than they should be expected to exhibit—given what we know about organizations more generally. Recall that "Murphy's Law" and trial-and-error learning are reasonably accurate descriptors of how all organizations generally behave. Routinely expecting otherwise is quite remarkable.

First, let us set a context. In your mind's eye, imagine space-related activities two or three decades into the future. President George W. Bush's current vision for NASA focused the Agency's efforts in the early 21st century, and

1. This paper draws on presentations to the Workshop on Space Policy held by the National Academies of Science in Irvine, CA, 12–13 November 2003; the National Academies' Board on Radioactive Waste Management Panels on "Principles and Operational Strategies for Staged Repository Systems," 27 June 2001, and "Long-Term Institutional Management of Hazards Sites," 7 August 2001, both held in Washington, DC; and the American Association for the Advancement of Science (AAAS) symposium, "Nuclear Waste: File and Forget? Institutional Challenges for High-Reliability Systems Across Many Operational Generations—Can Watchfulness Be Sustained?" held in Denver, CO, 18 February 2003. Since these presentations were given to quite different, nearly mutually exclusive audiences, the various conference sponsors have agreed to this repetition.

2. This conference on "Critical Issues" casts a wider net and includes issues relevant to the understanding of policy development, technical operations as well as systems safety, and the conduct of historical studies of large systems per se.

our reach has extended to periodic flights to the Moon and to an international space platform.[3] With international cooperation, three to four major launches and recoveries a year have become more or less routine. Another six or seven unmanned launches resupply the Station and various probes for scientific programs. Assume that national intelligence and communications demands require another half dozen annually. And imagine that commercial spaceflight enthusiasts have found enough "venture capitalists" and adventurers to sustain several highly visible, elite space experiences. This is edging toward 20 launches a year and evokes images of science fiction and early *Star Trek* tableaux.

This sort of future moves us well beyond the sharply defined, novel images of machinery and spectacularly framed astronauts spacewalking against the black of the heavens. It conjures the extraordinary organizations that these activities imply. There would be the early vestiges of, say, a U.S.–European Union space traffic control—analogous to the existing global air traffic control system—alert to tracking both space vehicles and the detritus of former flights, closely concentrating on bringing each flight to rest without encountering objects aloft or mishaps of human or mechanical origin. Operational scope would be widespread and expected to continue indefinitely. This organizational reach is extraordinary. It immediately raises the question of the "operational sustainability" of NASA's space missions, especially those that propel humans into space.

The missions and the technologies that typify NASA and its industrial contractors prompt demands that NASA programs exhibit highly reliable, humanly safe operations, often projected to continue for a number of management generations (say some 10 to 15 years each). NASA has, in the past, taken up these challenges emphasizing both engineering controls and administrative controls that embrace safety and effective performance.

This paper highlights a third emphasis: the organizational relationships and safety culture of the Agency and its contractors that would manage an astonishing array of complicated technical systems and far-flung facilities making up a global space complex. It draws on work examining the operations of several mature, large-scale technical systems. Then it considers in this light the qualities likely to be necessary in the evolution of NASA's humans-in-space activities if they are routinely to achieve a high degree of public acceptance and sustained credibility.

Putting the question directly: What organizational conditions have arisen when the operating technologies are so demanding or hazardous that trial-

3. President George W. Bush, "A Renewed Spirit of Discovery: The President's Vision for U.S. Space Exploration," 14 January 2004, folder 12886, NASA Historical Reference Collection, Washington, DC. For NASA's most recent expression of this declaration, see NASA, "The New Age of Exploration: NASA's Direction for 2005 and Beyond," February 2005, same folder. The operative portion from the mission: "To understand and protect our home planet, To explore the universe and search for life, To inspire the next generation of explorers."

and-error learning, while likely, no longer seems to be a confident mode of learning and when the next error may be your last trial?

What can be said about managing large-scale technical systems, responsible for often highly hazardous operations on missions that imply operational stability for many, many years? The institutional design challenges are to provide the work structures, institutional processes, and incentives in such ways that they assure highly reliable operations[4] over the very long term—perhaps up to 50 years[5]—in the context of continuously high levels of public trust and confidence.[6] My purpose here is less to provide a usable explication of these concepts (see the supporting references) and more to demonstrate, by a blizzard of lists, the complexity and range of the institutional conditions implied by NASA's program reach. I foreground properties that are especially demanding, keeping these questions in mind: How often and at what effort does one observe these characteristics in the organizational arenas you know best? Could one imagine such an ensemble within NASA in the foreseeable future?

PURSUING HIGHLY RELIABLE OPERATIONS

Meeting the challenges of highly reliable operations has been demonstrated in enough cases to gain a rough sense of the conditions that seem associated with extraordinary performance. These include both internal processes and external relations. What can be said with some confidence about the qualities NASA managers and their overseers could seek?[7] (See table 13.1.)

---

4. Initial empirical work included close study of the operations of U.S. Air Traffic Control, aircraft carriers at sea, and nuclear power plants. For summaries, see G. I. Rochlin, "Reliable Organizations: Present Research and Future Directions," and T. R. La Porte, "High Reliability Organizations: Unlikely, Demanding and at Risk," both in *Journal of Crisis and Contingency Management* 4, no. 2 (June 1996): 55–59 and 60–71, respectively; T. R. La Porte and P. M. Consolini, "Working in Practice but not in Theory: Theoretical Challenges of High Reliability Organizations," *Journal of Public Administration Research and Theory* 1, no. 1 (January 1991): 19–47; K. H. Roberts, "New Challenges to Organizational Research: High Reliability Organizations," *Industrial Crisis Quarterly* 3 (1989): 111–125.

5. Prompting the concept of "institutional constancy." See discussion later in this chapter, along with T. R. La Porte and A. Keller, "Assuring Institutional Constancy: Requisites for Managing Long-Lived Hazards," *Public Administration Review* 56, no. 6 (November/December 1996): 535–544.

6. In the context of this paper, sustaining public trust and confidence, while a very important consideration, takes second seat to the issues of reliable operations across multiple generations. Public trust is a condition that evokes high institutional demands and calls for a discussion that extends beyond the limitations of this paper. See, for example, U.S. Department of Energy (DOE), "Earning Public Trust and Confidence: Requisite for Managing Radioactive Waste. Report of the Task Force on Radioactive Waste Management, Secretary of Energy Advisory Board," November 1993, available online at *http://www.seab.energy.gov/publications/trust.pdf*; T. R. La Porte and D. Metlay, "Facing a Deficit of Trust: Hazards and Institutional Trustworthiness," *Public Administration Review* 56, no. 4 (July–August 1996): 341–347.

