Columbia Accident Case Study

This is an edited version of the Columbia Accident Investigation Board report released in August, 2003. It provides a comprehensive and often sobering example of management lapses that have severe consequences.

The original report was over 280 pages. This edited version eliminates the much of the technical discussion and focuses instead on the organizational factors that lead to the accident. You may obtain the entire report from [http://www.caib.us/news/report/default.html](http://www.caib.us/news/report/default.html)

I have included some sections for background. Read these sections to gain an overview of the accident and the report. I have included some pages simply to provide context for sections that relate to questions below.

I have placed arrows in the text to indicate those sections that are most important.

Questions to Consider:

1. According to the report, what were the causes of the Columbia accident?
2. What were the essential features of the culture at NASA?
3. Which factors played the greatest role in the events leading up to the accident: logical factors, such as schedule, technicalities of the shuttle design, testing, or psychological, such as politics, the perspective of deadlines?
4. What was the meaning of February 19, 2004?
5. How did February 19, 2004 contribute to the Columbia accident?
6. How did management and workforce differ in their perspective on the pressure to meet 2/19/04? Why did they differ?
7. What types of schedule management tools did NASA use? Were they effective?
8. What were the de facto priorities of the shuttle program leading up to the accident?
9. How did these priorities shape management’s perspective on “facts” presented by engineering after the launch of ST-107?
10. Which perspective on communication best explains the findings in the report: communication as information flow or communication as influence?
11. Which was most important in explaining the cultural factors leading up to the accident: a lack of management or a lack of leadership? Why?
12. What role did the management’s perception of NASA’s history play in the events leading up to the accident?
13. What role did a willingness to learn from mistakes play in the events leading up to the accident?
14. Given the example of the Navy’s reactor safety program, how could NASA correct these organizational deficiencies?
15. Could NASA managers have done a better job if they had followed Descartes’ four rules for thinking? Why?
16. What role did PowerPoint play in management’s failures?
17. How do the report’s conclusions about leadership, culture, change, structure and risk apply to the management of everyday projects?
On the Front Cover

This was the crew patch for STS-107. The central element of the patch was the microgravity symbol, µg, flowing into the rays of the Astronaut symbol. The orbital inclination was portrayed by the 39-degree angle of the Earth’s horizon to the Astronaut symbol. The sunrise was representative of the numerous science experiments that were the dawn of a new era for continued microgravity research on the International Space Station and beyond. The breadth of science conducted on this mission had widespread benefits to life on Earth and the continued exploration of space, illustrated by the Earth and stars. The constellation Columba (the dove) was chosen to symbolize peace on Earth and the Space Shuttle Columbia. In addition, the seven stars represent the STS-107 crew members, as well as honoring the original Mercury 7 astronauts who paved the way to make research in space possible. The Israeli flag represented the first person from that country to fly on the Space Shuttle.

On the Back Cover

This emblem memorializes the three U.S. human space flight accidents – Apollo 1, Challenger, and Columbia. The words across the top translate to: “To The Stars, Despite Adversity – Always Explore”
The Columbia Accident Investigation Board’s independent investigation into the February 1, 2003, loss of the Space Shuttle Columbia and its seven-member crew lasted nearly seven months. A staff of more than 120, along with some 400 NASA engineers, supported the Board’s 13 members. Investigators examined more than 30,000 documents, conducted more than 200 formal interviews, heard testimony from dozens of expert witnesses, and reviewed more than 3,000 inputs from the general public. In addition, more than 25,000 searches combed vast stretches of the Western United States to retrieve the spacecraft’s debris. In the process, Columbia’s tragedy was compounded when two debris searchers with the U.S. Forest Service perished in a helicopter accident.

The Board recognized early on that the accident was probably not an anomalous, random event, but rather likely rooted to some degree in NASA’s history and the human space flight program’s culture. Accordingly, the Board broadened its mandate at the outset to include an investigation of a wide range of historical and organizational issues, including political and budgetary considerations, compromises, and changing priorities over the life of the Space Shuttle Program. The Board’s conviction regarding the importance of these factors strengthened as the investigation progressed, with the result that this report, in its findings, conclusions, and recommendations, places as much weight on these causal factors as on the more easily understood and corrected physical cause of the accident.

The physical cause of the loss of Columbia and its crew was a breach in the Thermal Protection System on the leading edge of the left wing, caused by a piece of insulating foam which separated from the left bipod ramp section of the External Tank at 81.7 seconds after launch, and struck the wing in the vicinity of the lower half of Reinforced Carbon-Carbon panel number 8. During re-entry this breach in the Thermal Protection System allowed superheated air to penetrate through the leading edge insulation and progressively melt the aluminum structure of the left wing, resulting in a weakening of the structure until increasing aerodynamic forces caused loss of control, failure of the wing, and breakup of the Orbiter. This breakup occurred in a flight regime in which, given the current design of the Orbiter, there was no possibility for the crew to survive.

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, 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.

This report concludes with recommendations, some of which are specifically identified and prefaced as “before return to flight.” These recommendations are largely related to the physical cause of the accident, and include preventing the loss of foam, improved imaging of the Space Shuttle stack from liftoff through separation of the External Tank, and on-orbit inspection and repair of the Thermal Protection System. The remaining recommendations, for the most part, stem from the Board’s findings on organizational cause factors. While they are not “before return to flight” recommendations, they can be viewed as “continuing to fly” recommendations, as they capture the Board’s thinking on what changes are necessary to operate the Shuttle and future spacecraft safely in the mid- to long-term.

These recommendations reflect both the Board’s strong support for return to flight at the earliest date consistent with the overriding objective of safety, and the Board’s conviction that operation of the Space Shuttle, and all human space-flight, is a developmental activity with high inherent risks.
The Board is convinced that the factors that led to the Columbia accident go well beyond the physical mechanisms discussed in Chapter 3. The causal roots of the accident can also be traced, in part, to the turbulent post-Cold War policy environment in which NASA functioned during most of the years between the destruction of Challenger and the loss of Columbia. The end of the Cold War in the late 1980s meant that the most important political underpinning of NASA’s Human Space Flight Program – U.S.-Soviet space competition – was lost, with no equally strong political objective to replace it. No longer able to justify its projects with the kind of urgency that the superpower struggle had provided, the agency could not obtain budget increases through the 1990s. Rather than adjust its ambitions to this new state of affairs, NASA continued to push an ambitious agenda of space science and exploration, including a costly Space Station Program.

If NASA wanted to carry out that agenda, its only recourse, given its budget allocation, was to become more efficient, accomplishing more at less cost. The search for cost reductions led top NASA leaders over the past decade to downsize the Shuttle workforce, outsource various Shuttle Program responsibilities – including safety oversight – and consider eventual privatization of the Space Shuttle Program. The program’s budget was reduced by 40 percent in purchasing power over the past decade and repeatedly raided to make up for Space Station cost overruns, even as the Program maintained a launch schedule in which the Shuttle, a developmental vehicle, was used in an operational mode. In addition, the uncertainty of top policymakers in the White House, Congress, and NASA as to how long the Shuttle would fly before being replaced resulted in the delay of upgrades needed to make the Shuttle safer and to extend its service life.

The Space Shuttle Program has been transformed since the late 1980s implementation of post-Challenger management changes in ways that raise questions, addressed here and in later chapters of Part Two, about NASA’s ability to safely operate the Space Shuttle. While it would be inaccurate to say that NASA managed the Space Shuttle Program at the time of the Columbia accident in the same manner it did prior to Challenger, there are unfortunate similarities between the agency’s performance and safety practices in both periods.

## 5.1 The Challenger Accident and Its Aftermath

The inherently vulnerable design of the Space Shuttle, described in Chapter 1, was a product of policy and technological compromises made at the time of its approval in 1972. That approval process also produced unreasonable expectations, even myths, about the Shuttle’s future performance that NASA tried futilely to fulfill as the Shuttle became “operational” in 1982. At first, NASA was able to maintain the image of the Shuttle as an operational vehicle. During its early years of operation, the Shuttle launched satellites, performed on-orbit research, and even took members of Congress into orbit. At the beginning of 1986, the goal of “routine access to space” established by President Ronald Reagan in 1982 was ostensibly being achieved. That appearance soon proved illusory. On the cold morning of January 28, 1986, the Shuttle Challenger broke apart 73 seconds into its climb towards orbit. On board were Francis R. Scobee, Michael J. Smith, Ellison S. Onizuka, Judith A. Resnick, Ronald E. McNair, Sharon Christa McAuliffe, and Gregory B. Jarvis. All perished.

### Rogers Commission

On February 3, 1986, President Reagan created the Presidential Commission on the Space Shuttle Challenger Accident, which soon became known as the Rogers Commission after its chairman, former Secretary of State William Rogers. The Commission’s report, issued on June 6, 1986, concluded that the loss of Challenger was caused by a failure of the joint and seal between the two lower segments of the right Solid Rocket Booster. Hot gases blew past a rubber O-ring in the joint, leading to a structural failure and the explosive burn-
The Rogers Commission concluded “the decision to launch the Challenger was flawed.” Communication failures, incomplete and misleading information, and poor management judgments all figured in a decision-making process that permitted, in the words of the Commission, “internal flight safety problems to bypass key Shuttle managers.” As a result, if those making the launch decision “had known all the facts, it is highly unlikely that they would have decided to launch.” Far from meticulously guarding against potential problems, the Commission found that NASA had required “a contractor to prove that it was not safe to launch, rather than proving it was safe.”

The Commission also found that NASA had missed warning signs of the impending accident. When the joint began behaving in unexpected ways, neither NASA nor the Solid Rocket Motor manufacturer Morton-Thiokol adequately tested the joint to determine the source of the deviations from specifications or developed a solution to them, even though the problems frequently recurred. Nor did they respond to internal warnings about the faulty seal. Instead, Morton-Thiokol and NASA management came to see the problems as an acceptable flight risk – a violation of a design requirement that could be tolerated.

During this period of increasing uncertainty about the joint’s performance, the Commission found that NASA’s safety system had been “silent.” Of the management, organizational, and communication failures that contributed to the accident, four related to faults within the safety system, including “a lack of problem reporting requirements, inadequate trend analysis, misrepresentation of criticality, and lack of involvement in critical discussions.”

Still another factor influenced the decisions that led to the accident. The Rogers Commission noted that the Shuttle’s increasing flight rate in the mid-1980s created schedule pressure, including the compression of training schedules, a shortage of spare parts, and the focusing of resources on near-term problems. NASA managers “may have forgotten—partly because of past success, partly because of their own well-nurtured image of the program—that the Shuttle was still in a research and development phase.”

The Challenger accident had profound effects on the U.S. space program. On August 15, 1986, President Reagan announced that “NASA will no longer be in the business of launching private satellites.” The accident ended Air Force and intelligence community reliance on the Shuttle to launch national security payloads, prompted the decision to abandon the yet-to-be-opened Shuttle launch site at Vandenberg Air Force Base, and forced the development of improved expendable launch vehicles. A 1992 White House advisory committee concluded that the recovery from the Challenger disaster cost the country $12 billion, which included the cost of building the replacement Orbiter Endeavour.

It took NASA 32 months after the Challenger accident to redesign and requalify the Solid Rocket Booster and to return the Shuttle to flight. The first post-accident flight was launched on September 29, 1988. As the Shuttle returned to flight, NASA Associate Administrator for Space Flight
Richard Truly commented, “We will always have to treat it [the Shuttle] like an R&D test program, even many years into the future. I don’t think calling it operational fooled anybody within the program … It was a signal to the public that shouldn’t have been sent.”

The Shuttle Program After Return to Flight

After the Rogers Commission report was issued, NASA made many of the organizational changes the Commission recommended. The space agency moved management of the Space Shuttle Program from the Johnson Space Center to NASA Headquarters in Washington, D.C. The intent of this change was to create a management structure that better reflected that of the Apollo program, with the aim of preventing the kinds of inadequacies that contributed to the Challenger accident. NASA also established an Office of Safety, Reliability, and Quality Assurance at its Headquarters, though that office was not given the “direct authority” over all of NASA’s safety operations as the Rogers Commission had recommended. Rather, NASA human space flight centers each retained their own safety organization reporting to the Center Director.

In the almost 15 years between the return to flight and the loss of Columbia, the Shuttle was again being used on a regular basis to conduct space-based research, and, in line with NASA’s original 1969 vision, to build and service a space station. The Shuttle flew 87 missions during this period, compared to 24 before Challenger. Highlights from these missions include the 1990 launch, 1993 repair, and 1999 and 2002 servicing of the Hubble Space Telescope; the launch of several major planetary probes; a number of Shuttle-Spacelab missions devoted to scientific research; nine missions to rendezvous with the Russian space station Mir; the return of former Mercury astronaut Senator John Glenn to orbit in October 1998; and the launch of the first U.S. elements of the International Space Station.

After the Challenger accident, the Shuttle was no longer described as “operational” in the same sense as commercial aircraft. Nevertheless, NASA continued planning as if the Shuttle could be readied for launch at or near whatever date was set. Tying the Shuttle closely to International Space Station needs, such as crew rotation, added to the urgency of maintaining a predictable launch schedule. The Shuttle is currently the only means to launch the already-built European, Japanese, and remaining U.S. modules needed to complete Station assembly and to carry and return most experiments and on-orbit supplies. Even after three occasions when technical problems grounded the Shuttle fleet for a month or more, NASA continued to assume that the Shuttle could regularly and predictably service the Station. In recent years, this coupling between the Station and Shuttle has become the primary driver of the Shuttle launch schedule. Whenever a Shuttle launch is delayed, it impacts Station assembly and operations.

In September 2001, testimony on the Shuttle’s achievements during the preceding decade by NASA’s then-Deputy Associate Administrator for Space Flight William Readdy indicated the assumptions under which NASA was operating during that period:

The Space Shuttle has made dramatic improvements in the capabilities, operations and safety of the system. The payload-to-orbit performance of the Space Shuttle has been significantly improved – by over 70 percent to the Space Station. The safety of the Space Shuttle has also been dramatically improved by reducing risk by more than a factor of five. In addition, the operability of the system has been significantly improved, with five minute launch windows – which would not have been attempted a decade ago – now becoming routine. This record of success is a testament to the quality and dedication of the Space Shuttle management team and workforce, both civil servants and contractors.

5.2 The NASA Human Space Flight Culture

Though NASA underwent many management reforms in the wake of the Challenger accident and appointed new directors at the Johnson, Marshall, and Kennedy centers, the agency’s powerful human space flight culture remained intact, as did many institutional practices, even if in a modified form. As a close observer of NASA’s organizational culture has observed, “Cultural norms tend to be fairly resilient … The norms bounce back into shape after being stretched or bent. Beliefs held in common throughout the organization resist alteration.” This culture, as will become clear across the chapters of Part Two of this report, acted over time to resist externally imposed change. By the eve of the Columbia accident, institutional practices that were in effect at the time of the Challenger accident – such as inadequate concern over deviations from expected performance, a silent safety program, and schedule pressure – had returned to NASA.

Organizational Culture

Organizational culture refers to the basic values, norms, beliefs, and practices that characterize the functioning of a particular institution. At the most basic level, organizational culture defines the assumptions that employees make as they carry out their work; it defines “the way we do things here.” An organization’s culture is a powerful force that persists through reorganizations and the departure of key personnel.

The human space flight culture within NASA originated in the Cold War environment. The space agency itself was created in 1958 as a response to the Soviet launch of Sputnik, the first artificial Earth satellite. In 1961, President John F. Kennedy charged the new space agency with the task of reaching the moon before the end of the decade, and asked Congress and the American people to commit the immense resources for doing so, even though at the time NASA had only accumulated 15 minutes of human space flight experience. With its efforts linked to U.S.-Soviet competition for global leadership, there was a sense in the NASA workforce that the agency was engaged in a historic struggle central to the nation’s agenda.

The Apollo era created at NASA an exceptional “can-do” culture marked by tenacity in the face of seemingly impossible challenges. This culture valued the interaction among
About NASA possessing unique knowledge about how to safely launch people into space. As will be discussed later in this chapter, as well as in Chapters 6, 7, and 8, the Board views this cultural resistance as a fundamental impediment to NASA’s effective organizational performance.

5.3 An Agency Trying to Do Too Much With Too Little

A strong indicator of the priority the national political leadership assigns to a federally funded activity is its budget. By that criterion, NASA’s space activities have not been high on the list of national priorities over the past three decades (see Figure 5.3-1). After a peak during the Apollo program, when NASA’s budget was almost four percent of the federal budget, NASA’s budget since the early 1970s has hovered at one percent of federal spending or less.

![Figure 5.3-1. NASA budget as a percentage of the Federal budget. (Source: NASA History Office)](image)

Particularly in recent years, as the national leadership has confronted the challenging task of allocating scarce public resources across many competing demands, NASA has had difficulty obtaining a budget allocation adequate to its continuing ambitions. In 1990, the White House chartered a blue-ribbon committee chaired by aerospace executive Norman Augustine to conduct a sweeping review of NASA and its programs in response to Shuttle problems and the flawed mirror on the Hubble Space Telescope. The review found that NASA’s budget was inadequate for all the programs the agency was executing, saying that “NASA is currently over committed in terms of program obligations relative to resources available—in short, it is trying to do too much, and allowing too little margin for the unexpected.”

“A reinvigorated space program,” the Augustine committee went on to say, “will require real growth in the NASA budget of approximately 10 percent per year (through the year 2000) reaching a peak spending level of about $30 billion per year (in constant 1990 dollars) by about the year 2000.” Translated into the actual dollars of Fiscal Year 2000, that recommendation would have meant a NASA budget of over $40 billion; the actual NASA budget for that year was $13.6 billion.