7. Draw generalized inferences from this discussion with care. These findings are based mainly on three types of organizations, each with a limited number of cases, and bits from others (e.g., K. H.

continued on the next page

Table 13.1. Characteristics of Highly Reliable Organizations (HROs)

Internal Processes

1. Strong sense of mission and operational goals, commitment to highly reliable operations, both in production and safety.
2. Reliability-enhancing operations.
    A. Extraordinary technical competence.
    B. Sustained, high technical performance.
    C. Structural flexibility and redundancy.
    D. Collegial, decentralized authority patterns in the face of intense, high-tempo operational demands.
    E. Flexible decision-making processes involving *operating teams*.
    F. Processes enabling continual search for improvement.
    G. Processes that reward the discovery and reporting of error, *even one's own*.
3. Organizational culture of reliability, including norms, incentives, and management attitudes that stress the equal value of reliable production and operational safety.

External Relationships

1. External "watching" elements.
    A. Strong superordinate institutional visibility in parent organization.
    B. Strong presence of stakeholding groups.
2. Mechanisms for "boundary spanning" between the units and these watchers.
3. Venues for credible operational information on a timely basis.

---

continued from the previous page

Roberts, "Some aspects of organizational cultures and strategies to manage them in reliability enhancing organizations," *Journal of Managerial Issues* 5 [1993]: 165–181). Though these organizations operate in quite different institutional milieus, we cannot say they represent a systematic sample. No one now knows what the population of HROs might be. And highly reliable operations are keenly sought for situations that are not so dramatically hazardous in the physical sense, e.g., HRO operations in financial transactions or in the performance of sophisticated computer chips or large software programs. See K. H. Roberts and C. Libuser, "From Bhopal to banking: Organizational design can mitigate risk," *Organizational Dynamics* 21 (1993): 15–26. In these situations, motivation stems from fear of serious financial losses that are seen as amounting to institutional, not physical, death.

Internal Processes[8]

Organizationally defined intention. High-reliability organizations (HROs) exhibit a strong sense of mission and operational goals that stress assuring ready capacity for production and service with an *equal* commitment to reliability in operations and a readiness to invest in reliability-enhancing technology, processes, and personnel resources. In cases such as our space operations, these goals would be strongly reinforced by a clear understanding that the technologies upon which the organizations depend are intrinsically hazardous and potentially dangerous to human and other organisms. It is notable that for U.S. space operations, there is also high agreement within the operating organizations and in the society at large about the seriousness of failures and their potential costliness, as well as the value of what is being achieved (in terms of a combination of symbolic, economic, and political factors). This consensus is a crucial element underlying the achievement of high operational reliability and has, until recently, increased the assurance of relatively sufficient resources needed to carry out failure-preventing/quality-enhancing activities. Strong commitment also serves to stiffen corporate or agency resolve to provide the organizational status and financial and personnel resources such activities require. But resolve is not enough. Evidence of cogent operations is equally crucial.

Reliability-enhancing operations. These include the institutional and operational dynamics that arise when extraordinary performance must be the rule of the day—features that would be reinforced by an organizational culture of reliability, i.e., the norms and work ways of operations.[9] A dominant quality of organizations seeking to attain highly reliable operations is their intensive technical and social interdependence. Characterized by numerous specialized functions and coordination hierarchies, this prompts patterns of complexly related, tightly coupled technical and work processes which shape HROs' social, structural, and decision-making character.[10]

---

8. This section draws strongly from La Porte and Consolini, "Working in Practice but not in Theory"; Rochlin, La Porte, and Roberts, "The self-designing high-reliability organization: Aircraft carrier flight operations at sea," *Naval War College Review* 40, no. 4 (1987): 76–90; La Porte, "High Reliability Organizations"; Rochlin, "Reliable Organizations: Present Research and Future Directions," pp. 55–59; T. R. La Porte, "High Reliability Organizations: Unlikely, Demanding and at Risk," pp. 60–71; K. H. Roberts, "Some characteristics of high reliability organizations," *Organization Science* 1, no. 2 (1990): 160–177; P. R. Schulman, "Negotiated Order of Organizational Reliability," *Administration & Society* 25, no. 3 (November 1993): 356–372.

9. K. E. Weick, "Organizational culture as a source of high reliability," *California Management Review* 29 (1987): 112–127; K. H. Roberts, "Some aspects of organizational cultures and strategies to manage them in reliability enhancing organizations," *Journal of Managerial Issues* 5 (1993): 165–181.

10. La Porte and Consolini, "Working in Practice but not in Theory"; Rochlin, "Reliable Organizations: Present Research and Future Directions"; C. Perrow, *Normal Accidents: Living With High-Risk Technologies* (New York: Basic Books, 1984); K. H. Roberts, K. H. and G. Gargano, "Managing a High Reliability Organization: A Case for Interdependence," in *Managing Complexity in High Technology Industries: Systems and People*, ed. M. A. Von Glinow and S. Mohrmon (New York: Oxford University Press, 1989), pp. 147–159.

The social character of the HRO is typified by high technical/professional competence and performance, as well as thorough technical knowledge of the system and awareness of its operating state.

1. Extraordinary technical competence almost goes without saying. But this bears repeating because continuously attaining very high quality requires close attention to recruiting, training, staff incentives, and ultimately the authority relations and decision processes among operating personnel who are, or should be, consummately skilled at what they do. This means there would be a premium put on recruiting members with extraordinary skills and an organizational capacity to allow them to burnish these skills in situ via continuous training and an emphasis on deep knowledge of the operating systems involved. Maintaining high levels of competence and professional commitment also means a combination of elevated organizational status and visibility for the activities that enhance reliability. This would be embodied by "high reliability professionals"[11] in positions with ready access to senior management. In aircraft carrier operations, this is illustrated where high-ranking officers are assigned the position of Safety Officer reporting directly to the ship's captain.

2. HROs also continuously achieve high levels of operational performance accompanied by stringent quality assurance (QA) measures applied to maintenance functions buttressed by procedural acuity.[12] Extensive performance databases track and calibrate technical operations and provide an unambiguous description of the systems' operating state. NASA's extraordinary investment in collecting system performance data is a prime example of this characteristic. These data inform reliability statistics, quality-control processes, accident modeling, and interpretations of system readiness from a variety of perspectives. In some organizational settings, the effectiveness of these analyses is enhanced by vigorous competition between groups formally responsible for safety.[13]

---

11. P. Schulman, E. Roe, M. van Eeten, and M. de Bruijne, "High Reliability and the Management of Critical Infrastructures," *Journal of Crisis and Contingency Management* 12, no. 1 (March 2004): 14–28. Also see David Mindell's chapter in this book and his attention to the self "identity" of technical operators.

12. Schulman, "Negotiated Order of Organizational Reliability"; M. Bourrier, "Organizing Maintenance Work at Two American Nuclear Power Plants," *Journal of Crisis and Contingency Management* 4, no. 2 (June 1996): 104–112.

13. T. R. La Porte and C. Thomas, "Regulatory Compliance and the Ethos of Quality Enhancement: Surprises in Nuclear Power Plant Operations," *Journal of Public Administration Research and Theory* 5, no. 4 (December 1994): 250–295.

HROs' operations are enabled by structural features that exhibit operational flexibility and redundancy in pursuit of safety and performance, and overlapping or nested layers of authority relationships.

3. Working with complex technologies is often hazardous, and operations are also carried out within quite contingent environments. Effective performance calls for flexibility and "organizational slack" (or reserve capacity) to ensure safety and protect performance resilience. Such structural flexibility and redundancy are evident in three ways: key work processes are designed so that there are parallel or overlapping activities that can provide backup in the case of overload or unit breakdown and operational recombination in the face of surprise; operators and first-line supervisors are trained for multiple jobs via systematic rotation; and jobs and work groups are related in ways that limit the interdependence of incompatible functions.[14] NASA has devoted a good deal of attention to aspects of these features.

The three characteristics noted so far are, in a sense, to be expected and command the attention of systems engineering and operational managers in NASA and other large-scale technical programs. There is less explicit attention to understanding the organizational relationships that enhance their effectiveness. I give these a bit more emphasis below.

4. Patterns of formal authority in large organizations are likely to be predominately hierarchical (though this may have as much to do with adjudicative functions as directive ones). And, of course, these patterns are present in HROs as well. Top-down, commandlike authority behaviors are most clearly seen during times of routine operations. But importantly, two other authority patterns are also "nested or overlaid" within these formal relations. Exhibited by the same participants who, during routine times, act out the roles of rank relations and bureaucrats, in extraordinary times, when the tempo of operations increases, another pattern of collegial and functionally based authority relationships takes form. When demands increase, those members

14. For work on functional redundancy, see especially M. Landau, "Redundancy, Rationality, and the Problem of Duplication and Overlap," *Public Administration Review* 27 (July/August 1969): 346–358; A. W. Lerner, "There is More Than One Way to be Redundant: A Comparison of Alternatives for the Design and Use of Redundancy in Organizations," *Administration & Society* 18 (November 1986): 334–359; D. Chisholm, *Coordination Without Hierarchy: Informal Structures in Multi-organizational Systems* (Berkeley: University of California Press, 1989); C. F. L. Heimann, "Understanding the *Challenger* Disaster: Organizational Structure and the Design of Reliable Systems," *American Political Science Review* 87 (June 1993): 421–435.

who are the most skilled in meeting them step forward without bidding to take charge of the response, while others who may "outrank" them slip informally into subordinate, helping positions.

And nested within or overlaid upon these two patterns is yet another well-practiced, almost scripted set of relationships that is activated during times of acute emergency. Thus, as routine operations become high-tempo, then perhaps emergencies arise, observers see communication patterns and role relationships changing to integrate the skills and experience apparently called for by each particular situation. NASA has had dramatic experience with such patterns.

Within the context of HROs' structural patterns, decision-making dynamics are flexible, dispersed among operational teams, and include rewards for the discovery of incipient error.

5. Decision-making within the shifting authority patterns, especially operating decisions, tends to be decentralized to the level where actions must be taken. Tactical decisions often develop on the basis of intense bargaining and/or collegial interaction among those whose contributions are needed to operate effectively or problem-solve. Once determined, decisions are executed, often very quickly, with little chance for review or alteration.[15]

6. Due in part to the irreversibility of decisions once enacted, HROs put an unusual premium on assuring that decisions will be based on the best information available. They also try to insure that their internal technical and procedural processes, once put in motion, will not become the sources of failure. This leads, as it has within NASA, to quite formalized efforts, continually in search of improvement via systematically gleaned feedback, and periodic program and operational reviews. These are frequently conducted by internal groups formally charged with searching out sources of potential failure, as well as improvements or changes in procedures to minimize the likelihood of failure. On occasion, there may be several groups structured and rewarded in ways that puts them in direct competition with each other to discover potential error, and, due to their formal attachment to different reporting levels of the management hierarchy, this encourages the quick forwarding of information about potential flaws to higher authority.[16]

15. Roberts, "Some characteristics of high reliability organizations"; Schulman, "Negotiated Order of Organizational Reliability."

16. La Porte and Thomas, "Regulatory Compliance and the Ethos of Quality Enhancement"; Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (Chicago: University of Chicago Press, 1990).

> Notably, these activities, due to their intrinsic blame-placing potential, while they may be sought by upper management in a wide variety of other types of organizations, are rarely conducted with much enthusiasm at lower levels. In response, HROs exhibit a most unusual willingness to reward the discovery and reporting of error without peremptorily assigning blame for its commission at the same time. This obtains even for the reporting of one's own error in operations and procedural adherence. The premise of such reward is that it is better and more commendable for one to report an error immediately than to ignore or to cover it up, thus avoiding untoward outcomes as a consequence. These dynamics rarely exist within organizations that operate primarily on punishment-centered incentives, that is, most public and many private organizations.

Organizational culture of reliability. Sustaining the structural supports for reliability and the processes that increase it puts additional demands on the already intense lives of those who operate and manage large-scale, advanced technical systems. Operating effectiveness calls for a level of personal engagement and attentive behavior that is unlikely to be manifest merely on the basis of formal rules and economic employee contracts. It requires a fully engaged person responding heedfully to norms of individual and group relations that grow out of the particular demands and rewards of the hazardous systems involved.[17] For lack of a better concept to capture these phenomena, let us accept the slippery concept of "organizational culture" as a rough ordering notion.[18] A culture of organizational reliability refers to the norms, shared perceptions, work ways, and informal traditions that arise within the operating and overseeing groups closely involved with the systems of hazard.[19]

Recall that HROs strive equally for high levels of production and safety.[20] HROs face the challenge of being reliable both as producers (many under all manner of demanding conditions) *and* as safety providers (under conditions of high production demands). While most organizations combine varying

17. Weick, "Organizational culture as a source of high reliability"; Roberts, "Some aspects of organizational cultures."

18. The concept of organizational culture captures the sense that there are norms, values, and "taken for granted" modes of behavior and perceptions that shape interpersonal and group relations. At the same time, the concept retains a high degree operational ambiguity, its use subject to stiff criticism. See J. S. Ott, *The Organizational Culture Perspective* (Chicago: Dorsey Press, 1989); Roberts, "Some aspects of organizational cultures"; G. I. Rochlin, "Les organizations 'a' haute fabilite': bilan et perspective de recherche" (Highly Reliable Organizations: Exploration and Research Perspectives), chap. 2 in *Organiser la fiabilite*, ed. M. Bourrier (Paris: L'Harmattan, 2001).

19. Roberts, "Some characteristics of high reliability organizations"; "Nuclear Power Operations: A Cross-Cultural Perspective," *Annual Review of Energy and the Environment* 19 (1994): 153–187.