During the past decade, neither the White House nor Congress has been interested in “a reinvigorated space program.” Instead, the goal has been a program that would continue to
produce valuable scientific and symbolic payoffs for the nation without a need for increased budgets. Recent budget allocations reflect this continuing policy reality. Between 1993 and 2002, the government’s discretionary spending grew in purchasing power by more than 25 percent, defense spending by 15 percent, and non-defense spending by 40 percent (see Figure 5.3-2). NASA’s budget, in comparison, showed little change, going from $14.31 billion in Fiscal Year 1993 to a low of $13.6 billion in Fiscal Year 2000, and increasing to $14.87 billion in Fiscal Year 2002. This represented a loss of 13 percent in purchasing power over the decade (see Figure 5.3-3).\(^{19}\)

The lack of top-level interest in the space program led a 2002 review of the U.S. aerospace sector to observe that “a sense of lethargy has affected the space industry and community. Instead of the excitement and exuberance that dominated our early ventures into space, we at times seem almost apologetic about our continued investments in the space program.”\(^{20}\)

### WHAT THE EXPERTS HAVE SAID

#### Warnings of a Shuttle Accident

“Shuttle reliability is uncertain, but has been estimated to range between 97 and 99 percent. If the Shuttle reliability is 98 percent, there would be a 50-50 chance of losing an Orbiter within 34 flights … The probability of maintaining at least three Orbiters in the Shuttle fleet declines to less than 50 percent after flight 113.”\(^{21}\)

-The Office of Technology Assessment, 1989

“And although it is a subject that meets with reluctance to open discussion, and has therefore too often been relegated to silence, the statistical evidence indicates that we are likely to lose another Space Shuttle in the next several years … probably before the planned Space Station is completely established on orbit. This would seem to be the weak link of the civil space program – unpleasant to recognize, involving all the uncertainties of statistics, and difficult to resolve.”

-The Augustine Committee, 1990

#### Shuttle as Developmental Vehicle

“Shuttle is also a complex system that has yet to demonstrate an ability to adhere to a fixed schedule”

-The Augustine Committee, 1990

#### NASA Human Space Flight Culture

“NASA has not been sufficiently responsive to valid criticism and the need for change.”\(^{22}\)

-The Augustine Committee, 1990

Faced with this budget situation, NASA had the choice of either eliminating major programs or achieving greater efficiencies while maintaining its existing agenda. Agency leaders chose to attempt the latter. They continued to develop the space station, continued robotic planetary and scientific missions, and continued Shuttle-based missions for both scientific and symbolic purposes. In 1994 they took on the responsibility for developing an advanced technology launch vehicle in partnership with the private sector. They tried to do this by becoming more efficient. “Faster, better, cheaper” became the NASA slogan of the 1990s.\(^{23}\)

The flat budget at NASA particularly affected the human space flight enterprise. During the decade before the Columbia accident, NASA rebalanced the share of its budget allocated to human space flight from 48 percent of agency funding in Fiscal Year 1991 to 38 percent in Fiscal Year 1999, with the remainder going mainly to other science and technology efforts. On NASA’s fixed budget, that meant...
EARMARKS

Pressure on NASA's budget has come not only from the White House, but also from the Congress. In recent years there has been an increasing tendency for the Congress to add “earmarks” – congressional additions to the NASA budget request that reflect targeted Members' interests. These earmarks come out of already-appropriated funds, reducing the amounts available for the original tasks. For example, as Congress considered NASA's Fiscal Year 2002 appropriation, the NASA Administrator told the House Appropriations subcommittee with jurisdiction over the NASA budget that the agency was “extremely concerned regarding the magnitude and number of congressional earmarks” in the House and Senate versions of the NASA appropriations bill.\(^24\) He noted “the total number of House and Senate earmarks ... is approximately 140 separate items, an increase of nearly 50 percent over FY 2001.” These earmarks reflected “an increasing fraction of items that circumvent the peer review process, or involve construction or other objectives that have no relation to NASA mission objectives.” The potential Fiscal Year 2002 earmarks represented “a net total of $540 million in reductions to ongoing NASA programs to fund this extremely large number of earmarks.”\(^25\)

For the past 30 years, the Space Shuttle Program has been NASA's single most expensive activity, and of all NASA's efforts, that program has been hardest hit by the budget constraints of the past decade. Given the high priority assigned after 1993 to completing the costly International Space Station, NASA managers have had little choice but to attempt to reduce the costs of operating the Space Shuttle. This left little funding for Shuttle improvements. The squeeze on the Shuttle budget was even more severe after the Office of Management and Budget in 1994 insisted that any cost overruns in the International Space Station budget be made up from within the budget allocation for human space flight, rather than from the agency's budget as a whole. The Shuttle was the only other large program within that budget category.

Figures 5.3-4 and 5.3-5 show the trajectory of the Shuttle budget over the past decade. In Fiscal Year 1993, the outgoing Bush administration requested $4.128 billion for the Space Shuttle Program; five years later, the Clinton Administration request was for $2.977 billion, a 27 percent reduction. By Fiscal Year 2003, the budget request had increased to $3.208 billion, still a 22 percent reduction from a decade earlier. With inflation taken into account, over the past decade, there has been a reduction of approximately 40 percent in the purchasing power of the program's budget, compared to a reduction of 13 percent in the NASA budget overall.

<table>
<thead>
<tr>
<th>Fiscal Year</th>
<th>President's Request to Congress</th>
<th>Congressional Appropriation</th>
<th>Change</th>
<th>NASA Operating Plan*</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1993</td>
<td>4,128.0</td>
<td>4,078.0</td>
<td>-50.0</td>
<td>4,052.9</td>
<td>-25.1</td>
</tr>
<tr>
<td>1994</td>
<td>4,196.1</td>
<td>3,778.7</td>
<td>-417.4*</td>
<td>3,772.3</td>
<td>-6.4</td>
</tr>
<tr>
<td>1995</td>
<td>3,324.0</td>
<td>3,155.1</td>
<td>-168.9</td>
<td>3,155.1</td>
<td>0.0</td>
</tr>
<tr>
<td>1996</td>
<td>3,231.8</td>
<td>3,178.8</td>
<td>-53.0</td>
<td>3,143.8</td>
<td>-35.0</td>
</tr>
<tr>
<td>1997</td>
<td>3,150.9</td>
<td>3,150.9</td>
<td>0.0</td>
<td>2,960.9</td>
<td>-190.0</td>
</tr>
<tr>
<td>1998</td>
<td>2,977.8</td>
<td>2,927.8</td>
<td>-50.0</td>
<td>2,912.8</td>
<td>-15.0</td>
</tr>
<tr>
<td>1999</td>
<td>3,059.0</td>
<td>3,028.0</td>
<td>-31.0</td>
<td>2,998.3</td>
<td>-29.7</td>
</tr>
<tr>
<td>2000</td>
<td>2,986.2</td>
<td>3,011.2</td>
<td>+25.0</td>
<td>2,984.4</td>
<td>-26.8</td>
</tr>
<tr>
<td>2001</td>
<td>3,165.7</td>
<td>3,125.7</td>
<td>-40.0</td>
<td>3,118.8</td>
<td>-6.9</td>
</tr>
<tr>
<td>2002</td>
<td>3,283.8</td>
<td>3,278.8</td>
<td>-5.0</td>
<td>3,270.0</td>
<td>-8.9</td>
</tr>
<tr>
<td>2003</td>
<td>3,208.0</td>
<td>3,252.8</td>
<td>+44.8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5.3-4. Space Shuttle Program Budget (in millions of dollars). (Source: NASA Office of Space Flight)

* NASA's operating plan is the means for adjusting congressional appropriations among various activities during the fiscal year as changing circumstances dictate. These changes must be approved by NASA's appropriation subcommittees before they can be put into effect.

**This reduction primarily reflects the congressional cancellation of the Advanced Solid Rocket Motor Program
This budget squeeze also came at a time when the Space Shuttle Program exhibited a trait common to most aging systems: increased costs due to greater maintenance requirements, a declining second- and third-tier contractor support base, and deteriorating infrastructure. Maintaining the Shuttle was becoming more expensive at a time when Shuttle budgets were decreasing or being held constant. Only in the last few years have those budgets begun a gradual increase.

As Figure 5.3-5 indicates, most of the steep reductions in the Shuttle budget date back to the first half of the 1990s. In the second half of the decade, the White House Office of Management and Budget and NASA Headquarters held the Shuttle budget relatively level by deferring substantial funding for Shuttle upgrades and infrastructure improvements, while keeping pressure on NASA to limit increases in operating costs.

5.4 Turbulence in NASA Hits the Space Shuttle Program

In 1992 the White House replaced NASA Administrator Richard Truly with aerospace executive Daniel S. Goldin, a self-proclaimed “agent of change” who held office from April 1, 1992, to November 17, 2001 (in the process becoming the longest-serving NASA Administrator). Seeing “space exploration (manned and unmanned) as NASA's principal purpose with Mars as a destiny,” as one management scholar observed, and favoring “administrative transformation” of NASA, Goldin engineered “not one or two policy changes, but a torrent of changes. This was not evolutionary change, but radical or discontinuous change.”

His tenure at NASA was one of continuous turmoil, to which the Space Shuttle Program was not immune.

Of course, turbulence does not necessarily degrade organizational performance. In some cases, it accompanies productive change, and that is what Goldin hoped to achieve. He believed in the management approach advocated by W. Edwards Deming, who had developed a series of widely acclaimed management principles based on his work in Japan during the “economic miracle” of the 1980s. Goldin attempted to apply some of those principles to NASA, including the notion that a corporate headquarters should not attempt to exert bureaucratic control over a complex organization, but rather set strategic directions and provide operating units with the authority and resources needed to pursue those directions. Another Deming principle was that checks and balances in an organization were unnecessary.
on certain launch pad areas being exposed to the elements. When rain falls on these areas, it carries away zinc, runs onto the leading edge of the Orbiter’s wings, and causes pinholes in the Reinforced Carbon-Carbon panels (see Chapter 3).

In 2000, NASA identified 100 infrastructure items that demanded immediate attention. NASA briefed the Space Flight Advisory Committee on this “Infrastructure Revitalization” initiative in November of that year. The Committee concluded that “deteriorating infrastructure is a serious, major problem,” and, upon touring several Kennedy Space Center facilities, declared them “in deplorable condition.” NASA subsequently submitted a request to the White House Office of Management and Budget during Fiscal Year 2002 budget deliberations for $600 million to fund the infrastructure initiative. No funding was approved.

In Fiscal Year 2002, Congress added $25 million to NASA’s budget for Vehicle Assembly Building repairs. NASA has reallocated limited funds from the Shuttle budget to pressuring infrastructure repairs, and intends to take an integrated look at infrastructure as part of its new Shuttle Service Life Extension Program. Nonetheless, like Space Shuttle upgrades, infrastructure revitalization has been mired by the uncertainty surrounding the Shuttle Program’s lifetime. Considering that the Shuttle will likely be flying for many years to come, NASA, the White House, and Congress alike now face the specter of having to deal with years of infrastructure neglect.

5.6 A CHANGE IN NASA LEADERSHIP

Daniel Goldin left NASA in November 2001 after more than nine years as Administrator. The White House chose Sean O’Keefe, the Deputy Director of the White House Office of Management and Budget, as his replacement. O’Keefe stated as he took office that he was not a “rocket scientist,” but rather that his expertise was in the management of large government programs. His appointment was an explicit acknowledgement by the new Bush administration that NASA’s primary problems were managerial and financial.

By the time O’Keefe arrived, NASA managers had come to recognize that 1990s funding reductions for the Space Shuttle Program had resulted in an excessively fragile program, and also realized that a Space Shuttle replacement was not on the horizon. In 2002, with these issues in mind, O’Keefe made a number of changes to the Space Shuttle Program. He transferred management of both the Space Shuttle Program and the International Space Station from Johnson Space Center to NASA Headquarters. O’Keefe also began considering whether to expand the Space Flight Operations Contract to cover additional Space Shuttle elements, or to pursue “competitive sourcing,” a Bush administration initiative that encouraged government agencies to compete with the private sector for management responsibilities of publicly funded activities. To research whether competitive sourcing would be a viable approach for the Space Shuttle Program, NASA chartered the Space Shuttle Competitive Sourcing Task Force through the RAND Corporation, a federally funded think tank. In its report, the Task Force recognized the many obstacles to transferring the Space Shuttle to non-NASA management, primarily NASA’s reticence to relinquish control, but concluded that “NASA must pursue competitive sourcing in one form or another.”

NASA began a “Strategic Management of Human Capital” initiative to ensure the quality of the future NASA workforce. The goal is to address the various external and internal challenges that NASA faces as it tries to ensure an appropriate mix and depth of skills for future program requirements. A number of aspects to its Strategic Human Capital Plan require legislative approval and are currently before the Congress.

Figure 5.5-4. Age of the Space Shuttle infrastructure. (Source: Connie Milton to Space Flight Advisory Council, 2000.)

Figure 5.5-5 and 5.5-6. Examples of the seriously deteriorating infrastructure used to support the Space Shuttle Program. At left is Launch Complex 39A, and at right is the Vehicle Assembly building, both at the Kennedy Space Center.
The new NASA leadership also began to compare Space Shuttle program practices with the practices of similar high-technology, high-risk enterprises. The Navy nuclear submarine program was the first enterprise selected for comparative analysis. An interim report on this “benchmarking” effort was presented to NASA in December 2002.\

In November 2002, NASA made a fundamental change in strategy. In what was called the Integrated Space Transportation Plan (see Figure 5.6-1), NASA shifted money from the Space Launch Initiative to the Space Shuttle and International Space Station programs. The plan also introduced the Orbital Space Plane as a complement to the Shuttle for the immediate future. Under this strategy, the Shuttle is to fly through at least 2010, when a decision will be made on how long to extend Shuttle operations – possibly through 2020 or even beyond.

As a step in implementing the plan, NASA included $281.4 million in its Fiscal Year 2004 budget submission to begin a Shuttle Service Life Extension Program, which NASA describes as a “strategic and proactive program designed to keep the Space Shuttle flying safely and efficiently.” The program includes “high priority projects for safety, supportability, and infrastructure” in order to “combat obsolescence of vehicle, ground systems, and facilities.”

5. 7 THE RETURN OF SCHEDULE PRESSURE

The International Space Station has been the centerpiece of NASA’s human space flight program in the 1990s. In several instances, funds for the Shuttle Program have paid for various International Space Station items. The Space Station has also affected the Space Shuttle Program schedule. By the time the functional cargo block Zarya, the Space Station’s first element, was launched from the Baikonur Cosmodrome in Kazakhstan in November 1998, the Space Station was two years behind schedule. The launch of STS-88, the first of many Shuttle missions assigned to station assembly, followed a month later. Another four assembly missions in 1999 and 2000 readied the station for its first permanent crew, Expedition 1, which arrived in late 2000.

When the Bush Administration came to the White House in January 2001, the International Space Station program was $4 billion over its projected budget. The Administration’s Fiscal Year 2002 budget, released in February 2001, declared that the International Space Station would be limited to a “U.S Core Complete” configuration, a reduced design that could accommodate only three crew members. The last step in completing the U.S. portion of this configuration would be the addition of the Italian-supplied but U.S.-owned “Node 2,” which would allow Europe and Japan to connect their laboratory modules to the Station. Launching Node 2 and thereby finishing “core complete” configuration became an important political and programmatic milestone (see Figure 5.7-1).

During congressional testimony in May of 2001, Sean O’Keefe, who was then Deputy Director of the White House Office of Management and Budget, presented the Administration’s plan to bring International Space Station costs under control. The plan outlined a reduction in assembly and logistics flights to reach “core complete” configuration from 36 to 30. It also recommended redirecting about $1 billion in funding by canceling U.S. elements not yet completed, such as the habitation module and the X-38 Crew Return Vehicle. The X-38 would have allowed emergency evacuation and landing capability for a seven-member station crew. Without it, the crew was limited to three, the number that could fit into a Russian Soyuz crew rescue vehicle.

In his remarks, O’Keefe stated:

NASA’s degree of success in gaining control of cost growth on Space Station will not only dictate the capabilities that the Station will provide, but will send a strong signal about the ability of NASA’s Human Space Flight program to effectively manage large development programs. NASA’s credibility with the Administration and the Congress for delivering on what is promised and the longer-term implications that such credibility may have on the future of Human Space Flight hang in the balance.

At the request of the White House Office of Management and Budget, in July 2001 NASA Administrator Dan Goldin...
formed an International Space Station Management and Cost Evaluation Task Force. The International Space Station Management and Cost Evaluation Task Force was to assist NASA in identifying the reforms needed to restore the Station Program’s fiscal and management credibility.

While the primary focus of the Task Force was on the Space Station Program management, its November 2001 report issued a general condemnation of how NASA, and particularly Johnson Space Center, had managed the International Space Station, and by implication, NASA’s overall human space flight effort. The report noted “existing deficiencies in management structure, institutional culture, cost estimating, and program control,” and that “the institutional needs of the [human space flight] Centers are driving the Program, rather than Program requirements being served by the Centers.” The Task Force suggested that as a cost control measure, the Space Shuttle be limited to four flights per year and that NASA revise the station crew rotation period to six months. The cost savings that would result from eliminating flights could be used to offset cost overruns.

NASA accepted a reduced flight rate. The Space Shuttle Program office concluded that, based on a rate of four flights a year, Node 2 could be launched by February 19, 2004.

In testimony before the House Committee on Science on November 7, 2001, Task Force Chairman Thomas Young identified what became known as a “performance gate.” He suggested that over the next two years, NASA should plan and implement a credible “core complete” program. In Fall 2003, “an assessment would be made concerning the ISS program performance and NASA’s credibility. If satisfactory, resource needs would be assessed and an [ISS] ‘end state’ that realized the science potential would become the baseline. If unsatisfactory, the core complete program would become the ‘end state.’”

Testifying the same day, Office of Management and Budget Deputy Director Sean O’Keefe indicated the Administration’s agreement with the planned performance gate:

The concept presented by the task force of a decision gate in two years that could lead to an end state other than the U.S. core complete Station is an innovative approach, and one the Administration will adopt. It calls for NASA to make the necessary management reforms to successfully build the core complete Station and operate it within the $8.3 billion available through FY 2006 plus other human space flight resources … If NASA fails to meet the standards, then an end-state beyond core complete is not an option. The strategy places the burden of proof on NASA performance to ensure that NASA fully implements the needed reforms.75

Mr. O’Keefe added in closing:

A most important next step – one on which the success of all these reforms hinges – is to provide new leadership for NASA and its Human Space Flight activities. NASA has been well-served by Dan Goldin. New leadership is now necessary to continue moving the ball down the field with the goal line in sight. The Administration recognizes the importance of getting the right leaders in place as soon as possible, and I am personally engaged in making sure that this happens.

A week later, Sean O’Keefe was nominated by President Bush as the new NASA Administrator.

To meet the new flight schedule, in 2002 NASA revised its Shuttle manifest, calling for a docking adaptor to be installed in Columbia after the STS-107 mission so that it could make an October 2003 flight to the International Space Station. Columbia was not optimal for Station flights – the Orbiter could not carry enough payload – but it was assigned to this flight because Discovery was scheduled for 18 months of major maintenance. To ensure adequate Shuttle availability for the February 2004 Node 2 launch date, Columbia would fly an International Space Station resupply mission.

The White House and Congress had put the International Space Station Program, the Space Shuttle Program, and indeed NASA on probation. NASA had to prove it could meet schedules within cost, or risk halting Space Station construction at core complete – a configuration far short of what NASA anticipated. The new NASA management viewed the achievement of an on-schedule Node 2 launch as an endorsement of its successful approach to Shuttle and Station Programs. Any suggestions that it would be difficult to meet that launch date were brushed aside.

This insistence on a fixed launch schedule was worrisome. The International Space Station Management and Cost Evaluation Task Force, in particular, was concerned with the emphasis on a specific launch date. It noted in its 2002 review of progress toward meeting its recommendations that “significant progress has been made in nearly all aspects of the ISS Program,” but that there was “significant risk with the Node 2 (February ’04) schedule.”

By November 2002, NASA had flown 16 Space Shuttle missions dedicated to Station assembly and crew rotation. Five crews had lived onboard the Station, the last four of them delivered via Space Shuttles. As the Station had grown, so had the complexity of the missions required to complete it. With the International Space Station assembly more than half complete, the Station and Shuttle programs had become irreversibly linked. Any problems with or perturbations to the planned schedule of one program reverberated through both programs. For the Shuttle program, this meant that the conduct of all missions, even non-Station missions like STS-107, would have an impact on the Node 2 launch date.

In 2002, this reality, and the events of the months that would follow, began to place additional schedule pressures on the Space Shuttle Program. Those pressures are discussed in Section 6.2.

5.8 Conclusion

Over the last decade, the Space Shuttle Program has operated in a challenging and often turbulent environment. As
discussed in this chapter, there were at least three major contributing factors to that environment:

- Throughout the decade, the Shuttle Program has had to function within an increasingly constrained budget. Both the Shuttle budget and workforce have been reduced by over 40 percent during the past decade. The White House, Congress, and NASA leadership exerted constant pressure to reduce or at least freeze operating costs. As a result, there was little margin in the budget to deal with unexpected technical problems or make Shuttle improvements.

- The Shuttle was mischaracterized by the 1995 Kraft Report as “a mature and reliable system ... about as safe as today’s technology will provide.” Based on this mischaracterization, NASA believed that it could turn increased responsibilities for Shuttle operations over to a single prime contractor and reduce its direct involvement in ensuring safe Shuttle operations, instead monitoring contractor performance from a more detached position. NASA also believed that it could use the “mature” Shuttle to carry out operational missions without continually focusing engineering attention on understanding the mission-by-mission anomalies inherent in a developmental vehicle.

- In the 1990s, the planned date for replacing the Shuttle shifted from 2006 to 2012 and then to 2015 or later. Given the uncertainty regarding the Shuttle’s service life, there has been policy and budgetary ambivalence on investing in the vehicle. Only in the past year has NASA begun to provide the resources needed to sustain extended Shuttle operations. Previously, safety and support upgrades were delayed or deferred, and Shuttle infrastructure was allowed to deteriorate.

The Board observes that this is hardly an environment in which those responsible for safe operation of the Shuttle can function without being influenced by external pressures. It is to the credit of Space Shuttle managers and the Shuttle workforce that the vehicle was able to achieve its program objectives for as long as it did.

An examination of the Shuttle Program’s history from Challenger to Columbia raises the question: Did the Space Shuttle Program budgets constrained by the White House and Congress threaten safe Shuttle operations? There is no straightforward answer. In 1994, an analysis of the Shuttle budget concluded that reductions made in the early 1990s represented a “healthy tightening up” of the program. Certainly those in the Office of Management and Budget and in NASA’s congressional authorization and appropriations subcommittees thought they were providing enough resources to operate the Shuttle safely, while also taking into account the expected Shuttle lifetime and the many other demands on the Federal budget. NASA Headquarters agreed, at least until Administrator Goldin declared a “space launch crisis” in June 1999 and asked that additional resources for safety upgrades be added to the NASA budget. By 2001, however, one experienced observer of the space program described the Shuttle workforce as “The Few, the Tired,” and suggested that “a decade of downsizing and budget tightening has left NASA exploring the universe with a less experienced staff and older equipment.”

It is the Board’s view that this latter statement is an accurate depiction of the Space Shuttle Program at the time of STS-107. The Program was operating too close to too many margins. The Board also finds that recent modest increases in the Shuttle Program’s budget are necessary and overdue steps toward providing the resources to sustain the program for its now-extended lifetime. Similarly, NASA has recently recognized that providing an adequately sized and appropriately trained workforce is critical to the agency’s future success.

An examination of the Program’s management changes also leads to the question: Did turmoil in the management structure contribute to the accident? The Board found no evidence that the transition from many Space Shuttle contractors to a partial consolidation of contracts under a single firm has by itself introduced additional technical risk into the Space Shuttle Program. The transfer of responsibilities that has accompanied the Space Flight Operations Contract has, however, complicated an already complex Program structure and created barriers to effective communication. Designating the Johnson Space Center as the “lead center” for the Space Shuttle Program did resurface some of the Center rivalries and communication difficulties that existed before the Challenger accident. The specific ways in which this complexity and lack of an integrated approach to Shuttle management impinged on NASA’s performance during and before the flight of STS-107 are discussed in Chapters 6 and 7.

As the 21st century began, NASA’s deeply ingrained human space flight culture – one that has evolved over 30 years as the basis for a more conservative, less technically and organizationally capable organization than the Apollo-era NASA – remained strong enough to resist external pressures for adaptation and change. At the time of the launch of STS-107, NASA retained too many negative (and also many positive) aspects of its traditional culture: “flawed decision making, self deception, introversion and a diminished curiosity about the world outside the perfect place.” These characteristics were reflected in NASA’s less than stellar performance before and during the STS-107 mission, which is described in the following chapters.
ENDNOTES FOR CHAPTER 5

The citations that contain a reference to “CAIB document” with CAB or CTF followed by seven to eleven digits, such as CA0001-0010, refer to a document in the Columbia Accident Investigation Board database maintained by the Department of Justice and archived at the National Archives.

7 Vice President’s Space Policy Advisory Board, A Past Cold War Assessment of U.S. Space Policy, December 1992, p. 6.
10 There are proposals for using other U.S. systems, in development but not yet ready for flight, to provide an alternate U.S. means of station access. These “Alternate Access to Space” proposals have not been evaluated by the Board.
15 As NASA human space flight personnel began to become closely involved with their counterparts in the Russian space program after 1992, there was grudging acceptance that Russian human space flight personnel were also skilled in their work, although they carried it out rather differently than did NASA.
18 Report of the Advisory Committee on the Future of the U.S. Space Program. Measured in terms of total national spending, the report’s recommendations would have returned NASA spending to 0.38 percent of U.S. Gross Domestic Product – a level of investment not seen since 1969.
22 Report of the Advisory Committee on the Future of the U.S. Space Program.
25 Ibid.
27 Deming’s management philosophy was not the only new notion that Goldin attempted to apply to NASA. He was also an advocate of the “Total Quality Management” approach and other modern management schemes. Trying to adapt to these various management theories was a source of some stress.
28 For a discussion of Goldin’s approach, see Howard McCurdy, Faster, Better, Cheaper: Low-Cost Innovation in the U.S. Space Program (Baltimore: The Johns Hopkins University Press, 2001). It is worth noting that while the “faster, better, cheaper” approach led to many more NASA robotic missions being launched after 1992, not all of those missions were successful. In particular, there were two embarrassing failures of Mars missions in 1999.
29 Lambright, Transforming Government, provides an early but comprehensive evaluation of the Goldin record. The quote is from p. 28.
31 McCurdy, Faster, Better, Cheaper.

Information obtained from Anna Henderson, NASA Office of Space Flight, to e-mail to John Logsdon, June 13, 2003.


Ibid., pp. 3-18.


Russell Turner, testimony at public hearing before the Columbia Accident Investigation Board, June 12, 2003.

See Section 204 of Public Law 105-303, October 28, 1999.


Ibid.


The quotes are taken from NASA-submitted material appended to the statement of NASA Administrator Daniel Goldin to the Senate Subcommittee on Science, Technology and Space, March 22, 2000, p. 7.


“Statement of William F. Readdy, Deputy Associate Administrator, Office of Space Flight, National Aeronautics and Space Administration before the Subcommittee on Space and Aeronautics Committee on Science, House of Representatives,” October 21, 1999. CAIB document CAB026-0146.

Letter from Daniel Goldin to Jacob Lew, Director, Office of Management and Budget, July 6, 1999.


Ibid.

Ibid.


Ibid.

The few, the tired,” Public Papers of the Presidents of the United States: Ronald Reagan: Book I, January 1 to June 27, 1986. CAIB document CTF005-0283.


The dwindling post-Cold War Shuttle budget that launched NASA leadership on a crusade for efficiency in the decade before Columbia’s final flight powerfully shaped the environment in which Shuttle managers worked. The increased organizational complexity, transitioning authority structures, and ambiguous working relationships that defined the restructured Space Shuttle Program in the 1990s created turbulence that repeatedly influenced decisions made before and during STS-107.

This chapter connects Chapter 5’s analysis of NASA’s broader policy environment to a focused scrutiny of Space Shuttle Program decisions that led to the STS-107 accident. Section 6.1 illustrates how foam debris losses that violated design requirements came to be defined by NASA management as an acceptable aspect of Shuttle missions, one that posed merely a maintenance “turnaround” problem rather than a safety-of-flight concern. Section 6.2 shows how, at a pivotal juncture just months before the Columbia accident, the management goal of completing Node 2 of the International Space Station on time encouraged Shuttle managers to continue flying, even after a significant bipod-foam debris strike on STS-112. Section 6.3 notes the decisions made during STS-107 in response to the bipod foam strike, and reveals how engineers’ concerns about risk and safety were competing with – and were defeated by – management’s belief that foam could not hurt the Orbiter, as well as the need to keep on schedule. In relating a rescue and repair scenario that might have enabled the crew’s safe return, Section 6.4 grapples with yet another latent assumption held by Shuttle managers during and after STS-107: that even if the foam strike had been discovered, nothing could have been done.

6.1 A History of Foam Anomalies

The shedding of External Tank foam – the physical cause of the Columbia accident – had a long history. Damage caused by debris has occurred on every Space Shuttle flight, and most missions have had insulating foam shed during ascent. This raises an obvious question: Why did NASA continue flying the Shuttle with a known problem that violated design requirements? It would seem that the longer the Shuttle Program allowed debris to continue striking the Orbiters, the more opportunity existed to detect the serious threat it posed. But this is not what happened. Although engineers have made numerous changes in foam design and application in the 25 years that the External Tank has been in production, the problem of foam-shedding has not been solved, nor has the Orbiter’s ability to tolerate impacts from foam or other debris been significantly improved.

The Need for Foam Insulation

The External Tank contains liquid oxygen and hydrogen propellants stored at minus 297 and minus 423 degrees Fahrenheit. Were the super-cold External Tank not sufficiently insulated from the warm air, its liquid propellants would boil, and atmospheric nitrogen and water vapor would condense and form thick layers of ice on its surface. Upon launch, the ice could break off and damage the Orbiter. (See Chapter 3.)

To prevent this from happening, large areas of the External Tank are machine-sprayed with one or two inches of foam, while specific fixtures, such as the bipod ramps, are hand-sculpted with thicker coats. Most of these insulating materials fall into a general category of “foam,” and are outwardly similar to hardware store-sprayable foam insulation. The problem is that foam does not always stay where the External Tank manufacturer Lockheed Martin installs it. During flight, popcorn- to briefcase-size chunks detach from the External Tank.

Original Design Requirements

Early in the Space Shuttle Program, foam loss was considered a dangerous problem. Design engineers were extremely concerned about potential damage to the Orbiter and its fragile Thermal Protection System, parts of which are so vulnerable to impacts that lightly pressing a thumbnail into them leaves a mark. Because of these concerns, the baseline
Columbia having been equipped with umbilical cameras earlier than other Orbiters.

F6.1–4 There is lack of effective processes for feedback or integration among project elements in the resolution of In-Flight Anomalies.

F6.1–5 Foam bipod debris-shedding incidents on STS-52 and STS-62 were undetected at the time they occurred, and were not discovered until the Board directed NASA to examine External Tank separation images more closely.

F6.1–6 Foam bipod debris-shedding events were classified as In-Flight Anomalies up until STS-112, which was the first known bipod foam-shedding event not classified as an In-Flight Anomaly.

F6.1–7 The STS-112 assignment for the External Tank Project to “identify the cause and corrective action of the bipod ramp foam loss event” was due after the planned launch of STS-113, and then slipped to after the launch of STS-107.

F6.1–8 No External Tank configuration changes were made after the bipod foam loss on STS-112.

F6.1–9 Although it is sometimes possible to obtain imagery of night launches because of light provided by the Solid Rocket Motor plume, no imagery was obtained for STS-113.

F6.1–10 NASA failed to adequately perform trend analysis on foam losses. This greatly hampered the agency’s ability to make informed decisions about foam losses.

F6.1–11 Despite the constant shedding of foam, the Shuttle Program did little to harden the Orbiter against foam impacts through upgrades to the Thermal Protection System. Without impact resistance and strength requirements that are calibrated to the energy of debris likely to impact the Orbiter, certification of new Thermal Protection System tile will not adequately address the threat posed by debris.

Recommendations:

• None

6.2 SCHEDULE PRESSURE

Countdown to Space Station “Core Complete:” A Workforce Under Pressure

During the course of this investigation, the Board received several unsolicited comments from NASA personnel regarding pressure to meet a schedule. These comments all concerned a date, more than a year after the launch of Columbia, that seemed etched in stone: February 19, 2004, the scheduled launch date of STS-120. This flight was a milestone in the minds of NASA management since it would carry a section of the International Space Station called “Node 2.” This would configure the International Space Station to its “U.S. Core Complete” status.

At first glance, the Core Complete configuration date seemed noteworthy but unrelated to the Columbia accident. However, as the investigation continued, it became apparent that the complexity and political mandates surrounding the International Space Station Program, as well as Shuttle Program management’s responses to them, resulted in pressure to meet an increasingly ambitious launch schedule.

In mid-2001, NASA adopted plans to make the over-budget and behind-schedule International Space Station credible to the White House and Congress. The Space Station Program and NASA were on probation, and had to prove they could meet schedules and budgets. The plan to regain credibility focused on the February 19, 2004, date for the launch of Node 2 and the resultant Core Complete status. If this goal was not met, NASA would risk losing support from the White House and Congress for subsequent Space Station growth.

By the late summer of 2002, a variety of problems caused Space Station assembly work and Shuttle flights to slip beyond their target dates. With the Node 2 launch endpoint fixed, these delays caused the schedule to become ever more compressed.

Meeting U.S. Core Complete by February 19, 2004, would require preparing and launching 10 flights in less than 16 months. With the focus on retaining support for the Space Station program, little attention was paid to the effects the aggressive Node 2 launch date would have on the Shuttle Program. After years of downsizing and budget cuts (Chapter 5), this mandate and events in the months leading up to STS-107 introduced elements of risk to the Program. Columbia and the STS-107 crew, who had seen numerous launch slips due to missions that were deemed higher priorities, were further affected by the mandatory Core Complete date. The high-pressure environments created by NASA Headquarters unquestionably affected Columbia, even though it was not flying to the International Space Station.