20. Cf. Rochlin, "Reliable Organizations: Present Research and Future Directions"; Schulman, "Negotiated Order of Organizational Reliability."

degrees of production plus service/safety emphasis, HROs have continuously to strike a balance. In times of routine, safety wins out formally (though watchfulness is harder to sustain); in times of high tempo/surge, this becomes reordered (though watchfulness is much more acute). This suggests an organizational culture integrating the familiar norms of mission accomplishment and production with those of the so-called safety culture.[21]

Elements of the results are operator/member élan, operator autonomy, and intrinsic tension between skilled operators and technical experts.

- Operating personnel evince an intense élan and strongly held expectations for themselves about the value of skilled performance. In the face of hazard, it takes on a kind of prideful wariness. There are often intense peer-group pressures to excel as a highly competitive team and to cooperate with and assist each other in the face of high operating demands. This includes expectations of fulfilling responsibilities that often go well beyond formal role specifications. For example, there is a view that "whoever spots a problem owns it" until it is mitigated or solved in the interest of full, safe functioning. This sometimes results in operators realizing that, in the face of unexpected contingencies, they may have to "go illegal," i.e., to go against established, formal procedures if the safety operating procedures appear to increase the difficulty of safely meeting the service demands placed on the organization. Operator élan is reinforced by clearly recognized peer-group incentives that signal high status and respect, pride in one's team, emphasis on peer "retention" and social discipline, and reward for contributing to quality-enhancing, failure-preventing activities.

- Hazardous operations are often time-critical, where effectiveness depends on keen situational awareness. When it becomes clear that speedy, decisive action must be taken, there is little opportunity for assistance or approval from others.[22] Partly as a result, HRO operators come to develop, indeed insist upon, a high degree of discretion, autonomy, and responsibility for activities "on their watch."[23] Often typified as being "king of my turf," this is seen as highly appropriate by both other operators and supervisors.

---

21. See G. I. Rochlin, "Safe operations as a social construct," *Ergonomics* 42, no. 11 (1999): 1549–1560; cf. Weick, "Organizational culture as a source of high reliability."

22. See K. E. Weick, K. M. Sutcliffe, and D. Obstfeld, "Organizing for high reliability: Processes of collective mindfulness," *Research in Organizational Behavior* 21 (1999): 81–123, for a related perspective.

23. K. H. Roberts, D. M. Rousseau, and T. R. La Porte, "The culture of high reliability: Quantitative and qualitative assessment aboard nuclear powered aircraft carriers," *Journal of High Technology Management Research* 5, vol. 1 (spring 1994): 141–161.

- But operator autonomy is often bought at a moderate price. The HROs we studied all operated complex technical systems that put a premium on technical engineering knowledge as well as highly skilled operating knowledge and experience. These two types of skills are usually formally distinguished in the occupational roles designations within HROs. Each has a measure of status; each depends on the other for critical information in the face of potential system breakdown and recovery if problems cannot be contained. But in the operators' eyes, *they* have the ultimate responsibility for safe, effective operation. They also have an almost tactile sense of how the technical systems actually function in the organization's operating environments, environments that are likely to be more situationally refined and intuitively more credibly understood than can be derived from the more abstract, cognitively based knowledge possessed by engineers. The result is an intrinsic tension between operators and technical experts, especially when operators judge technical experts to be distant from actual operations, where there is considerable confidence placed on tacit knowledge of system operations based on long operating experience.[24]

These dominant work ways and attitudes about behavior at the operating levels of HROs are prompted by carrying out activities that are closest to the hazards and suggest the important affective nature of HRO dynamics. These patterns provide the basis for the expressive authority and "identitive compliance"[25] norms that sustain the close cooperation necessary when facing the challenges of unexpected high-tempo/high-surge situations with minimum internal harm to people and capital equipment. But HROs operate in the context of many interested outsiders: sponsors, clients, regulators, and surrounding neighborhoods. Relations with outside groups and institutions also play a crucial role.

External Relationships

HRO performance is clearly dependent on extraordinarily dense patterns of cooperative behavior within the organization. These are extensive, often quite intense, and unusual both in terms of achieving continuous reliability and in higher costs. As such, they are difficult to sustain in the absence of external reinforcement. Continuous attention both to achieving organizational missions and to avoiding serious failures requires repeated interactions with—one might

24. G. I. Rochlin and A. von Meier, "Nuclear Power Operations: A Cross-Cultural Perspective," pp. 153–187; Rochlin, "Safe operations."

25. See A. Etzioni, "Organizational Control Structure," chap. 15 in *Handbook of Organizations*, ed. J. G. March (Chicago: Rand McNally, 1965), pp. 650–677.

say pressures from—elements in the external environment, not only to insure resources, but, as importantly, to buttress management resolve to maintain the internal relations outlined above and to nurture HROs' culture of reliability. These cultural characteristics are the most important of all the properties of HROs, for if they are absent, the rest are difficult to achieve and sustain.

NASA has certainly learned how external interests—we will call them "the watchers"—can enter into the Agency's everyday life, especially when major failures are seized upon as a chance to ventilate concerns about operational reliability.[26] "Watchers" include externally situated, independent public bodies and stakeholding interest groups and the institutional processes that assure their presence, efficacy, and use of tools for external monitoring in the interest of hazard evaluations.

Aggressive, knowledgeable "watchers" increase the likelihood that a) reliability-enhancing operations and investments will be seen as legitimate by corporate and regulatory actors, b) such costs *should* be absorbed, and c) regulations and internal social demands should be allowed in the interest of safety. This may mean investing, on one hand, in developing and training external review groups and in some instruments of behavioral surveillance, e.g., random drug tests, and, on the other, assuring these "watchers" that HRO leaders will quickly be held accountable for changes that could reduce reliability in service or safety. These watching groups may be either formal or informal and are found both within the HRO's immediate institutional environment, e.g., congressional committees, and outside it.

It is crucial that there be clear institutional interests in highly reliable performance. This should be evident in strong, superordinate institutional elements of the parent organization, such as agency and corporate headquarters or command-level officers (e.g., utility corporate headquarters, higher military command, and Washington agency headquarters), and sometimes industrial association watchdogs (e.g., the nuclear industry's Institute for Nuclear Power Operators, or INPO).[27]

At the same time, the persistent presence of external stakeholding groups assures attentiveness (and occasional resentment). These groups range from quite formal public watchers, such as regulatory overseers (e.g., state Public Utility Commissions, Nuclear Regulatory Commissions, the Environmental Protection Agency, the Federal Emergency Management Agency, and the Occupational Safety and Health Administration), user and client groups (e.g., instrument-rated pilots using air traffic control services and Congresspersons), to a wide sweep of "public interveners" (e.g., state, local governments, land-

26. Diane Vaughan's work (cited above) and conference paper contrasting the *Challenger* and *Columbia* accident reports gives eloquent testament to the dynamics of intense external scrutiny.