February 19, 2004 – “A Line in the Sand”

Schedules are essential tools that help large organizations effectively manage their resources. Aggressive schedules by themselves are often a sign of a healthy institution. However, other institutional goals, such as safety, sometimes compete with schedules, so the effects of schedule pressure in an organization must be carefully monitored. The Board posed the question: Was there undue pressure to nail the Node 2 launch date to the February 19, 2004, signpost? The management and workforce of the Shuttle and Space Station programs each answered the question differently. Various members of NASA upper management gave a definite “no.” In contrast, the workforce within both programs thought there was considerable management focus on Node 2 and resulting pressure to hold firm to that launch date, and individuals were becoming concerned that safety might be compromised. The weight of evidence supports the workforce view.

Employees attributed the Node 2 launch date to the new Administrator, Sean O’Keefe, who was appointed to execute a Space Station management plan he had proposed as Deputy Director of the White House Office of Management and Budget. They understood the scrutiny that NASA, the new Administrator, and the Space Station Program were under,
but now it seemed to some that budget and schedule were of paramount concern. As one employee reflected:

I guess my frustration was … I know the importance of showing that you … manage your budget and that’s an important impression to make to Congress so you can continue the future of the agency, but to a lot of people, February 19th just seemed like an arbitrary date … It doesn’t make sense to me why at all costs we were marching to this date.

The importance of this date was stressed from the very top. The Space Shuttle and Space Station Program Managers briefed the new NASA Administrator monthly on the status of their programs, and a significant part of those briefings was the days of margin remaining in the schedule to the launch of Node 2 – still well over a year away. The Node 2 schedule margin typically accounted for more than half of the briefing slides.

Figure 6.2-1 is one of the charts presented by the Shuttle Program Manager to the NASA Administrator in December 2002. The chart shows how the days of margin in the existing schedule were being managed to meet the requirement of a Node 2 launch on the prescribed date. The triangles are events that affected the schedule (such as the slip of a Russian Soyuz flight). The squares indicate action taken by management to regain the lost time (such as authorizing work over the 2002 winter holidays).

Figure 6.2-2 shows a slide from the International Space Station Program Manager’s portion of the briefing. It indicates that International Space Station Program management was also taking actions to regain margin. Over the months, the extent of some testing at Kennedy was reduced, the number of tasks done in parallel was increased, and a third shift of workers would be added in 2003 to accomplish the processing. These charts illustrate that both the Space Shuttle and Space Station Programs were being managed to a particular launch date – February 19, 2004. Days of margin in that schedule were one of the principle metrics by which both programs came to be judged.

NASA Headquarters stressed the importance of this date in other ways. A screen saver (see Figure 6.2-3) was mailed to managers in NASA’s human spaceflight program that depicted a clock counting down to February 19, 2004 – U.S. Core Complete.
While employees found this amusing because they saw it as a date that could not be met, it also reinforced the message that NASA Headquarters was focused on and promoting the achievement of that date. This schedule was on the minds of the Shuttle managers in the months leading up to STS-107.

The Background: Schedule Complexity and Compression

In 2001, the International Space Station Cost and Management Evaluation Task Force report recommended, as a cost-saving measure, a limit of four Shuttle flights to the International Space Station per year. To meet this requirement, managers began adjusting the Shuttle and Station manifests to “get back in the budget box.” They rearranged Station assembly sequences, moving some elements forward and taking others out. When all was said and done, the launch of STS-120, which would carry Node 2 to the International Space Station, fell on February 19, 2004.

The Core Complete date simply emerged from this planning effort in 2001. By all accounts, it was a realistic and achievable date when first approved. At the time there was more concern that four Shuttle flights a year would limit the capability to carry supplies to and from the Space Station, to rotate its crew, and to transport remaining Space Station segments and equipment. Still, managers felt it was a rea-
sonable goal and assumed that if circumstances warranted a slip of that date, it would be granted.

Shuttle and Station managers worked diligently to meet the schedule. Events gradually ate away at the schedule margin. Unlike the “old days” before the Station, the Station/Shuttle partnership created problems that had a ripple effect on both programs’ manifests. As one employee described it, “the serial nature” of having to fly Space Station assembly missions in a specific order made staying on schedule more challenging. Before the Space Station, if a Shuttle flight had to slip, it would; other missions that had originally followed it would be launched in the meantime. Missions could be flown in any sequence. Now the manifests were a delicate balancing act. Missions had to be flown in a certain order and were constrained by the availability of the launch site, the Russian Soyuz and Progress schedules, and a myriad of other processes. As a result, employees stated they were now experiencing a new kind of pressure. Any necessary change they made on one mission was now impacting future launch dates. They had a sense of being “under the gun.”

Shuttle and Station program personnel ended up with manifests that one employee described as “changing, changing, changing” all the time. One of the biggest issues they faced entering 2002 was “up mass,” the amount of cargo the Shuttle can carry to the Station. Up mass was not a new problem, but when the Shuttle flight rate was reduced to four per year, it became critical. Working groups were actively evaluating options in the summer of 2002 and bartering to get each flight to function as expected.

Sometimes the up mass being traded was actual Space Station crew members. A crew rotation planned for STS-118 was moved to a later flight because STS-118 was needed for other cargo. This resulted in an increase of crew duration on the Space Station, which was creeping past the 180-day limit agreed to by the astronaut office, flight surgeons, and Space Station international partners. A space station worker described how this one change created many other problems, and added: “… we had a train wreck coming …” Future on-orbit crew time was being projected at 205 days or longer to maintain the assembly sequence and meet the schedule.

By July 2002, the Shuttle and Space Station Programs were facing a schedule with very little margin. Two setbacks occurred when technical problems were found during routine maintenance on Discovery. STS-107 was four weeks away from launch at the time, but the problems grounded the entire Shuttle fleet. The longer the fleet was grounded, the more schedule margin was lost, which further complicated the complexity of the intertwined Shuttle and Station schedules. As one worker described the situation:

… a one-week hit on a particular launch can start a steam roll effect including all [the] constraints and by the time you get out of here, that one-week slip has turned into a couple of months.

In August 2002, the Shuttle Program realized it would be unable to meet the Space Station schedule with the available Shuttles. Columbia had never been outfitted to make a Space Station flight, so the other three Orbiters flew the Station missions. But Discovery was in its Orbiter Maintenance Down Period, and would not be available for another 17 months. All Space Station flights until then would have to be made by Atlantis and Endeavour. As managers looked ahead to 2003, they saw that after STS-107, these two Orbiters would have to alternate flying five consecutive missions, STS-114 through STS-118. To alleviate this pressure, and regain schedule margin, Shuttle Program managers elected to modify Columbia to enable it to fly Space Station missions. Those modifications were to take place immediately after STS-107 so that Columbia would be ready to fly its first Space Station mission eight months later. This decision put Columbia directly in the path of Core Complete.

As the autumn of 2002 began, both the Space Shuttle and Space Station Programs began to use what some employees termed “tricks” to regain schedule margin. Employees expressed concern that their ability to gain schedule margin using existing measures was waning.

In September 2002, it was clear to Space Shuttle and Space Station Program managers that they were not going to meet the schedule as it was laid out. The two Programs proposed a new set of launch dates, documented in an e-mail (right) that included moving STS-120, the Node 2 flight, to mid-March 2004. (Note that the first paragraph ends with “… the 10A [U.S. Core Complete, Node 2] launch remains 2/19/04.”)

These launch date changes made it possible to meet the early part of the schedule, but compressed the late 2003/early 2004 schedule even further. This did not make sense to many in the program. One described the system as at “an uncomfortable point,” noting having to go to great lengths to reduce vehicle-processing time at Kennedy, and added:

… I don't know what Congress communicated to O'Keefe. I don't really understand the criticality of February 19th, that if we didn't make that date, did that mean the end of NASA? I don't know … I would like to think that the technical issues and safely resolving the technical issues can take priority over any budget issue or scheduling issue.

When the Shuttle fleet was cleared to return to flight, attention turned to STS-112, STS-113, and STS-107, set for October, November, and January. Workers were uncomfortable with the rapid sequence of flights.

The thing that was beginning to concern me … is I wasn’t convinced that people were being given enough time to work the problems correctly.

The problems that had grounded the fleet had been handled well, but the program nevertheless lost the rest of its margin. As the pressure to keep to the Node 2 schedule continued, some were concerned that this might influence the future handling of problems. One worker expressed the concern:

… and I have to think that subconsciously that even though you don’t want it to affect decision-making, it probably does.
This was the environment for October and November of 2002. During this time, a bipod foam event occurred on STS-112. For the first time in the history of the Shuttle Program, the Program Requirements Control Board chose to classify that bipod foam loss as an “action” rather than a more serious In-Flight Anomaly. At the STS-113 Flight Readiness Review, managers accepted with little question the rationale that it was safe to fly with the known foam problem.

The Operations Tempo Following STS-107

After STS-107, the tempo was only going to increase. The vehicle processing schedules, training schedules, and mission control flight staffing assignments were all overburdened.

The vehicle-processing schedule for flights from February 2003, through February 2004, was optimistic. The schedule...
could not be met with only two shifts of workers per day. In late 2002, NASA Headquarters approved plans to hire a third shift. There were four Shuttle launches to the Space Station scheduled in the five months from October 2003, through the launch of Node 2 in February 2004. To put this in perspective, the launch rate in 1985, for which NASA was criticized by the Rogers Commission, was nine flights in 12 months – and that was accomplished with four Orbiters and a manifest that was not complicated by Space Station assembly.

*Endeavour* was the Orbiter on the critical path. Figure 6.2-4 shows the schedule margin for STS-115, STS-117, and STS-120 (Node 2). To preserve the margin going into 2003, the vehicle processing team would be required to work the late 2002–early 2003 winter holidays. The third shift of workers at Kennedy would be available in March 2003, and would buy eight more days of margin for STS-117 and STS-120. The workforce would likely have to work on the 2003 winter holidays to meet the Node 2 date.

Figure 6.2-5 shows the margin for each vehicle (*Discovery*, OV-103, was in extended maintenance). The large boxes indicate the “margin to critical path” (to Node 2 launch date). The three smaller boxes underneath indicate (from left to right) vehicle processing margin, holiday margin, and Dryden margin. The vehicle processing margin indicates how many days there are in addition to the days required for that mission’s vehicle processing. *Endeavour* (OV-105) had zero days of margin for the processing flows for STS-115, STS-117, and STS-120. The holiday margin is the number of days that could be gained by working holidays. The Dryden margin is the six days that are always reserved to accommodate an Orbiter landing at Edwards Air Force Base in California and having to be ferried to Kennedy. If the Orbiter landed at Kennedy, those six days would automatically be regained. Note that the Dryden margin had already been surrendered in the STS-114 and STS-115 schedules. If bad weather at Kennedy forced those two flights to land at Edwards, the schedule would be directly affected.

The clear message in these charts is that any technical problem that resulted in a slip to one launch would now directly affect the Node 2 launch.

The lack of housing for the Orbiters was becoming a factor as well. Prior to launch, an Orbiter can be placed in an Orbiter Processing Facility, the Vehicle Assembly Building, or on one of the two Shuttle launch pads. Maintenance and
refurbishment is performed in the three Orbiter Processing Facilities at Kennedy. One was occupied by Discovery during its scheduled extended maintenance. This left two to serve the other three Orbiters over the next several months. The 2003 schedule indicated plans to move Columbia (after its return from STS-107) from an Orbiter Processing Facility to the Vehicle Assembly Building and back several times in order to make room for Atlantis (OV-104) and Endeavour (OV-105) and prepare them for missions. Moving an Orbiter is tedious, time-consuming, carefully orchestrated work. Each move introduces an opportunity for problems. Those 2003 moves were often slated to occur without a day of margin between them – another indication of the additional risks that managers were willing to incur to meet the schedule.

The effect of the compressed schedule was also evident in the Mission Operations Directorate. The plans for flight controller staffing of Mission Control showed that of the seven flight controllers who lacked current certifications during STS-107 (see Chapter 4), five were scheduled to work the next mission, and three were scheduled to work the next three missions (STS-114, -115, and -116). These controllers would have been constantly either supporting missions or supporting mission training, and were unlikely to have the time to complete the recertification requirements. With the pressure of the schedule, the things perceived to be less important, like recertification (which was not done before STS-107), would likely continue to be deferred. As a result of the schedule pressure, managers either were willing to delay recertification or were too busy to notice that deadlines for recertification had passed.

Columbia: Caught in the Middle

STS-112 flew in October 2002. At 33 seconds into the flight, a piece of the bipod foam from the External Tank struck one of the Solid Rocket Boosters. As described in Section 6.1, the STS-112 foam strike was discussed at the Program Requirements Control Board following the flight. Although the initial recommendation was to treat the foam loss as an In-Flight Anomaly, the Shuttle Program instead assigned it as an action, with a due date after the next launch. (This was the first instance of bipod foam loss that was not designated an In-Flight Anomaly.) The action was noted at the STS-113 Flight Readiness Review. Those Flight Readiness Review charts (see Section 6.1) provided a flawed flight rationale by concluding that the foam loss was "not a safety-of-flight" issue.

**SSP Schedule Reserve**

![SSP Schedule Reserve Diagram]

Figure 6.2-5. This slide shows the margin for each Orbiter. The large boxes show the number of days margin to the Node 2 launch date, while the three smaller boxes indicate vehicle processing margin, holiday margin, and the margin if a Dryden landing was not required.

**SSP Core Complete Schedule Threats**

- Space Shuttle technical problems
- Station on-orbit technical problems/mission requirements impact
- Range launch cutouts
- Weather delays
- Soyuz and Progress conflicts

**Management Options**

- USA commit holiday/weekend reserves and apply additional resources (i.e., 3rd shift) to hold schedule (Note: 3rd shift not yet included)
- HQ mitigate Range Cutout
- HQ and ISS mitigate Soyuz conflict threat
Interestingly, during Columbia’s mission, the Chair of the Mission Management Team, Linda Ham, would characterize that reasoning as “lousy” – though neither she nor Shuttle Program Manager Ron Dittemore, who were both present at the meeting, questioned it at the time. The pressing need to launch STS-113 to retrieve the International Space Station Expedition 5 crew before they surpassed the 180-day limit and to continue the countdown to Node 2 were surely in the back of managers’ minds during these reviews.

By December 2002, every bit of padding in the schedule had disappeared. Another chart from the Shuttle and Station Program Managers’ briefing to the NASA Administrator summarizes the schedule dilemma (see Figure 6.2-6).

Even with work scheduled on holidays, a third shift of workers being hired and trained, future crew rotations drifting beyond 180 days, and some tests previously deemed “requirements” being skipped or deferred, Program managers estimated that Node 2 launch would be one to two months late. They were slowly accepting additional risk in trying to meet a schedule that probably could not be met.

Interviews with workers provided insight into how this situation occurred. They noted that people who work at NASA have the legendary can-do attitude, which contributes to the agency’s successes. But it can also cause problems. When workers are asked to find days of margin, they work furiously to do so and are praised for each extra day they find. But those same people (and this same culture) have difficulty admitting that something “can’t” or “shouldn’t” be done, that the margin has been cut too much, or that resources are being stretched too thin. No one at NASA wants to be the one to stand up and say, “We can’t make that date.”

STS-107 was launched on January 16, 2003. Bipod foam separated from the External Tank and struck Columbia’s left wing 81.9 seconds after liftoff. As the mission proceeded over the next 16 days, critical decisions about that event would be made.

The STS-107 Mission Management Team Chair, Linda Ham, had been present at the Program Requirements Control Board discussing the STS-112 foam loss and the STS-113 Flight Readiness Review. So had many of the other Shuttle Program managers who had roles in STS-107. Ham was also the Launch Integration Manager for the next mission, STS-114. In that capacity, she would chair many of the meetings leading up to the launch of that flight, and many of those individuals would have to confront Columbia’s foam strike and its possible impact on the launch of STS-114. Would the Columbia foam strike be classified as an In-Flight Anomaly? Would the fact that foam had detached from the bipod ramp on two out of the last three flights have made this problem a constraint to flight that would need to be solved before the next launch? Could the Program develop a solid rationale to fly STS-114, or would additional analysis be required to clear the flight for launch?

---

**Summary**

- Critical Path to U.S. Core Complete driven by Shuttle Launch
  - Program Station assessment: up to 14 days late
  - Program Shuttle assessment: up to 45 days late
- Program proactively managing schedule threats
- Most probable launch date is March 19-April 19
  - Program Target Remains 2/19/04

*Figure 6.2-6. By December 2002, every bit of padding in the schedule had disappeared. Another chart from the Shuttle and Station Program Managers’ briefing to the NASA Administrator summarizes the schedule dilemma.*
In fact, most of Linda Ham’s inquiries about the foam strike were not to determine what action to take during Columbia’s mission, but to understand the implications for STS-114. During a Mission Management Team meeting on January 21, she asked about the rationale put forward at the STS-113 Flight Readiness Review, which she had attended. Later that morning she reviewed the charts presented at that Flight Readiness Review. Her assessment, which she e-mailed to Shuttle Program Manager Ron Dittemore on January 21, was “Rationale was lousy then and still is …” (See Section 6.3 for the e-mail.)

One of Ham’s STS-114 duties was to chair a review to determine if the mission’s Orbiter, Atlantis, should be rolled from the Orbiter Processing Facility to the Vehicle Assembly Building, per its pre-launch schedule. In the above e-mail to Ron Dittemore, Ham indicates a desire to have the same individual responsible for the “lousy” STS-113 flight rationale start working the foam shedding issue – and presumably present a new flight rationale – very soon.