27. T. Rees, *Hostages to Each Other* (Chicago: University of Chicago Press, 1994).

use advocates, and citizen interest groups). Finally, this important function is also played by professional peer bodies and by HRO alumni who are seen as operationally knowledgeable observers. They are likely to be accorded respect both by other outsiders and by the HRO operators themselves.

An abundance of external watchers seems crucial in attaining continuous, highly reliable operations and a culture of reliability. So are boundary-spanning processes through which encouragement and constraints are exercised in the interest of product/safety reliability. Two types are evident. First, there are formally designated positions and/or groups who have external oversight responsibilities. Two examples of formalized channels are Nuclear Regulatory Commission On-site Residents, two or three of whom are assigned to each nuclear power plant, with nearly complete access to power plant information, review meetings, etc., and, second, military liaison officers who are permanently assigned to air traffic control centers. Sometimes these boundary-spanning activities are expressed in aircraft carriers' operations via dual reporting requirements for nuclear engineering officers to report problems immediately, not only to the ship's captain, but to a central nuclear affairs office at naval headquarters in Washington, DC, as well.

Boundary spanning, and with it increased transparency, also occurs intermittently in the form of periodic formal visits from "check" or review groups, who often exercise powerful sanctions if their reviews do not measure up. These activities come in a number of forms, for example, phased inspections and training checks in aircraft carrier combat preparations, as well as the more familiar Inspector General reviews, and nuclear power utilities requirements to satisfy rigorous performance in responding to the NRC-mandated, biannual activation of power plant emergency scenarios in which all the relevant local and state decision-makers engage in a daylong simulation leading to possible regional evacuation under the watchful eye of NRC and FEMA inspectors.[28]

Finally, external watchers, however well provided with avenues of access, must have available full, credible, and current information about system performance. This almost goes without saying, for these data, often in the form of annual evaluations, hazard indices, statistical summaries noted above, and indicators of incipient harm and the early onset of danger, become a crucial basis for insightful reviews and public credibility.

This is a formidable array of conditions for any organization to seek or to sustain, even for the short term. To what degree would they suffice over the long term? This will become a major challenge for NASA as missions take on multiyear scope and programs are premised on a long-term human presence in space.

28. La Porte and Thomas, "Regulatory Compliance and the Ethos of Quality Enhancement."

ASSURING INSTITUTIONAL CONSTANCY AND FAITHFULNESS IN THE FUTURE

Many highly reliable organizations operate systems whose full range of positive and negative outcomes can be perceived more or less immediately.[29] When this happens, organizational leaders can be rewarded or held accountable. But when operating systems are also capable of large-scale and/or widely distributed harm which may not occur or be detected for several operational generations, our familiar processes of accountability falter and overseers and the public are likely to be concerned that such HROs be worthy of the trust placed in them across several generations. In NASA's case, these challenges stem from the extraordinary reach of the administration's vision for the Agency's future.

NASA is contemplating missions that will send humans in space for several years to facilities that are likely to be designed to last 10 to 20 years (two management generations). Add to this any of half a dozen hoped-for lunar and exploratory missions. In a much more extreme case, the management of nuclear materials, obligations can be expected to continue for at least 50 to 100 years, perhaps centuries.[30] These cases suggest that shouldering an obligation to demonstrate the faithful adherence to a mission and its operational imperatives for a remarkably long time is inherent in accepting the program—even in the face of a variety of social and institutional environmental changes. As the longer term effects of such technologies become more clear, trying to take into account their transgenerational nature presents particularly troublesome challenges for managers and for students of organization.[31] And it is this aspect of highly reliable operations about which the social and management sciences have the least to say.

---

29. This section draws from portions of T. R. La Porte and A. Keller, "Assuring Institutional Constancy: Requisite for Managing Long-Lived Hazards," *Public Administration Review* 56, no. 6 (November/December 1996): 535–544. It is also informed by my work at Los Alamos National Laboratory (LANL) exploring the organizational challenges posed for the laboratory by its missions of science-based stockpile stewardship (of nuclear weapons), nuclear materials stewardship, and sometimes environmental stewardship. While the operations of the first two, contrasted to the latter, are very different, the challenges provoked by the longevity of the materials involved prompt very similar organizational puzzles. For a similar rendering, see T. R. La Porte, "Fiabilite et legitimaite soutenable" (Reliability and Sustainable Legitimacy), chap. 3 in *Organiser la fiabilite*, ed. M. Bourrier (Paris: L'Harmattan, 2001).

30. Readers can add other technically oriented programs or activities that have a similar extraordinary property, say in the environmental or public works domain.

31. Two conditions, noted here, increase the public demands for constancy because they undermine our typical means of ensuring accountability and are sometimes characteristic of hazardous technical systems. These two are 1) when the information needed to provide unequivocal evidence of effects is so extensive and costly that the public comes to expect that it will not be forthcoming and 2) if harmful effects occur, they are unlikely to be unequivocally detected for some time into the future due to the intrinsic properties of the production processes and their operating

continued on the next page

A partial remedy is to consider what we might call "institutional constancy." More formally, institutional constancy refers to "faithful, unchanging commitment to, and repeated attainment of performance, effects, or outcomes in accord with agreements by agents of an institution made at one time as expressed or experienced in a future time."[32] An organization exhibits constancy when, year after year, it achieves outcomes it agreed in the past to pursue in the spirit of the original public policy bargain.[33]

Conditions Encouraging Institutional Constancy[34]

What little systematic examination of this remarkable intention there is suggests that institutional constancy requires demonstrating to the public or its major opinion leaders that the agency, public contractors, or firms in question (for example, NASA operating very reliably) can both be trusted to keep its word—to be steadfast—for long into the future and to show the capacity to enact programs that are faithful to the original spirit of its commitments.[35] What conditions signal continued political and institutional will, steadfastness in "keeping the faith"? What conditions assure the capacity to follow through for many years, i.e., the organizational infrastructure of institutional constancy?

Institutional purpose. Constancy is about future behavior, and the organization must signal its collective resolve to persist in its agreements, especially

---

continued from the previous page

environments. While the mind's eye turns quickly to public organizations for examples, the argument applies with nearly equal force to the private sector in the United States, especially to those firms responding to the strong economic incentives for short-term gain with the systematic deferral of costs for some time.

32. T. R. La Porte and A. Keller, "Assuring Institutional Constancy."

33. Think, for example, of the FAA's air traffic control operations, together with air carriers. They have consistently achieved high levels of flight safety and traffic coordination in commercial aviation and flight operations at sea. And the Navy has a long-term record of exceptional safety aboard nuclear submarines. Electrical utilities have made remarkably high levels of electrical power available. Great universities exhibit constancy in commitments to intellectual excellence, generation after generation, through producing very skilled undergraduates and professionals as well as pathbreaking research.

34. Note: There are strong analytical and practical limitations to attaining institutional constancy over many generations, especially a) weak analytical bases for confidently predicting the outcomes of institutional activities over long periods of time, b) limited means to reinforce or reward generations of consistent behavior, and c) scanty knowledge about designing institutional relationships that improve rather than degrade the quality of action-taking in the future that is faithful to the spirit of present commitments and agreements. Incentives to improve conditions that would assure constancy of institutional capacities are scant. And so is interest in analysis that would improve our understanding of institutional and administrative design. Indeed, there is almost nothing insightful in the literature about *increasing* institutional inertia or constancy. It is still an analytical puzzle.

35. While these two qualities are closely related, one can imagine succeeding at one without achieving the other. An HRO might be able to persuade the public that it was firmly committed to certain objectives but actually turn out to be in no position to realize them. Conversely, an HRO could very well be situated, motivated, and structured to carry out its commitments for years to come but be unable to convince the public of its steadfastness.

with strong commitments to trusteeship in the interests of future generations. Measures that reinforce this perception are as follows:

- The necessary formal, usually written goal of unswerving adherence to the spirit of the initial agreement or commitment; documents that can be used in the future to hold each generation's organizational leaders accountable for their actions.

- Strong, public articulation of commitments to constancy by high-status figures within an agency or firm, calling especially on professional staff and perhaps key labor representatives to emphasize the importance of constancy. Coupled with formal declarations, consistent emphasis upon steadfastness within an organization reinforces the otherwise difficult commitments of energy and public witness that are needed by key members of the technical staff and workforce.

- Strong evidence of institutional norms and processes that nurture the resolve to persist across many work generations, including, in the public sector, elements in labor contracts that extend over several political generations.[36] When these exist, they bind workers and their leaders to the goals of the agency, often transcending episodes of leadership succession. The content of these norms and the processes that reinforce them are now not well calibrated, though examples are likely to be found in public activities that draw the deep loyalty of technical staff and former members. This seems to be the case for elite military units, e.g., the U.S. Marine Corps and Navy Seals; groups within the Centers for Disease Control (CDC) and some other public health activities; and some elements within U.S. air traffic control circles. A close examination of the internal processes of socialization the produce such loyalty is warranted.[37]

- Commitments to courses of action, particularly those where benefits may be delayed until a succeeding management or political genera-

36. This point is akin to the arguments made classically by P. Selznick, *Leadership in Administration* (New York: Harper & Row, 1957), and J. Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (New York: Basic Books, 1989), pp. 99–102, about the importance of institutional leadership and the character of the organization's sense of mission.

37. For an early exploration of this aspect, see Selznick, *Leadership in Administration*, and his discussion of the transformation of an instrumental organization into one that has been "infused with value," i.e., that becomes an "institution." For a recent project attempting to address these questions, see A. Boin, "The Early Years of Public Institutions: A Research Agenda" (paper issued by the Department of Public Administration, Leiden University, Netherlands, 2004).

tion, are difficult to sustain in the face of U.S. political metabolism. Therefore, vigorous external reinforcement from both regulatory agencies and "public watching" groups must be present to assure that the relevant agencies and their contractors will not flag in attending to the performance promised by one generation to the next. This would include reinforcing the vigor of outside groups by regularly assuring their formal involvement and providing sufficient resources to sustain their expectations and prompt their demands for consultation if the next generation of leaders wavers in its resolve. The optimum would be when these measures lead to laws, formal agreements, and foundation/nongovernmental funding and infrastructure for continual encouragement and sanctions for "keeping the faith."

The infrastructure of constancy. While strong motivations and earnestness are necessary, they alone do not carry the day. Other conditions should also be present to assure interested outsiders that actions will, in fact, be carried out in realizing important commitments across multiple generations. As I outline

Table 13.2. Characteristics Associated with Institutional Constancy (i.e., Organizational Perseverance, Faithful Adherence to the Mission and Its Operational Imperatives)

1. Assurance of steadfast political will.
   - A. Formal goal of unswerving adherence to the spirit of the initial agreement.
   - B. Strong articulation of commitments by high-status agency leaders calling on staff in achieving constancy.
   - C. Clear evidence of institutional norms that nurture the persistence of commitments across many generations.
   - D. Vigorous external reinforcement from regulatory agencies and public watching groups.
2. Organizational infrastructure of constancy.
   - A. Administrative and technical capacity to carry out constancy-assurance activities reinforced by agency rewards.
   - B. Adequate resources to assure the "transfer" of requisite technical and institutional knowledge across worker and management generations.
   - C. Analytical and resource support for "future impact analyses."
   - D. Capacity to detect and remedy the early onset of likely failure that threatens the future, with the assurance of remediation if failures occur.

these, return in your mind's eye to the U.S. space community and the many organizations revolving satellite-like around the central sun/star of NASA. How many of the conditions I will suggest below already exist within NASA? How difficult would their introduction and persistence likely be? If these seem sparse, or absent, this points to a "critical institutional issue."

These conditions of constancy include the following:

- The technical capabilities and administrative infrastructure which are needed to assure performance, along with agency or contractor rewards and incentives for articulating and pursuing measures that enhance constancy and intergenerational fairness. These would include executive socialization and training processes to reinforce commitments and long-term perspectives to nurture a culture of constancy. Such processes and resources are rarely provided in today's institutional environments. Rather, perspectives and rewards are intensely generation-centric, characterized by quite short-term evaluations, and strongly reinforced by contemporary business and legislative cycles.

- In addition to assuring consistency in organizational culture, the resources and activities needed to "transfer" or "pass on" the organization's critical operating, technical, and institutional knowledge from one work and management generation to the next are crucial. This includes systematic capture of critical skills and operating histories, as well as continuous training and evaluation of each generation's capabilities. Some portion of each future generation should be present in the current one.

The remaining conditions point to keen powers of analysis in service to the future.

- Analytical supports should be evident for analysis and decision-making which take into account the interests of the future and enable work, such as "future impact analyses," that seeks to identify the effects of present institutional actions on future capabilities. Something like this goes on during budgetary planning efforts, but, in the U.S. system, the timeframes are invariably merely short-term, tied to legislative or corporate profit reporting cycles. Scanning further into an institution's future—at least beyond the present generation—is also called for. Analytical capabilities to do this are likely to require at least a small cadre of highly skilled professionals, systems for rewarding their efforts, and organizational and agency venues where their reflections will have a respected voice.