As STS-107 prepared for re-entry, Shuttle Program managers prepared for STS-114 flight rationale by arranging to have post-flight photographs taken of Columbia’s left wing rushed to Johnson Space Center for analysis.

As will become clear in the next section, most of the Shuttle Program’s concern about Columbia’s foam strike were not about the threat it might pose to the vehicle in orbit, but about the threat it might pose to the schedule.

Conclusion

The agency’s commitment to hold firm to a February 19, 2004, launch date for Node 2 influenced many of decisions in the months leading up to the launch of STS-107, and may well have subtly influenced the way managers handled the STS-112 foam strike and Columbia’s as well.

When a program agrees to spend less money or accelerate a schedule beyond what the engineers and program managers think is reasonable, a small amount of overall risk is added. These little pieces of risk add up until managers are no longer aware of the total program risk, and are, in fact, gambling. Little by little, NASA was accepting more and more risk in order to stay on schedule.

Findings

F6.2-1 NASA Headquarters’ focus was on the Node 2 launch date, February 19, 2004.
F6.2-2 The intertwined nature of the Space Shuttle and Space Station programs significantly increased the complexity of the schedule and made meeting the schedule far more challenging.
F6.2-3 The capabilities of the system were being stretched to the limit to support the schedule. Projections into 2003 showed stress on vehicle processing at the Kennedy Space Center, on flight controller training at Johnson Space Center, and on Space Station crew rotation schedules. Effects of this stress included neglecting flight controller recertification requirements, extending crew rotation schedules, and adding incremental risk by scheduling additional Orbiter movements at Kennedy.
F6.2-4 The four flights scheduled in the five months from October 2003, to February 2004, would have required a processing effort comparable to the effort immediately before the Challenger accident.
F6.2-5 There was no schedule margin to accommodate unforeseen problems. When flights come in rapid succession, there is no assurance that anomalies on one flight will be identified and appropriately addressed before the next flight.
F6.2-6 The environment of the countdown to Node 2 and the importance of maintaining the schedule may have begun to influence managers’ decisions, including those made about the STS-112 foam strike.
F6.2-7 During STS-107, Shuttle Program managers were concerned with the foam strike’s possible effect on the launch schedule.

Recommendation:

R6.2-1 Adopt and maintain a Shuttle flight schedule that is consistent with available resources. Although schedule deadlines are an important management tool, those deadlines must be regularly evaluated to ensure that any additional risk incurred to meet the schedule is recognized, understood, and acceptable.
In the Mission Evaluation Room, a safety representative from Science Applications International Corporation, NASA's contract safety company, made a log entry at the Safety and Quality Assurance console on January 28, at 12:15 p.m. It was only the second mention of the debris strike in the safety console log during the mission (the first was also minor).

“[MCC SAIC] called asking if any SR&QA people were involved in the decision to say that the ascent debris hit (left wing) is safe. [SAIC engineer] has indeed been involved in the analysis and stated that he concurs with the analysis. Details about the debris hit are found in the Flight Day 12 MER Manager and our Daily Report.” [MCC=Mission Control Center, SAIC=Science Applications International Corporation, SR&QA=Safety, Reliability, and Quality Assurance, MER=Mission Evaluation Room]

**Missed Opportunity 8**

According to a Memorandum for the Record written by William Readdy, Associate Administrator for Space Flight, Readdy and Michael Card, from NASA's Safety and Mission Assurance Office, discussed an offer of Department of Defense imagery support for Columbia. This January 29, conversation ended with Readdy telling Card that NASA would accept the offer but because the Mission Management Team had concluded that this was not a safety-of-flight issue, the imagery should be gathered only on a low priority “not-to-interfere” basis. Ultimately, no imagery was taken.

The Board notes that at the January 31, Mission Management Team meeting, there was only a minor mention of the debris strike. Other issues discussed included onboard crew consumables, the status of the leaking water separator, an intercom anomaly, SPACEHAB water flow rates, an update of the status of onboard experiments, end-of-mission weight concerns, landing day weather forecasts, and landing opportunities. The only mention of the debris strike was a brief comment by Bob Page, representing Kennedy Space Center’s Launch Integration Office, who stated that the crew’s hand-held cameras and External Tank films would be expedited to Marshall Space Flight Center via the Shuttle Training Aircraft for post-flight foam/debris imagery analysis, per Linda Ham’s request.

**Summary: Mission Management Decision Making**

**Discovery and Initial Analysis of Debris Strike**

In the course of examining film and video images of Columbia’s ascent, the Intercenter Photo Working Group identified, on the day after launch, a large debris strike to the leading edge of Columbia’s left wing. Alarmed at seeing so severe a hit so late in ascent, and at not having a clear view of damage the strike might have caused, Intercenter Photo Working Group members alerted senior Program managers by phone and sent a digitized clip of the strike to hundreds of NASA personnel via e-mail. These actions initiated a contingency plan that brought together an interdisciplinary group of experts from NASA, Boeing, and the United Space Alliance to analyze the strike. So concerned were Intercenter Photo Working Group personnel that on the day they discovered the debris strike, they tapped their Chair, Bob Page, to see through a request to image the left wing with Department of Defense assets in anticipation of analysts needing these images to better determine potential damage. By the Board’s count, this would be the first of three requests to secure imagery of Columbia on-orbit during the 16-day mission.

**Imagery Requests**

1. Flight Day 2. Bob Page, Chair, Intercenter Photo Working Group to Wayne Hale, Shuttle Program Manager for Launch Integration at Kennedy Space Center (in person).
2. Flight Day 6. Bob White, United Space Alliance manager, to Lambert Austin, head of the Space Shuttle Systems Integration at Johnson Space Center (by phone).
3. Flight Day 6. Rodney Rocha, Co-Chair of Debris Assessment Team to Paul Shack, Manager, Shuttle Engineering Office (by e-mail).
MISSED OPPORTUNITIES

1. Flight Day 4. Rodney Rocha inquires if crew has been asked to inspect for damage. No response.
2. Flight Day 6. Mission Control fails to ask crew member David Brown to downlink video he took of External Tank separation, which may have revealed missing bipod foam.
4. Flight Day 7. Wayne Hale phones Department of Defense representative, who begins identifying imaging assets, only to be stopped per Linda Ham’s orders.
7. Flight Day 8. Barbara Conte, after discussing imagery request with Rodney Rocha, calls LeRoy Cain, the STS-107 ascent/entry Flight Director. Cain checks with Phil Engelau, and then delivers a “no” answer.
8. Flight Day 14. Michael Card, from NASA’s Safety and Mission Assurance Office, discusses the imaging request with William Readdy, Associate Administrator for Space Flight. Readdy directs that imagery should only be gathered on a “not-to-interfere” basis. None was forthcoming.

Upon learning of the debris strike on Flight Day Two, the responsible system area manager from United Space Alliance and her NASA counterpart formed a team to analyze the debris strike in accordance with mission rules requiring the careful examination of any “out-of-family” event. Using film from the Intercenter Photo Working Group, Boeing systems integration analysts prepared a preliminary analysis that afternoon. (Initial estimates of debris size and speed, origin of debris, and point of impact would later prove remarkably accurate.)

As Flight Day Three and Four unfolded over the Martin Luther King Jr. holiday weekend, engineers began their analysis. One Boeing analyst used Crater, a mathematical prediction tool, to assess possible damage to the Thermal Protection System. Analysis predicted tile damage deeper than the actual tile depth, and penetration of the RCC coating at impact angles above 15 degrees. This suggested the potential for a burn-through during re-entry. Debris Assessment Team members judged that the actual damage would not be as severe as predicted because of the inherent conservatism in the Crater model and because, in the case of tile, Crater does not take into account the tile’s stronger and more impact-resistant “densified” layer, and in the case of RCC, the lower density of foam would preclude penetration at impact angles under 21 degrees.

On Flight Day Five, impact assessment results for tile and RCC were presented at an informal meeting of the Debris Assessment Team, which was operating without direct Shuttle Program or Mission Management leadership. Mission Control’s engineering support, the Mission Evaluation Room, provided no direction for team activities other than to request the team’s results by January 24. As the problem was being worked, Shuttle managers did not formally direct the actions of or consult with Debris Assessment Team leaders about the team’s assumptions, uncertainties, progress, or interim results, an unusual circumstance given that NASA managers are normally engaged in analyzing what they view as problems. At this meeting, participants agreed that an image of the area of the wing in question was essential to refine their analysis and reduce the uncertainties in their damage assessment.

Each member supported the idea to seek imagery from an outside source. Due in part to a lack of guidance from the Mission Management Team or Mission Evaluation Room managers, the Debris Assessment Team chose an unconventional route for its request. Rather than working the request up the normal chain of command – through the Mission Evaluation Room to the Mission Management Team for action to Mission Control – team members nominated Rodney Rocha, the team’s Co-Chair, to pursue the request through the Engineering Directorate at Johnson Space Center. As a result, even after the accident the Debris Assessment Team’s request was viewed by Shuttle Program managers as a non-critical engineering desire rather than a critical operational need.
When the team learned that the Mission Management Team was not pursuing on-orbit imaging, members were concerned. What Debris Assessment Team members did not realize was the negative response from the Program was not necessarily a direct and final response to their official request. Rather, the “no” was in part a response to requests for imagery initiated by the Intercenter Photo Working Group at Kennedy on Flight Day 2 in anticipation of analysts’ needs that had become by Flight Day 6 an actual engineering request by the Debris Assessment Team, made informally through Bob White to Lambert Austin, and formally through Rodney Rocha’s e-mail to Paul Shack. Even after learning that the Shuttle Program was not going to provide the team with imagery, some members sought information on how to obtain it anyway.

Debris Assessment Team members believed that imaging of potentially damaged areas was necessary even after the January 24, Mission Management Team meeting, where they had reported their results. Why they did not directly approach Shuttle Program managers and share their concern and uncertainty, and why Shuttle Program managers claimed to be isolated from engineers, are points that the Board labored to understand. Several reasons for this communications failure relate to NASA’s internal culture and the climate established by Shuttle Program management, which are discussed in more detail in Chapters 7 and 8.

A Flawed Analysis

An inexperienced team, using a mathematical tool that was not designed to assess an impact of this estimated size, performed the analysis of the potential effect of the debris impact. Crater was designed for “in-family” impact events and was intended for day-of-launch analysis of debris impacts. It was not intended for large projectiles like those observed on STS-107. Crater initially predicted possible damage, but the Debris Assessment Team assumed, without theoretical or experimental validation, that because Crater is a conservative tool – that is, it predicts more damage than will actually occur – the debris would stop at the tile’s densified layer, even though their experience did not involve debris strikes as large as STS-107’s. Crater-like equations were also used as part of the analysis to assess potential impact damage to the wing leading edge RCC. Again, the tool was used for something other than that for which it was designed; again, it predicted possible penetration; and again, the Debris Assessment Team used engineering arguments and their experience to discount the results.

As a result of a transition of responsibility for Crater analysis from the Boeing Huntington Beach facility to the Houston-based Boeing office, the team that conducted the Crater analyses had been formed fairly recently, and therefore could be considered less experienced when compared with the more senior Huntington Beach analysts. In fact, STS-107 was the first mission for which they were solely responsible for providing analysis with the Crater tool. Though post-accident interviews suggested that the training for the Houston Boeing analysts was of high quality and adequate in substance and duration, communications and theoretical understandings of the Crater model among the Houston-based team members had not yet developed to the standard of a more senior team. Due in part to contractual arrangements related to the transition, the Houston-based team did not take full advantage of the Huntington Beach engineers’ experience.

At the January 24, Mission Management Team meeting at which the “no safety-of-flight” conclusion was presented, there was little engineering discussion about the assumptions made, and how the results would differ if other assumptions were used.

Engineering solutions presented to management should have included a quantifiable range of uncertainty and risk analysis. Those types of tools were readily available, routinely used, and would have helped management understand the risk involved in the decision. Management, in turn, should have demanded such information. The very absence of a clear and open discussion of uncertainties and assumptions in the analysis presented should have caused management to probe further.

Shuttle Program Management’s Low Level of Concern

While the debris strike was well outside the activities covered by normal mission flight rules, Mission Management Team members and Shuttle Program managers did not treat the debris strike as an issue that required operational action by Mission Control. Program managers, from Ron Dittemore to individual Mission Management Team members, had, over the course of the Space Shuttle Program, gradually become inured to External Tank foam losses and on a funda-
mental level did not believe foam striking the vehicle posed a critical threat to the Orbiter. In particular, Shuttle managers exhibited a belief that RCC panels are impervious to foam impacts. Even after seeing the video of Columbia’s debris impact, learning estimates of the size and location of the strike, and noting that a foam strike with sufficient kinetic energy could cause Thermal Protection System damage, management’s level of concern did not change.

The opinions of Shuttle Program managers and debris and photo analysts on the potential severity of the debris strike diverged early in the mission and continued to diverge as the mission progressed, making it increasingly difficult for the Debris Assessment Team to have their concerns heard by those in a decision-making capacity. In the face of Mission managers’ low level of concern and desire to get on with the mission, Debris Assessment Team members had to prove unequivocally that a safety-of-flight issue existed before Shuttle Program management would move to obtain images of the left wing. The engineers found themselves in the unusual position of having to prove that the situation was unsafe – a reversal of the usual requirement to prove that a situation is safe.

Other factors contributed to Mission management’s ability to resist the Debris Assessment Team’s concerns. A tile expert told managers during frequent consultations that strike damage was only a maintenance-level concern and that on-orbit imaging of potential wing damage was not necessary. Mission management welcomed this opinion and sought no others. This constant reinforcement of managers’ pre-existing beliefs added another block to the wall between decision makers and concerned engineers.

Another factor that enabled Mission management’s detachment from the concerns of their own engineers is rooted in the culture of NASA itself. The Board observed an unofficial hierarchy among NASA programs and directorates that hindered the flow of communications. The effects of this unofficial hierarchy are seen in the attitude that members of the Debris Assessment Team held. Part of the reason they chose the institutional route for their imagery request was that without direction from the Mission Evaluation Room and Mission Management Team, they felt more comfortable with their own chain of command, which was outside the Shuttle Program. Further, when asked by investigators why they were not more vocal about their concerns, Debris Assessment Team members opined that by raising contrary points of view about Shuttle mission safety, they would be singled out for possible ridicule by their peers and managers.

A Lack of Clear Communication

Communication did not flow effectively up to or down from Program managers. As it became clear during the mission that managers were not as concerned as others about the danger of the foam strike, the ability of engineers to challenge those beliefs greatly diminished. Managers’ tendency to accept opinions that agree with their own dams the flow of effective communications.

After the accident, Program managers stated privately and publicly that if engineers had a safety concern, they were obligated to communicate their concerns to management. Managers did not seem to understand that as leaders they had a corresponding and perhaps greater obligation to create viable routes for the engineering community to express their views and receive information. This barrier to communications not only blocked the flow of information to managers, but it also prevented the downstream flow of information from managers to engineers, leaving Debris Assessment Team members no basis for understanding the reasoning behind Mission Management Team decisions.

The January 27 to January 31, phone and e-mail exchanges, primarily between NASA engineers at Langley and Johnson, illustrate another symptom of the “cultural fence” that impairs open communications between mission managers and working engineers. These exchanges and the reaction to them indicated that during the evaluation of a mission contingency, the Mission Management Team failed to disseminate information to all system and technology experts who could be consulted. Issues raised by two Langley and Johnson engineers led to the development of “what-if” landing scenarios of the potential outcome if the main landing gear door sustained damaged. This led to behind-the-scenes networking by these engineers to use NASA facilities to make simulation runs of a compromised landing configuration. These engineers – who understood their systems and related technology – saw the potential for a problem on landing and ran it down in case the unthinkable occurred. But their concerns never reached the managers on the Mission Management Team that had operational control over Columbia.
A Lack of Effective Leadership

The Shuttle Program, the Mission Management Team, and through it the Mission Evaluation Room, were not actively directing the efforts of the Debris Assessment Team. These management teams were not engaged in scenario selection or discussions of assumptions and did not actively seek status, inputs, or even preliminary results from the individuals charged with analyzing the debris strike. They did not investigate the value of imagery, did not intervene to consult the more experienced Crater analysts at Boeing’s Huntington Beach facility, did not probe the assumptions of the Debris Assessment Team’s analysis, and did not consider actions to mitigate the effects of the damage on re-entry. Managers’ claims that they didn’t hear the engineers’ concerns were due in part to their not asking or listening.

The Failure of Safety’s Role

As will be discussed in Chapter 7, safety personnel were present but passive and did not serve as a channel for the voicing of concerns or dissenting views. Safety representatives attended meetings of the Debris Assessment Team, Mission Evaluation Room, and Mission Management Team, but were merely party to the analysis process and conclusions instead of an independent source of questions and challenges. Safety contractors in the Mission Evaluation Room were only marginally aware of the debris strike analysis. One contractor did question the Debris Assessment Team safety representative about the analysis and was told that it was adequate. No additional inquiries were made. The highest-ranking safety representative at NASA headquarters deferred to Program managers when asked for an opinion on imaging of Columbia. The safety manager he spoke to also failed to follow up.

Summary

Management decisions made during Columbia’s final flight reflect missed opportunities, blocked or ineffective communications channels, flawed analysis, and ineffective leadership. Perhaps most striking is the fact that management – including Shuttle Program, Mission Management Team, Mission Evaluation Room, and Flight Director and Mission Control – displayed no interest in understanding a problem and its implications. Because managers failed to avail themselves of the wide range of expertise and opinion necessary to achieve the best answer to the debris strike question – “Was this a safety-of-flight concern?” – some Space Shuttle Program managers failed to fulfill the implicit contract to do whatever is possible to ensure the safety of the crew. In fact, their management techniques unknowingly imposed barriers that kept at bay both engineering concerns and dissenting views, and ultimately helped create “blind spots” that prevented them from seeing the danger the foam strike posed.