- And, perhaps most important, publicly obvious, effective capacity would be in place to detect the early onset of likely failures related to the activities that could threaten the future. This analytical capacity should then be joined with institutional capabilities to initiate remedies, along with the assurance of remediation resources in the event failures should occur.[38] Without quite visible, publicly evident, and well-exercised capacity for early warning and *preemptive* remediation, the public is likely to remain skeptical, potentially suspicious, and ripe for mobilization into recalcitrant opposition.[39]

This suite of conditions intended to assure institutional constancy is very demanding and costly. Whether leaders would consider developing them is likely to be contingent upon external demand. Pressure to try is increased when programs exhibit three characteristics. There will be particularly aggressive insistence on faithfulness when agency programs a) are perceived to be large-scale efforts whose activities may occur across broad spatial and temporal spans and seem to pose potentially irreversible effects; b) are seen as intensely hazardous, even if the likelihood of failure is small and accompanied by substantial gains for the program's prime beneficiaries; and c) pose significant risks whose costs are likely to be borne by future generations who receive little benefit.

This third characteristic—temporal asymmetry of benefits and costs—raises a particularly difficult dilemma. Put in question form: should current populations endure costs today so that future populations will not have to?[40] In NASA's case, this would include investing to avoid future risks against the accrual of present benefits, say, in symbolic returns, or perhaps knowledge that is potentially useful in providing novel artifacts. These long-term benefits

38. See, for example, T. R. La Porte and C. Thomas, "Regulatory Compliance and the Ethos of Quality Enhancement: Surprises in Nuclear Power Plant Operations," *Journal of Public Administration Research and Theory* 5, no. 4 (December 1994): 250–295. Cf. K. Shrader-Frechette, "Risk Methodology and Institution Bias," *Research in Social Problems and Public Policy* 5 (1993): 207–223; and L. Clarke, "The Disqualification Heuristic: When Do Organizations Misperceive Risk?" *Research in Social Problems and Public Policy* 5 (1993): 289–312, for discussions of the conditions that result in operator misperception of risk, conditions that would require strong antidotes if constancy is to be assured.

39. This seems clearly to be the case for the many years of political and legal travail experienced by the Department of Energy. See DOE, "Earning Public Trust and Confidence."

40. See, for example, R. M. Green, "Inter-generational Distributive Justice and Environmental Responsibility," in *Responsibilities to Future Generations: Environmental Ethics*, ed. E. D. Partridge (Buffalo: Prometheus Books, 1980); R. Howarth, "Inter-generational Competitive Equilibria Under Technological Uncertainty and an Exhaustible Resource Constraint," *Journal of Environmental Economics and Management* 21 (1991): 225–243; B. Norton, "Environmental Ethics and the Rights of Future Generations," *Environmental Ethics* (winter 1982): 319–338; P. Wenz, "Ethics, Energy Policy, and Future Generations," *Environmental Ethics* 5 (1983): 195–209.

would have to be balanced against present costs and, as importantly, future industrial environmental damage from large-scale facilities, or having to abandon teams of astronauts due to the inability to retrieve them, and, more remotely, infecting terrestrial populations with extraterrestrial organisms.

Uncertainty about the knowledge and technological capacity of future generations exacerbates the problem. An optimistic view assumes that difficult problems of today will be more easily solved by future generations.[41] No problem today is too big for the future. Skepticism about this, however, makes it an equivocal basis for proceeding with multigenerational programs. An inherent part of assuring constancy would be an agreed-upon basis, an "ethic," of how costs and benefits should be distributed across generations. This is especially true when operational effects extend well into the future, for it demands that generation after generation respond to new information and changing value structures in coping with long-term effects.

This array of constancy-enhancing characteristics raises serious, unresolved operational, political, and ethical questions. If an organization's program provokes demands for nearly error-free operations, then assurances of institutional constancy in meeting the conditions for reliability are likely to be demanded as a substitute for accountability.[42] Apprehensive publics seek assurances that these institutions, such as NASA, will be uncompromising in their pursuit of highest quality operations through the relevant lifetimes of the systems in question.

When harmful effects may be visited upon future generations, assurances of continuity or institutional constancy take on increasing importance.[43] Why would this be the case? Those who implement such programs could quite probably escape accountability for failures. They would have retired,

---

41. For comment on how responsibility should be divided between generations that accounts for changes in knowledge, see W. Halfele, "Energy from Nuclear Power," *Scientific American* 263, no. 3 (September 1990): 136–144; C. Perrings, "Reserved Rationality and the Precautionary Principle: Technological Change, Time and Uncertainty in Environmental Decision Making," in *Ecological Economics: The Science and Management of Sustainability*, ed. R. Costanza (New York: Columbia University Press, 1991).

42. For those HROs whose technical operations and consequences of failure can be seen as having constancy-evoking characteristics, ignoring "constancy magnets" is an institutionally risky business. This is especially the case for the combination of uneven distribution of benefits and costs among generations and the potential for a long lag in discovering information about possibly grievous damages. Setting these matters aside allows festering seeds of suspicion to multiply, and, if coupled with conditions that also evoke "reliability and regulatory magnets," they are likely grounds for political opposition and demands for increasing rigorous regulation as a condition for even initial approval for new projects. But if organizational remedies are called for, how much additional effort and evolution of institutional capabilities could be entailed?

43. While the mind's eye turns quickly to public organizations, the argument applies equally to the private sector in the United States, especially those firms responding to the strong economic incentives for short-term gain and deferral of costs.

died, or moved on. Leaders of such institutions, therefore, are quite likely to be pressed to assure the public (especially able opinion leaders) that, as a condition of winning approval and resources to initiate or continue programs, agencies and corporate contractors involved should credibly be expected to keep agreements and commitments with potentially affected communities far into the future.

CONCLUDING REFLECTIONS

The reach of NASA's space programs continues to levy remarkable operational demands, for the programs imply very long-term management of both the unmanned and manned aspects of space exploration and possibly commercial and security exploitation. This rather cryptic application to NASA's space exploration programs of work done in other technical domains hints at the challenges involved when we insist on extraordinary levels of reliability that should go on for a number of management generations. It suggests an array of conditions that would become increasingly salient as NASA seeks to regularize and sustain its space traffic regime.

These are very demanding conditions for organizational leaders to consider, much less actively insist upon, encourage, and nurture, even if we knew how to establish organizational patterns I have summarized.[44] It is notable that my discussion is based on work dealing with operations that, *unlike NASA spaceflights*, were quite mature, pretty routine, and had managed to continue for some time. Although the HRO field work involved nearly 10 years of observing and intensive subjective onsite experience with each of three large technical systems in the study, it was not so intensive as discovering the process through which these organizations had gone to result in the variegated patterns that were described. We do not know exactly how they got there.

If the constructs I have outlined here are taken seriously, it is likely to pose unwelcome challenges to agency and program leaders. Our workshop discussions called out a range of critical institutional (as well as historiographical) issues and point toward matters of serious design examination. But the analytical bases for designing and assuring institutional forms at substantial

44. They are also conditions that are not likely to flourish without a high degree of public trust and confidence in operating and overseeing institutions—something that is in increasingly short supply in contemporary American culture. NASA has skated across the increasingly thin ice of waning public confidence in programs involving humans in space. The several high-profile congressional investigations and the Agency's agony over the past decade have eroded a general sense of public confidence in future operations. This in itself should be seen as a major critical institutional issue. For an earlier consideration of this, see T. La Porte, "Institutional Challenges for Continued Space Exploration: High-reliability systems across many operational generations. Are these aspirations publicly credible?" (presented at the Workshop on Space Policy, National Academies of Science, Irvine, CA, 12–13 November 2003).

scale are limited at best.[45] For example, there is scant work on effecting institutional constancy per se, and only limited study of the evolution of highly reliable organizations. A remedy to these important gaps in understanding requires both analytical and experimental efforts to calibrate the dynamics of highly reliable operations, and especially probing the requisites for long-term institutional constancy and trustworthiness.

At least three additional aspects of this challenge are apparent; each prompts a demanding set of research imperatives (see table 13.3).

First, we need to improve our knowledge about the wider institutional currents within U.S. patterns of public and corporate governance that provoke repeated, stubborn resistance to the organizational changes needed to sustain very reliable operations, and reassure citizens that the responsible institutions will be able to keep their word through the relevant program timeframes—and do so in ways that enhance their trustworthiness. Even if there is a reasonably benign political and social environment, these are qualities that are very difficult to establish and maintain. In answering "Why can't we do

Table 13.3. Research Directions: When Highly Reliable Operations, Long-Term Institutional Constancy, and Trustworthiness Are Indicated

Q: Why can't we do it?

A: Institutional impediments to conditions sustaining very reliable operations, institutional constancy, and trustworthiness.

Q: Why do we have to?

A: Technical imperatives requiring very reliable operations over multiple political generations. (Seek technical design alternatives having equivalent physical and organic effects without HRO or institutional constancy imperatives.)

Q: Why do we need to?

A: Alternatively, there are institutional activities that reduce the public's

1. risk-averse demand for very reliable operations of intrinsically hazardous systems,
2. worry about the longer term consequences of operational errors, and
3. sense of vulnerability that fosters a demand for trustworthy public institutions.

45. Some of these are highlighted in the chapters by Diane Vaughan and Philip Scranton.

it?" historical insight surely can be brought to bear. NASA is a particularly visible case, certainly not the only instance in which a public agency seems unable to alter its internal dynamics so that it avoids repeating what outsiders perceive (invariably after a serious mishap) to be dysfunctional organizational patterns. Observers of the Department of Energy's Radioactive Waste Programs are also likely to regard these efforts as deeply flawed. In these and other cases, such evaluations arise during nearly each generation of new management. For NASA, it is observed that dysfunctions have afflicted each of the last seven Administrators with repeated problems in the evolution of NASA's institutional culture. The conference papers contributed by Scranton and Vaughan give witness to many of these debilitating dynamics. Some of this is internally self-inflicted, to be sure. But for my part, I suspect more important sources lurk in NASA's relations with Congress and the Agency's extensive contractual community. In the early pages of the *Columbia* report, these sources of dysfunction were noted. They then escaped detailed examination thereafter. In the future, these should be the objects of as much analysis as NASA's internal dynamics. The historical community seems particularly positioned to furnish keen insight into what—in repeated instances—seems likely to be the result of a much deeper structural relationship than merely a series of very able people somehow succumbing to individual weakness and local bureaucratic perversity.

Second, we need to deepen our understanding of the technical sources that drive systems operators toward "having to" attain very high reliability. Technologies vary in the degree they require closely harmonized operator behavior. They also vary in their intrinsic hazardousness. Both of these characteristics can be shaped by the engineering design teams who provide the technical heart of operating systems. What is it about technical communities that prompts their members to propose technologies that require extraordinary behavior as a *condition* of delivering the hoped-for benefits? Is this intrinsic to some technical domains and not others? This suggests studies that calibrate the degree to which present technical and operational directions in the development of, at least, environmentally sensitive operations, materials management, and transportation and biological technologies a) require highly reliable operating organizations, b) imply long-term operating trajectories and potentially negative effects, and hence c) produce a requirement for high levels of public trust and confidence. In-depth sociological and historical studies could, one imagines, shed light on these matters.

A better understanding of these relationships can be crucial in democratic societies. It can be argued that the more the requirements for HRO, institutional constancy, and public trust and confidence are present, the more demanding the institutional challenges will be in sustaining public legitimacy. A closely related emphasis follows: what changed within technical design com-

munities would be necessary for them aggressively to seek technical design alternatives that provide equivalent physical and organic effects varying the degree to which they produce demands for high-reliability operations over many work generations.

But wait, wait! Is there an alternative to the two research and development vectors just noted? They are very demanding R&D domains. Actually realizing the organizational imperatives that lurk within such designs is even more difficult to assure within private or public enterprises in the U.S. and abroad. Indeed, even entertaining the desirability of such changes is disputed by institutional leaders and provokes strong managerial reluctance to consider them seriously. So why are we trying? "Why do we need to?"

The need to try (or act as if we were trying) stems, importantly, from the public's expressed worry about their own exposure to what they perceive to be "risky systems." They worry and appear to have a very low tolerance for risk-taking. It could be argued, we need to try because "they" demand it. However, an alternative program of research and activities could be launched.

What activities could be carried out which would *reduce* the public's risk-averse demand for very reliable operations of intrinsically hazardous systems, *reduce* the public's worry about the longer term consequences of operational errors, and *lessen* the public's sense of vulnerability that nourishes a deep longing for trustworthy public institutions? As far as I know, there is very little systematic work exploring the grounds upon which alert publics would come to understand the rationality of accepting the likelihood of increased exposure to malfunctions of hazardous technical systems in the interest of smoothing production flows or stabilizing revenue streams for major investors. Nor do I know of any efforts to understand the basis for convincing the public explicitly that it would be acceptable to engage in developments that promise attractive short-term benefits which would export severe costs across several future generations to their grandchildren's children. Worries about the potential for immediate exposure to personal injury or environmentally derived insult, and a more diffuse concern that important dangers may await our children some years from now, continue to spawn irritating (probably irrational) objections to developing and deploying exciting new technical possibilities. Well, perhaps they could produce untoward surprises, but they are (probably) manageable. We can count on clever technical solutions.

"Why can't they trust us?" Indeed, this deserves analytical attention as well. Why do alert publics feel so vulnerable that they increasingly wish for trustworthy institutions? What developments could be devised that publics would relax their demand for trustworthiness and accept technical leaders and provide support for the technical future we designers see? In effect, "Why," as Henry Higgins and one technical designer put it, "why can't they be more like us?"