Because this chapter has focused on key personnel who participated in STS-107 bipod foam debris strike decisions, it is tempting to conclude that replacing them will solve all NASA’s problems. However, solving NASA’s problems is not quite so easily achieved. Peoples’ actions are influenced by the organizations in which they work, shaping their choices in directions that even they may not realize. The Board explores the organizational context of decision making more fully in Chapters 7 and 8.

Findings

Intercenter Photo Working Group

F6.3-1 The foam strike was first seen by the Intercenter Photo Working Group on the morning of Flight Day Two during the standard review of launch video and high-speed photography. The strike was larger than any seen in the past, and the group was concerned about possible damage to the Orbiter. No conclusive images of the strike existed. One camera that may have provided an additional view was out of focus because of an improperly maintained lens.

F6.3-2 The Chair of the Intercenter Photo Working Group asked management to begin the process of getting outside imagery to help in damage assessment. This request, the first of three, began its journey through the management hierarchy on Flight Day Two.

F6.3-3 The Intercenter Photo Working Group distributed its first report, including a digitized video clip and initial assessment of the strike, on Flight Day Two. This information
was widely disseminated to NASA and contractor engineers, Shuttle Program managers, and Mission Operations Directorate personnel.

F6.3-4 Initial estimates of debris size, speed, and origin were remarkably accurate. Initial information available to managers stated that the debris originated in the left bipod area of the External Tank, was quite large, had a high velocity, and struck the underside of the left wing near its leading edge. The report stated that the debris could have hit the RCC or tile.

**The Debris Assessment Team**

F6.3-5 A Debris Assessment Team began forming on Flight Day two to analyze the impact. Once the debris strike was categorized as “out of family” by United Space Alliance, contractual obligations led to the Team being Co-Chaired by the cognizant contractor sub-system manager and her NASA counterpart. The team was not designated a Tiger Team by the Mission Evaluation Room or Mission Management Team.

F6.3-6 Though the Team was clearly reporting its plans (and final results) through the Mission Evaluation Room to the Mission Management Team, no Mission manager appeared to “own” the Team’s actions. The Mission Management Team, through the Mission Evaluation Room, provided no direction for team activities, and Shuttle managers did not formally consult the Team’s leaders about their progress or interim results.

F6.3-7 During an organizational meeting, the Team discussed the uncertainty of the data and the value of on-orbit imagery to “bound” their analysis. In its first official meeting the next day, the Team gave its NASA Co-Chair the action to request imagery of Columbia on-orbit.

F6.3-8 The Team routed its request for imagery through Johnson Space Center’s Engineering Directorate rather than through the Mission Evaluation Room to the Mission Management Team to the Flight Dynamics Officer, the channel used during a mission. This routing diluted the urgency of their request. Managers viewed it as a non-critical engineering desire rather than a critical operational need.

F6.3-9 Team members never realized that management’s decision against seeking imagery was not intended as a direct or final response to their request.

F6.3-10 The Team’s assessment of possible tile damage was performed using an impact simulation that was well outside Crater’s test database. The Boeing analyst was inexperienced in the use of Crater and the interpretation of its results. Engineers with extensive Thermal Protection System expertise at Huntington Beach were not actively involved in determining if the Crater results were properly interpreted.

F6.3-11 Crater initially predicted tile damage deeper than the actual tile depth, but engineers used their judgment to conclude that damage would not penetrate the densified layer of tile. Similarly, RCC damage conclusions were based primarily on judgment and experience rather than analysis.

F6.3-12 For a variety of reasons, including management failures, communication breakdowns, inadequate imagery, inappropriate use of assessment tools, and flawed engineering judgments, the damage assessments contained substantial uncertainties.

F6.3-13 The assumptions (and their uncertainties) used in the analysis were never presented or discussed in full to either the Mission Evaluation Room or the Mission Management Team.

F6.3-14 While engineers and managers knew the foam could have struck RCC panels; the briefings on the analysis to the Mission Evaluation Room and Mission Management Team did not address RCC damage, and neither Mission Evaluation Room nor Mission Management Team managers asked about it.

**Space Shuttle Program Management**

F6.3-15 There were lapses in leadership and communication that made it difficult for engineers to raise concerns or understand decisions. Management failed to actively engage in the analysis of potential damage caused by the foam strike.

F6.3-16 Mission Management Team meetings occurred infrequently (five times during a 16 day mission), not every day, as specified in Shuttle Program management rules.

F6.3-17 Shuttle Program Managers entered the mission with the belief, recently reinforced by the STS-113 Flight Readiness Review, that a foam strike is not a safety-of-flight issue.
F6.3-18 After Program managers learned about the foam strike, their belief that it would not be a problem was confirmed (early, and without analysis) by a trusted expert who was readily accessible and spoke from “experience.” No one in management questioned this conclusion.

F6.3-19 Managers asked “Who’s requesting the photos?” instead of assessing the merits of the request. Management seemed more concerned about the staff following proper channels (even while they were themselves taking informal advice) than they were about the analysis.

F6.3-20 No one in the operational chain of command for STS-107 held a security clearance that would enable them to understand the capabilities and limitations of National imagery resources.

F6.3-21 Managers associated with STS-107 began investigating the implications of the foam strike on the launch schedule, and took steps to expedite post-flight analysis.

F6.3-22 Program managers required engineers to prove that the debris strike created a safety-of-flight issue: that is, engineers had to produce evidence that the system was unsafe rather than prove that it was safe.

F6.3-23 In both the Mission Evaluation Room and Mission Management Team meetings over the Debris Assessment Team’s results, the focus was on the bottom line – was there a safety-of-flight issue, or not? There was little discussion of analysis, assumptions, issues, or ramifications.

**Communication**

F6.3-24 Communication did not flow effectively up to or down from Program managers.

F6.3-25 Three independent requests for imagery were initiated.

F6.3-26 Much of Program managers’ information came through informal channels, which prevented relevant opinion and analysis from reaching decision makers.

F6.3-27 Program Managers did not actively communicate with the Debris Assessment Team. Partly as a result of this, the Team went through institutional, not mission-related, channels with its request for imagery, and confusion surrounded the origin of imagery requests and their subsequent denial.

F6.3-28 Communication was stifled by the Shuttle Program attempts to find out who had a “mandatory requirement” for imagery.

**Safety Representative’s Role**

F6.3-29 Safety representatives from the appropriate organizations attended meetings of the Debris Assessment Team, Mission Evaluation Room, and Mission Management Team, but were passive, and therefore were not a channel through which to voice concerns or dissenting views.

**Recommendation:**

R6.3-1 Implement an expanded training program in which the Mission Management Team faces potential crew and vehicle safety contingences beyond launch and ascent. These contingencies should involve potential loss of Shuttle or crew, contain numerous uncertainties and unknowns, and require the Mission Management Team to assemble and interact with support organizations across NASA/Contractor lines and in various locations.

R6.3-2 Modify the Memorandum of Agreement with the National Imagery and Mapping Agency (NIMA) to make the imaging of each Shuttle flight while on orbit a standard requirement.
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.

**Organizational Cause Statement**

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.

**Understanding Causes**

In the Board’s view, NASA’s organizational culture and structure had as much to do with this accident as the External Tank foam. Organizational culture refers to the values, norms, beliefs, and practices that govern how an institution functions. At the most basic level, organizational culture defines the assumptions that employees make as they carry out their work. It is a powerful force that can persist through reorganizations and the reassignment of key personnel.

Given that today’s risks in human space flight are as high and the safety margins as razor thin as they have ever been, there is little room for overconfidence. Yet the attitudes and decision-making of Shuttle Program managers and engineers during the events leading up to this accident were clearly overconfident and often bureaucratic in nature. They deferred to layered and cumbersome regulations rather than the fundamentals of safety. The Shuttle Program’s safety culture is straining to hold together the vestiges of a once robust systems safety program.

As the Board investigated the Columbia accident, it expected to find a vigorous safety organization, process, and culture at NASA, bearing little resemblance to what the Rogers Commission identified as the ineffective “silent safety” system in which budget cuts resulted in a lack of resources, personnel, independence, and authority. NASA’s initial briefings to the Board on its safety programs espoused a risk-averse philosophy that empowered any employee to stop an operation at the mere glimmer of a problem. Unfortunately, NASA’s views of its safety culture in those briefings did not reflect reality. Shuttle Program safety personnel failed to adequately assess anomalies and frequently accepted critical risks without qualitative or quantitative support, even when the tools to provide more comprehensive assessments were available.

Similarly, the Board expected to find NASA’s Safety and Mission Assurance organization deeply engaged at every
level of Shuttle management: the Flight Readiness Review, the Mission Management Team, the Debris Assessment Team, the Mission Evaluation Room, and so forth. This was not the case. In briefing after briefing, interview after interview, NASA remained in denial: in the agency’s eyes, “there were no safety-of-flight issues,” and no safety compromises in the long history of debris strikes on the Thermal Protection System. The silence of Program-level safety processes undermined oversight; when they did not speak up, safety personnel could not fulfill their stated mission to provide “checks and balances.” A pattern of acceptance prevailed throughout the organization that tolerated foam problems without sufficient engineering justification for doing so.

This chapter presents an organizational context for understanding the Columbia accident. Section 7.1 outlines a short history of safety at NASA, beginning in the pre-Apollo era when the agency reputedly had the finest system safety-engineering programs in the world. Section 7.2 discusses organizational theory and its importance to the Board’s investigation, and Section 7.3 examines the practices of three organizations that successfully manage high risk. Sections 7.4 and 7.5 look at NASA today and answer the question, “How could NASA have missed the foam signal?” by highlighting the blind spots that rendered the Shuttle Program’s risk perspective myopic. The Board’s conclusion and recommendations are presented in 7.6. (See Chapter 10 for a discussion of the differences between industrial safety and mission assurance/quality assurance.)

7.1 Organizational Causes: Insights from History

NASA’s organizational culture is rooted in history and tradition. From NASA’s inception in 1958 to the Challenger accident in 1986, the agency’s Safety, Reliability, and Quality Assurance (SRQA) activities, “although distinct disciplines,” were “typically treated as one function in the design, development, and operations of NASA’s manned space flight programs.” Contractors and NASA engineers collaborated closely to assure the safety of human space flight. Solid engineering practices emphasized defining goals and relating system performance to them; establishing and using decision criteria; developing alternatives; modeling systems for analysis; and managing operations. Although a NASA Office of Reliability and Quality Assurance existed for a short time during the early 1960s, it was funded by the human space flight program. By 1963, the office disappeared from the agency’s organization charts. For the next few years, the only type of safety program that existed at NASA was a decentralized “loose federation” of risk assessment oversight run by each program’s contractors and the project offices at each of the three Human Space Flight Centers.

Fallout from Apollo – 1967

In January 1967, months before the scheduled launch of Apollo 1, three astronauts died when a fire erupted in a ground-test capsule. In response, Congress, seeking to establish an independent safety organization to oversee space flight, created the Aerospace Safety Advisory Panel (ASAP). The ASAP was intended to be a senior advisory committee to NASA, reviewing space flight safety studies and operations plans, and evaluating “systems procedures and management policies that contribute to risk.” The panel’s main priority was human space flight missions. Although four of the panel’s nine members can be NASA employees, in recent years few have served as members. While the panel’s support staff generally consists of full-time NASA employees, the group technically remains an independent oversight body.

Congress simultaneously mandated that NASA create separate safety and reliability offices at the agency’s headquarters and at each of its Human Space Flight Centers and Programs. Overall safety oversight became the responsibility of NASA’s Chief Engineer. Although these offices were not totally independent – their funding was linked with the very programs they were supposed to oversee – their existence allowed NASA to treat safety as a unique function. Until the Challenger accident in 1986, NASA safety remained linked organizationally and financially to the agency’s Human Space Flight Program.

Challenger – 1986

In the aftermath of the Challenger accident, the Rogers Commission issued recommendations intended to remedy what it considered to be basic deficiencies in NASA’s safety system. These recommendations centered on an underlying theme: the lack of independent safety oversight at NASA. Without independence, the Commission believed, the slate of safety failures that contributed to the Challenger accident – such as the undue influence of schedule pressures and the flawed Flight Readiness process – would not be corrected. “NASA should establish an Office of Safety, Safety, and Quality Assurance to be headed by an Associate Administrator, reporting directly to the NASA Administrator,” concluded the Commission. “It would have direct authority for safety, reliability, and quality assurance throughout the Agency. The office should be assigned the workforce to ensure adequate oversight of its functions and should be independent of other NASA functional and program responsibilities” [emphasis added].

In July 1986, NASA Administrator James Fletcher created a Headquarters Office of Safety, Reliability, and Quality Assurance, which was given responsibility for all agency-wide safety-related policy functions. In the process, the position of Chief Engineer was abolished. The new office’s Associate Administrator promptly initiated studies on Shuttle in-flight anomalies, oil levels, the lack of spare parts, and landing and crew safety systems, among other issues. Yet NASA’s response to the Rogers Commission recommendation did not meet the Commission’s intent: the Associate Administrator did not have direct authority, and safety, reliability, and mission assurance activities across the agency remained dependent on other programs and Centers for funding.

General Accounting Office Review – 1990

A 1990 review by the U.S. General Accounting Office questioned the effectiveness of NASA’s new safety organi-
zations in a report titled “Space Program Safety: Funding for NASA’s Safety Organizations Should Be Centralized.” The report concluded “NASA did not have an independent and effective safety organization” [emphasis added]. Although the safety organizational structure may have “appeared adequate,” in the late 1980s the space agency had concentrated most of its efforts on creating an independent safety office at NASA Headquarters. In contrast, the safety offices at NASA’s field centers “were not entirely independent because they obtained most of their funds from activities whose safety-related performance they were responsible for overseeing.” The General Accounting Office worried that “the lack of centralized independent funding may also restrict the flexibility of center safety managers.” It also suggested “most NASA safety managers believe that centralized SRM&QA [Safety, Reliability, Maintainability and Quality Assurance] funding would ensure independence.” NASA did not institute centralized funding in response to the General Accounting Office report, nor has it since. The problems outlined in 1990 persist to this day.

**Space Flight Operations Contract – 1996**

The Space Flight Operations Contract was intended to streamline and modernize NASA’s cumbersome contracting practices, thereby freeing the agency to focus on research and development (see Chapter 5). Yet its implementation complicated issues of safety independence. A single contractor would, in principle, provide “oversight” on production, safety, and mission assurance, as well as cost management, while NASA maintained “insight” into safety and quality assurance through reviews and metrics. Indeed, the reduction to a single primary contract simplified some aspects of the NASA/contractor interface. However, as a result, experienced engineers changed jobs, NASA grew dependent on contractors for technical support, contract monitoring requirements increased, and positions were subsequently staffed by less experienced engineers who were placed in management roles.

Collectively, this eroded NASA’s in-house engineering and technical capabilities and increased the agency’s reliance on the United Space Alliance and its subcontractors to identify, track, and resolve problems. The contract also involved substantial transfers of safety responsibility from the government to the private sector; rollbacks of tens of thousands of Government Mandated Inspection Points; and vast reductions in NASA’s in-house safety-related technical expertise (see Chapter 10). In the aggregate, these mid-1990s transformations rendered NASA’s already problematic safety system simultaneously weaker and more complex.

The effects of transitioning Shuttle operations to the Space Flight Operations Contract were not immediately apparent in the years following implementation. In November 1996, as the contract was being implemented, the Aerospace Safety Advisory Panel published a comprehensive contract review, which concluded that the effort “to streamline the Space Shuttle program has not inadvertently created unacceptable flight or ground risks.” The Aerospace Safety Advisory Panel’s passing grades proved temporary.

**Shuttle Independent Assessment Team – 1999**

Just three years later, after a number of close calls, NASA chartered the Shuttle Independent Assessment Team to examine Shuttle sub-systems and maintenance practices (see Chapter 5). The Shuttle Independent Assessment Team Report sounded a stern warning about the quality of NASA’s Safety and Mission Assurance efforts and noted that the Space Shuttle Program had undergone a massive change in structure and was transitioning to “a slimmed down, contractor-run operation.”

The team produced several pointed conclusions: the Shuttle Program was inappropriately using previous success as a justification for accepting increased risk; the Shuttle Program’s ability to manage risk was being eroded “by the desire to reduce costs;” the size and complexity of the Shuttle Program and NASA/contractor relationships demanded better communication practices; NASA’s safety and mission assurance organization was not sufficiently independent; and “the workforce has received a conflicting message due to the emphasis on achieving cost and staff reductions, and the pressures placed on increasing scheduled flights as a result of the Space Station” [emphasis added]. The Shuttle Independent Assessment Team found failures of communication to flow up from the “shop floor” and down from supervisors to workers, deficiencies in problem and waiver-tracking systems, potential conflicts of interest between Program and contractor goals, and a general failure to communicate requirements and changes across organizations. In general, the Program’s organizational culture was deemed “too insular.”

NASA subsequently formed an Integrated Action Team to develop a plan to address the recommendations from previous Program-specific assessments, including the Shuttle Independent Assessment Team, and to formulate improvements. In part this effort was also a response to program missteps in the drive for efficiency seen in the “faster, better, cheaper” NASA of the 1990s. The NASA Integrated Action Team observed: “NASA should continue to remove communication barriers and foster an inclusive environment where open communication is the norm.” The intent was to establish an initiative where “the importance of communication and a culture of trust and openness permeate all facets of the organization.” The report indicated that “multiple processes to get the messages across the organizational structure” would need to be explored and fostered [emphasis added]. The report recommended that NASA solicit expert advice in identifying and removing barriers, providing tools, training, and education, and facilitating communication processes.

The Shuttle Independent Assessment Team and NASA Integrated Action Team findings mirror those presented by the Rogers Commission. The same communication problems persisted in the Space Shuttle Program at the time of the Columbia accident.

**Space Shuttle Competitive Source Task Force – 2002**

In 2002, a 14-member Space Shuttle Competitive Task Force supported by the RAND Corporation examined com-
petitive sourcing options for the Shuttle Program. In its final report to NASA, the team highlighted several safety-related concerns, which the Board shares:

- Flight and ground hardware and software are obsolete, and safety upgrades and aging infrastructure repairs have been deferred.
- Budget constraints have impacted personnel and resources required for maintenance and upgrades.
- International Space Station schedules exert significant pressures on the Shuttle Program.
- Certain mechanisms may impede worker anonymity in reporting safety concerns.
- NASA does not have a truly independent safety function with the authority to halt the progress of a critical mission element.  

Based on these findings, the task force suggested that an Independent Safety Assurance function should be created that would hold one of “three keys” in the Certification of Flight Readiness process (NASA and the operating contractor would hold the other two), effectively giving this function the ability to stop any launch. Although in the Board’s view the “third key” Certification of Flight Readiness process is not a perfect solution, independent safety and verification functions are vital to continued Shuttle operations. This independent function should possess the authority to shut down the flight preparation processes or intervene post-launch when an anomaly occurs.

7.2 ORGANIZATIONAL CAUSES: INSIGHTS FROM THEORY

To develop a thorough understanding of accident causes and risk, and to better interpret the chain of events that led to the Columbia accident, the Board turned to the contemporary social science literature on accidents and risk and sought insight from experts in High Reliability, Normal Accident, and Organizational Theory. Additionally, the Board held a forum, organized by the National Safety Council, to define the essential characteristics of a sound safety program.

High Reliability Theory argues that organizations operating high-risk technologies, if properly designed and managed, can compensate for inevitable human shortcomings, and therefore avoid mistakes that under other circumstances would lead to catastrophic failures. Normal Accident Theory, on the other hand, has a more pessimistic view of the ability of organizations and their members to manage high-risk technology. Normal Accident Theory holds that organizational and technological complexity contributes to failures. Organizations that aspire to failure-free performance are inevitably doomed to fail because of the inherent risks in the technology they operate. Normal Accident models also emphasize systems approaches and systems thinking, while the High Reliability model works from the bottom up; if each component is highly reliable, then the system will be highly reliable and safe.

Though neither High Reliability Theory nor Normal Accident Theory is entirely appropriate for understanding this accident, insights from each figured prominently in the Board’s deliberation. Fundamental to each theory is the importance of strong organizational culture and commitment to building successful safety strategies.

The Board selected certain well-known traits from these models to use as a yardstick to assess the Space Shuttle Program, and found them particularly useful in shaping its views on whether NASA’s current organization of its Human Space Flight Program is appropriate for the remaining years of Shuttle operation and beyond. Additionally, organizational theory, which encompasses organizational culture, structure, history, and hierarchy, is used to explain the Columbia accident, and, ultimately, combines with Chapters 5 and 6 to produce an expanded explanation of the accident’s causes.

The Board believes the following considerations are critical to understand what went wrong during STS-107. They will become the central motifs of the Board’s analysis later in this chapter.

- **Commitment to a Safety Culture:** NASA’s safety culture has become reactive, complacent, and dominated by unjustified optimism. Over time, slowly and unintentionally, independent checks and balances intended to increase safety have been eroded in favor of detailed processes that produce massive amounts of data and unwarranted consensus, but little effective communication. Organizations that successfully deal with high-risk technologies create and sustain a disciplined safety system capable of identifying, analyzing, and controlling hazards throughout a technology’s life cycle.

- **Ability to Operate in Both a Centralized and Decentralized Manner:** The ability to operate in a centralized manner when appropriate, and to operate in a decentralized manner when appropriate, is the hallmark of a high-reliability organization. On the operational side, the Space Shuttle Program has a highly centralized structure. Launch commit criteria and flight rules govern every imaginable contingency. The Mission Control Center and the Mission Management Team have very capable decentralized processes to solve problems that are not covered by such rules. The process is so highly regarded that it is considered one of the best problem-solving organizations of its type. In these situations, mature processes anchor rules, procedures, and routines to make the Shuttle Program’s matrixed workforce seamless, at least on the surface.

Nevertheless, it is evident that the position one occupies in this structure makes a difference. When supporting organizations try to “push back” against centralized Program direction – like the Debris Assessment Team did during STS-107 – independent analysis generated by a decentralized decision-making process can be stifled. The Debris Assessment Team, working in an essentially decentralized format, was well-led and had the right expertise to work the problem, but their charter was “fuzzy,” and the team had little direct connection to the Mission Management Team. This lack of connection to the Mission Management Team and the Mission Evaluation Room is the single most compelling reason why communications were so poor during the debris
assessment. In this case, the Shuttle Program was unable to simultaneously manage both the centralized and decentralized systems.

• **Importance of Communication:** At every juncture of STS-107, the Shuttle Program’s structure and processes, and therefore the managers in charge, resisted new information. Early in the mission, it became clear that the Program was not going to authorize imaging of the Orbiter because, in the Program’s opinion, images were not needed. Overwhelming evidence indicates that Program leaders decided the foam strike was merely a maintenance problem long before any analysis had begun. Every manager knew the party line: “we’ll wait for the analysis – no safety-of-flight issue expected.” Program leaders spent at least as much time making sure hierarchical rules and processes were followed as they did trying to establish why anyone would want a picture of the Orbiter. These attitudes are incompatible with an organization that deals with high-risk technology.

• **Avoiding Oversimplification:** The Columbia accident is an unfortunate illustration of how NASA’s strong cultural bias and its optimistic organizational thinking undermined effective decision-making. Over the course of 22 years, foam strikes were normalized to the point where they were simply a “maintenance” issue – a concern that did not threaten a mission’s success. This oversimplification of the threat posed by foam debris rendered the issue a low-level concern in the minds of Shuttle managers. Ascent risk, so evident in Challenger, biased leaders to focus on strong signals from the Shuttle System Main Engine and the Solid Rocket Boosters. Foam strikes, by comparison, were a weak and consequently overlooked signal, although they turned out to be no less dangerous.

• **Conditioned by Success:** Even after it was clear from the launch videos that foam had struck the Orbiter in a manner never before seen, Space Shuttle Program managers were not unduly alarmed. They could not imagine why anyone would want a photo of something that could be fixed after landing. More importantly, learned attitudes about foam strikes diminished management’s wariness of their danger. The Shuttle Program turned “the experience of failure into the memory of success.”18 Managers also failed to develop simple contingency plans for a re-entry emergency. They were convinced, without study, that nothing could be done about such an emergency. The intellectual curiosity and skepticism that a solid safety culture requires was almost entirely absent. Shuttle managers did not embrace safety-conscious attitudes. Instead, their attitudes were shaped and reinforced by an organization that, in this instance, was incapable of stepping back and gauging its biases. Bureaucracy and process trumped thoroughness and reason.

• **Significance of Redundancy:** The Human Space Flight Program has compromised the many redundant processes, checks, and balances that should identify and correct small errors. Redundant systems essential to every high-risk enterprise have fallen victim to bureaucratic efficiency. Years of workforce reductions and outsourcing have culled from NASA’s workforce the layers of experience and hands-on systems knowledge that once provided a capacity for safety oversight. Safety and Mission Assurance personnel have been eliminated, careers in safety have lost organizational prestige, and the Program now decides on its own how much safety and engineering oversight it needs. Aiming to align its inspection regime with the International Organization for Standardization 9000/9001 protocol, commonly used in industrial environments – environments very different than the Shuttle Program – the Human Space Flight Program shifted from a comprehensive “oversight” inspection process to a more limited “insight” process, cutting mandatory inspection points by more than half and leaving even fewer workers to make “second” or “third” Shuttle systems checks (see Chapter 10).

**Implications for the Shuttle Program Organization**

The Board’s investigation into the Columbia accident revealed two major causes with which NASA has to contend: one technical, the other organizational. As mentioned earlier, the Board studied the two dominant theories on complex organizations and accidents involving high-risk technologies. These schools of thought were influential in shaping the Board’s organizational recommendations, primarily because each takes a different approach to understanding accidents and risk.

The Board determined that high-reliability theory is extremely useful in describing the culture that should exist in the human space flight organization. NASA and the Space Shuttle Program must be committed to a strong safety culture, a view that serious accidents can be prevented, a willingness to learn from mistakes, from technology, and from others, and a realistic training program that empowers employees to know when to decentralize or centralize problem-solving. The Shuttle Program cannot afford the mindset that accidents are inevitable because it may lead to unnecessarily accepting known and preventable risks.

The Board believes normal accident theory has a key role in human spaceflight as well. Complex organizations need specific mechanisms to maintain their commitment to safety and assist their understanding of how complex interactions can make organizations accident-prone. Organizations cannot put blind faith into redundant warning systems because they inherently create more complexity, and this complexity in turn often produces unintended system interactions that can lead to failure. The Human Space Flight Program must realize that additional protective layers are not always the best choice. The Program must also remain sensitive to the fact that despite its best intentions, managers, engineers, safety professionals, and other employees, can, when confronted with extraordinary demands, act in counterproductive ways.

The challenges to failure-free performance highlighted by these two theoretical approaches will always be present in an organization that aims to send humans into space. What
can the Program do about these difficulties? The Board considered three alternatives. First, the Board could recommend that NASA follow traditional paths to improving safety by making changes to policy, procedures, and processes. These initiatives could improve organizational culture. The analysis provided by experts and the literature leads the Board to conclude that although reforming management practices has certain merits, it also has critical limitations. Second, the Board could recommend that the Shuttle is simply too risky and should be grounded. As will be discussed in Chapter 9, the Board is committed to continuing human space exploration, and believes the Shuttle Program can and should continue to operate. Finally, the Board could recommend a significant change to the organizational structure that controls the Space Shuttle Program’s technology. As will be discussed at length in this chapter’s conclusion, the Board believes this option has the best chance to successfully manage the complexities and risks of human space flight.

3. ORGANIZATIONAL CAUSES: EVALUATING BEST SAFETY PRACTICES

Many of the principles of solid safety practice identified as crucial by independent reviews of NASA and in accident and risk literature are exhibited by organizations that, like NASA, operate risky technologies with little or no margin for error. While the Board appreciates that organizations dealing with high-risk technology cannot sustain accident-free performance indefinitely, evidence suggests that there are effective ways to minimize risk and limit the number of accidents.

In this section, the Board compares NASA to three specific examples of independent safety programs that have strived for accident-free performance and have, by and large, achieved it: the U.S. Navy Submarine Flooding Prevention and Recovery (SUBSAFE), Naval Nuclear Propulsion (Naval Reactors) programs, and the Aerospace Corporation’s Launch Verification Process, which supports U.S. Air Force space launches.¹⁹ The safety cultures and organizational structure of all three make them highly adept in dealing with inordinately high risk by designing hardware and management systems that prevent seemingly inconsequential failures from leading to major accidents. Although size, complexity, and missions in these organizations and NASA differ, the following comparisons yield valuable lessons for the space agency to consider when re-designing its organization to increase safety.

Navy Submarine and Reactor Safety Programs

Human space flight and submarine programs share notable similarities. Spacecraft and submarines both operate in hazardous environments, use complex and dangerous systems, and perform missions of critical national significance. Both NASA and Navy operational experience include failures (for example, USS Thresher, USS Scorpion, Apollo 1 capsule fire, Challenger, and Columbia). Prior to the Columbia mishap, Administrator Sean O’Keefe initiated the NASA/Navy Benchmarking Exchange to compare and contrast the programs, specifically in safety and mission assurance.²⁰

The Navy SUBSAFE and Naval Reactor programs exercise a high degree of engineering discipline, emphasize total responsibility of individuals and organizations, and provide redundant and rapid means of communicating problems to decision-makers. The Navy’s nuclear safety program emerged with its first nuclear-powered warship (USS Nautilus), while non-nuclear SUBSAFE practices evolved from past flooding mishaps and philosophies first introduced by Naval Reactors. The Navy lost two nuclear-powered submarines in the 1960s – the USS Thresher in 1963 and the Scorpion 1968 – which resulted in a renewed effort to prevent accidents.²¹ The SUBSAFE program was initiated just two months after the Thresher mishap to identify critical changes to submarine certification requirements. Until a ship was independently recertified, its operating depth and maneuvers were limited. SUBSAFE proved its value as a means of verifying the readiness and safety of submarines, and continues to do so today.²²

The Naval Reactor Program is a joint Navy/Department of Energy organization responsible for all aspects of Navy nuclear propulsion, including research, design, construction, testing, training, operation, maintenance, and the disposition of the nuclear propulsion plants onboard many Naval ships and submarines, as well as their radioactive materials. Although the naval fleet is ultimately responsible for day-to-day operations and maintenance, those operations occur within parameters established by an entirely independent division of Naval Reactors.

The U.S. nuclear Navy has more than 5,500 reactor years of experience without a reactor accident. Put another way, nuclear-powered warships have steamed a cumulative total of over 127 million miles, which is roughly equivalent to over 265 lunar roundtrips. In contrast, the Space Shuttle Program has spent about three years on-orbit, although its spacecraft have traveled some 420 million miles.

Naval Reactor success depends on several key elements:

- Concise and timely communication of problems using redundant paths
- Insistence on airing minority opinions
- Formal written reports based on independent peer-reviewed recommendations from prime contractors
- Facing facts objectively and with attention to detail
- Ability to manage change and deal with obsolescence of classes of warships over their lifetime

These elements can be grouped into several thematic categories:

- Communication and Action: Formal and informal practices ensure that relevant personnel at all levels are informed of technical decisions and actions that affect their area of responsibility. Contractor technical recommendations and government actions are documented in peer-reviewed formal written correspondence. Unlike NASA, PowerPoint briefings and papers for technical seminars are not substitutes for completed staff work. In addition, contractors strive to provide recommendations

³⁸
based on a technical need, uninfluenced by headquarters or its representatives. Accordingly, division of responsibilities between the contractor and the Government remain clear, and a system of checks and balances is therefore inherent.

- **Recurring Training and Learning From Mistakes:** The Naval Reactor Program has yet to experience a reactor accident. This success is partially a testament to design, but also due to relentless and innovative training, grounded on lessons learned both inside and outside the program. For example, since 1996, Naval Reactors has educated more than 5,000 Naval Nuclear Propulsion Program personnel on the lessons learned from the *Challenger* accident. Senior NASA managers recently attended the 143rd presentation of the Naval Reactors seminar entitled “The Challenger Accident Re-examined.” The Board credits NASA’s interest in the Navy nuclear community, and encourages the agency to continue to learn from the mistakes of other organizations as well as from its own.

- **Encouraging Minority Opinions:** The Naval Reactor Program encourages minority opinions and “bad news.” Leaders continually emphasize that when no minority opinions are present, the responsibility for a thorough and critical examination falls to management. Alternate perspectives and critical questions are always encouraged. In practice, NASA does not appear to embrace these attitudes. Board interviews revealed that it is difficult for minority and dissenting opinions to percolate up through the agency’s hierarchy, despite processes like the anonymous NASA Safety Reporting System that supposedly encourages the airing of opinions.

- **Retaining Knowledge:** Naval Reactors uses many mechanisms to ensure knowledge is retained. The Director serves a minimum eight-year term, and the program documents the history of the rationale for every technical requirement. Key personnel in Headquarters routinely rotate into field positions to remain familiar with every aspect of operations, training, maintenance, development and the workforce. Current and past issues are discussed in open forum with the Director and immediate staff at “all-hands” informational meetings under an in-house professional development program. NASA lacks such a program.

- **Worst-Case Event Failures:** Naval Reactors hazard analyses evaluate potential damage to the reactor plant, potential impact on people, and potential environmental impact. The Board identified NASA’s failure to adequately prepare for a range of worst-case scenarios as a weakness in the agency’s safety and mission assurance training programs.

**SUBSAFE**

The Board observed the following during its study of the Navy’s SUBSAFE Program.

- **SUBSAFE requirements are clearly documented and achievable, with minimal “tailoring” or granting of waivers. NASA requirements are clearly documented but are also more easily waived.**

- **A separate compliance verification organization independently assesses program management. NASA’s Flight Preparation Process, which leads to Certification of Flight Readiness, is supposed to be an independent check-and-balance process. However, the Shuttle Program’s control of both engineering and safety compromises the independence of the Flight Preparation Process.**

- **The submarine Navy has a strong safety culture that emphasizes understanding and learning from past failures. NASA emphasizes safety as well, but training programs are not robust and methods of learning from past failures are informal.**

- **The Navy implements extensive safety training based on the *Thresher* and *Scorpion* accidents. NASA has not focused on any of its past accidents as a means of mentoring new engineers or those destined for management positions.**

- **The SUBSAFE structure is enhanced by the clarity, uniformity, and consistency of submarine safety requirements and responsibilities. Program managers are not permitted to “tailor” requirements without approval from the organization with final authority for technical requirements and the organization that verifies SUBSAFE’s compliance with critical design and process requirements.**

- **The SUBSAFE Program and implementing organization are relatively immune to budget pressures. NASA’s program structure requires the Program Manager position to consider such issues, which forces the manager to juggle cost, schedule, and safety considerations. Independent advice on these issues is therefore inevitably subject to political and administrative pressure.**

- **Compliance with critical SUBSAFE design and process requirements is independently verified by a highly capable centralized organization that also “owns” the processes and monitors the program for compliance.**

- **Quantitative safety assessments in the Navy submarine program are deterministic rather than probabilistic. NASA does not have a quantitative, program-wide risk and safety database to support future design capabilities and assist risk assessment teams.**

**Comparing Navy Programs with NASA**

Significant differences exist between NASA and Navy submarine programs.

- **Requirements Ownership (Technical Authority): Both the SUBSAFE and Naval Reactors’ organizational**
approach separates the technical and funding authority from program management in safety matters. The Board believes this separation of authority of program managers – who, by nature, must be sensitive to costs and schedules – and “owners” of technical requirements and waiver capabilities – who, by nature, are more sensitive to safety and technical rigor – is crucial. In the Naval Reactors Program, safety matters are the responsibility of the technical authority. They are not merely relegated to an independent safety organization with oversight responsibilities. This creates valuable checks and balances for safety matters in the Naval Reactors Program technical “requirements owner” community.

- **Emphasis on Lessons Learned:** Both Naval Reactors and the SUBSAFE have “institutionalized” their “lessons learned” approaches to ensure that knowledge gained from both good and bad experience is maintained in corporate memory. This has been accomplished by designating a central technical authority responsible for establishing and maintaining functional technical requirements as well as providing an organizational and institutional focus for capturing, documenting, and using operational lessons to improve future designs. NASA has an impressive history of scientific discovery, but can learn much from the application of lessons learned, especially those that relate to future vehicle design and training for contingencies. NASA has a broad Lessons Learned Information System that is strictly voluntary for program/project managers and management teams. Ideally, the Lessons Learned Information System should support overall program management and engineering functions and provide a historical experience base to aid conceptual developments and preliminary design.

**The Aerospace Corporation**

The Aerospace Corporation, created in 1960, operates as a Federally Funded Research and Development Center that supports the government in science and technology that is critical to national security. It is the equivalent of a $500 million enterprise that supports U.S. Air Force planning, development, and acquisition of space launch systems. The Aerospace Corporation employs approximately 3,200 people including 2,200 technical staff (29 percent Doctors of Philosophy, 41 percent Masters of Science) who conduct advanced planning, system design and integration, verify readiness, and provide technical oversight of contractors.

The Aerospace Corporation’s independent launch verification process offers another relevant benchmark for NASA’s safety and mission assurance program. Several aspects of the Aerospace Corporation launch verification process and independent mission assurance structure could be tailored to the Shuttle Program.

Aerospace’s primary product is a formal verification letter to the Air Force Systems Program Office stating a vehicle has been independently verified as ready for launch. The verification includes an independent General Systems Engineering and Integration review of launch preparations by Aerospace staff, a review of launch system design and payload integration, and a review of the adequacy of flight and ground hardware, software, and interfaces. This “concept-to-orbit” process begins in the design requirements phase, continues through the formal verification to countdown and launch, and concludes with a post-flight evaluation of events with findings for subsequent missions. Aerospace Corporation personnel cover the depth and breadth of space disciplines, and the organization has its own integrated engineering analysis, laboratory, and test matrix capability. This enables the Aerospace Corporation to rapidly transfer lessons learned and respond to program anomalies. Most importantly, Aerospace is uniquely independent and is not subject to any schedule or cost pressures.

The Aerospace Corporation and the Air Force have found the independent launch verification process extremely valuable. Aerospace Corporation involvement in Air Force launch verification has significantly reduced engineering errors, resulting in a 2.9 percent “probability-of-failure” rate for expendable launch vehicles, compared to 14.6 percent in the commercial sector.

**Conclusion**

The practices noted here suggest that responsibility and authority for decisions involving technical requirements and safety should rest with an independent technical authority. Organizations that successfully operate high-risk technologies have a major characteristic in common: they place a premium on safety and reliability by structuring their programs so that technical and safety engineering organizations own the process of determining, maintaining, and waiving technical requirements with a voice that is equal to yet independent of Program Managers, who are governed by cost, schedule and mission-accomplishment goals. The Naval Reactors Program, SUBSAFE program, and the Aerospace Corporation are examples of organizations that have invested in redundant technical authorities and processes to become highly reliable.

**7.4 ORGANIZATIONAL CAUSES: A BROKEN SAFETY CULTURE**

Perhaps the most perplexing question the Board faced during its seven-month investigation into the *Columbia* accident was “How could NASA have missed the signals the foam was sending?” Answering this question was a challenge. The investigation revealed that in most cases, the Human Space Flight Program is extremely aggressive in reducing threats to safety. But we also know – in hindsight – that detection of the dangers posed by foam was impeded by “blind spots” in NASA’s safety culture.

From the beginning, the Board witnessed a consistent lack of concern about the debris strike on *Columbia*. NASA managers told the Board “there was no safety-of-flight issue” and “we couldn’t have done anything about it anyway.” The investigation uncovered a troubling pattern in which Shuttle Program management made erroneous assumptions about the robustness of a system based on prior success rather than on dependable engineering data and rigorous testing.
The Shuttle Program’s complex structure erected barriers to effective communication and its safety culture no longer asks enough hard questions about risk. (Safety culture refers to an organization’s characteristics and attitudes – promoted by its leaders and internalized by its members – that serve to make safety the top priority.) In this context, the Board believes the mistakes that were made on STS-107 are not isolated failures, but are indicative of systemic flaws that existed prior to the accident. Had the Shuttle Program observed the principles discussed in the previous two sections, the threat that foam posed to the Orbiter, particularly after the STS-112 and STS-107 foam strikes, might have been more fully appreciated by Shuttle Program management.

In this section, the Board examines the NASA’s safety policy, structure, and process, communication barriers, the risk assessment systems that govern decision-making and risk management, and the Shuttle Program’s penchant for substituting analysis for testing.

NASA’s Safety: Policy, Structure, and Process

Safety Policy

NASA’s current philosophy for safety and mission assurance calls for centralized policy and oversight at Headquarters and decentralized execution of safety programs at the enterprise, program, and project levels. Headquarters dictates what must be done, not how it should be done. The operational premise that logically follows is that safety is the responsibility of program and project managers. Managers are subsequently given flexibility to organize safety efforts as they see fit, while NASA Headquarters is charged with maintaining oversight through independent surveillance and assessment. NASA policy dictates that safety programs should be placed high enough in the organization, and be vested with enough authority and seniority, to “maintain independence.” Signals of potential danger, anomalies, and critical information should, in principle, surface in the hazard identification process and be tracked with risk assessments supported by engineering analyses. In reality, such a process demands a more independent status than NASA has ever been willing to give its safety organizations, despite the recommendations of numerous outside experts over nearly two decades, including the Rogers Commission (1986), General Accounting Office (1990), and the Shuttle Independent Assessment Team (2000).

Safety Organization Structure

Center safety organizations that support the Shuttle Program are tailored to the missions they perform. Johnson and
Marshall Safety and Mission Assurance organizations are organized similarly. In contrast, Kennedy has decentralized its Safety and Mission Assurance components and assigned them to the Shuttle Processing Directorate. This management change renders Kennedy’s Safety and Mission Assurance structure even more dependent on the Shuttle Program, which reduces effective oversight.

At Johnson, safety programs are centralized under a Director who oversees five divisions and an Independent Assessment Office. Each division has clearly-defined roles and responsibilities, with the exception of the Space Shuttle Division Chief, whose job description does not reflect the full scope of authority and responsibility ostensibly vested in the position. Yet the Space Shuttle Division Chief is empowered to represent the Center, the Shuttle Program, and NASA Headquarters Safety and Mission Assurance at critical junctures in the safety process. The position therefore represents a critical node in NASA’s Safety and Mission Assurance architecture that seems to the Board to be plagued by conflict of interest. It is a single point of failure without any checks or balances.

Johnson also has a Shuttle Program Safety and Mission Assurance Manager who oversees United Space Alliance’s safety organization. The Shuttle Program further receives program safety support from the Center’s Safety, Reliability, and Quality Assurance Space Shuttle Division. Johnson’s Space Shuttle Division Chief has the additional role of Shuttle Program Safety, Reliability, and Quality Assurance Manager (see Figure 7.4-1). Over the years, this dual designation has resulted in a general acceptance of the fact that the Johnson Space Shuttle Division Chief performs duties on both the Center’s and Program’s behalf. The detached nature of the support provided by the Space Shuttle Division Chief, and the wide band of the position’s responsibilities throughout multiple layers of NASA’s hierarchy, confuses lines of authority, responsibility, and accountability in a manner that almost defies explanation.

A March 2001 NASA Office of Inspector General Audit Report on Space Shuttle Program Management Safety Observations made the same point:

The job descriptions and responsibilities of the Space Shuttle Program Manager and Chief, Johnson Safety Office Space Shuttle Division, are nearly identical with each official reporting to a different manager. This overlap in responsibilities conflicts with the SFOC [Space Flight Operations Contract] and NSTS 07700, which requires the Chief, Johnson Safety Office Space Shuttle Division, to provide matrixed personnel support to the Space Shuttle Program Safety Manager in fulfilling requirements applicable to the safety, reliability, and quality assurance aspects of the Space Shuttle Program.

The fact that Headquarters, Center, and Program functions are rolled-up into one position is an example of how a carefully designed oversight process has been circumvented and made susceptible to conflicts of interest. This organizational construct is unnecessarily bureaucratic and defeats NASA’s stated objective of providing an independent safety function. A similar argument can be made about the placement of quality assurance in the Shuttle Processing Divisions at Kennedy, which increases the risk that quality assurance personnel will become too “familiar” with programs they are charged to oversee, which hinders oversight and judgment.

The Board believes that although the Space Shuttle Program has effective safety practices at the “shop floor” level, its operational and systems safety program is flawed by its dependence on the Shuttle Program. Hindered by a cumbersome organizational structure, chronic understaffing, and poor management principles, the safety apparatus is not currently capable of fulfilling its mission. An independent safety structure would provide the Shuttle Program a more effective operational safety process. Crucial components of this structure include a comprehensive integration of safety across all the Shuttle programs and elements, and a more independent system of checks and balances.

Safety Process

In response to the Rogers Commission Report, NASA established what is now known as the Office of Safety and Mission Assurance at Headquarters to independently monitor safety and ensure communication and accountability agency-wide. The Office of Safety and Mission Assurance monitors unusual events like “out of family” anomalies and establishes agency-wide Safety and Mission Assurance policy. (An out-of-family event is an operation or performance outside the expected performance range for a given parameter or which has not previously been experienced.) The Office of Safety and Mission Assurance also screens the Shuttle Program’s Flight Readiness Process and signs the Certificate of Flight Readiness. The Shuttle Program Manager, in turn, is responsible for overall Shuttle safety and is supported by a one-person safety staff.

The Shuttle Program has been permitted to organize its safety program as it sees fit, which has resulted in a lack of standardized structure throughout NASA’s various Centers, enterprises, programs, and projects. The level of funding a program is granted impacts how much safety the Program can “buy” from a Center’s safety organization. In turn, Safety and Mission Assurance organizations struggle to anticipate program requirements and guarantee adequate support for the many programs for which they are responsible.

It is the Board’s view, shared by previous assessments, that the current safety system structure leaves the Office of Safety and Mission Assurance ill-equipped to hold a strong and central role in integrating safety functions. NASA Headquarters has not effectively integrated safety efforts across its culturally and technically distinct Centers. In addition, the practice of “buying” safety services establishes a relationship in which programs sustain the very livelihoods of the safety experts hired to oversee them. These idiosyncrasies of structure and funding preclude the safety organization from effectively providing independent safety analysis.

The commit-to-flight review process, as described in Chapters 2 and 6, consists of program reviews and readiness polls that are structured to allow NASA’s senior leaders to assess
mission readiness. In like fashion, safety organizations affiliated with various projects, programs, and Centers at NASA, conduct a Pre-launch Assessment Review of safety preparations and mission concerns. The Shuttle Program does not officially sanction the Pre-launch Assessment Review, which updates the Associate Administrator for Safety and Mission Assurance on safety concerns during the Flight Readiness Review/Certification of Flight Readiness process.

The Johnson Space Shuttle Safety, Reliability, and Quality Assurance Division Chief orchestrates this review on behalf of Headquarters. Note that this division chief also advises the Shuttle Program Manager of Safety. Because it lacks independent analytical rigor, the Pre-launch Assessment Review is only marginally effective. In this arrangement, the Johnson Shuttle Safety, Reliability, and Quality Assurance Division Chief is expected to render an independent assessment of his own activities. Therefore, the Board is concerned that the Pre-Launch Assessment Review is not an effective check and balance in the Flight Readiness Review.

Given that the entire Safety and Mission Assurance organization depends on the Shuttle Program for resources and simultaneously lacks the independent ability to conduct detailed analyses, cost and schedule pressures can easily and unintentionally influence safety deliberations. Structure and process places Shuttle safety programs in the unenviable position of having to choose between rubber-stamping engineering analyses, technical efforts, and Shuttle program decisions, or trying to carry the day during a committee meeting in which the other side almost always has more information and analytic capability.

**NASA Barriers to Communication: Integration, Information Systems, and Databases**

By their very nature, high-risk technologies are exceptionally difficult to manage. Complex and intricate, they consist of numerous interrelated parts. Standing alone, components may function adequately, and failure modes may be anticipated. Yet when components are integrated into a total system and work in concert, unanticipated interactions can occur that can lead to catastrophic outcomes. The risks inherent in these technical systems are heightened when they are produced and operated by complex organizations that can also break down in unanticipated ways. The Shuttle Program is such an organization. All of these factors make effective communication – between individuals and between programs – absolutely critical. However, the structure and complexity of the Shuttle Program hinders communication.

The Shuttle Program consists of government and contract personnel who cover an array of scientific and technical disciplines and are affiliated with various dispersed space, research, and test centers. NASA derives its organizational complexity from its origins as much as its widely varied missions. NASA Centers naturally evolved with different points of focus, a “divergence” that the Rogers Commission found evident in the propensity of Marshall personnel to resolve problems without including program managers outside their Center – especially managers at Johnson, to whom they officially reported (see Chapter 5).

Despite periodic attempts to emphasize safety, NASA’s frequent reorganizations in the drive to become more efficient reduced the budget for safety, sending employees conflicting messages and creating conditions more conducive to the development of a conventional bureaucracy than to the maintenance of a safety-conscious research-and-development organization. Over time, a pattern of ineffective communication has resulted, leaving risks improperly defined, problems unreported, and concerns unexpressed. The question is, why?

The transition to the Space Flight Operations Contract – and the effects it initiated – provides part of the answer. In the Space Flight Operations Contract, NASA encountered a completely new set of structural constraints that hindered effective communication. New organizational and contractual requirements demanded an even more complex system of shared management reviews, reporting relationships, safety oversight and insight, and program information development, dissemination, and tracking.

The Shuttle Independent Assessment Team’s report documented these changes, noting that “the size and complexity of the Shuttle system and of the NASA/contractor relationships place extreme importance on understanding, communication, and information handling.” Among other findings, the Shuttle Independent Assessment Team observed that:

- The current Shuttle program culture is too insular
- There is a potential for conflicts between contractual and programmatic goals
- There are deficiencies in problem and waiver-tracking systems
- The exchange of communication across the Shuttle program hierarchy is structurally limited, both upward and downward.

The Board believes that deficiencies in communication, including those spelled out by the Shuttle Independent Assessment Team, were a foundation for the *Columbia* accident. These deficiencies are byproducts of a cumbersome, bureaucratic, and highly complex Shuttle Program structure and the absence of authority in two key program areas that are responsible for integrating information across all programs and elements in the Shuttle program.

**Integration Structures**

NASA did not adequately prepare for the consequences of adding organizational structure and process complexity in the transition to the Space Flight Operations Contract. The agency’s lack of a centralized clearinghouse for integration and safety further hindered safe operations. In the Board’s opinion, the Shuttle Integration and Shuttle Safety, Reliability, and Quality Assurance Offices do not fully integrate information on behalf of the Shuttle Program. This is due, in part, to an irregular division of responsibilities between the Integration Office and the Orbiter Vehicle Engineering Office and the absence of a truly independent safety organization.

Within the Shuttle Program, the Orbiter Office handles many key integration tasks, even though the Integration Office ap-
ears to be the more logical office to conduct them; the Orbiter Office does not actively participate in the Integration Control Board; and Orbiter Office managers are actually ranked above their Integration Office counterparts. These uncoordinated roles result in conflicting and erroneous information, and support the perception that the Orbiter Office is isolated from the Integration Office and has its own priorities.

The Shuttle Program’s structure and process for Safety and Mission Assurance activities further confuse authority and responsibility by giving the Program’s Safety and Mission Assurance Manager technical oversight of the safety aspects of the Space Flight Operations Contract, while simultaneously making the Johnson Space Shuttle Division Chief responsible for advising the Program on safety performance. As a result, no one office or person in Program management is responsible for developing an integrated risk assessment above the sub-system level that would provide a comprehensive picture of total program risks. The net effect is that many Shuttle Program safety, quality, and mission assurance roles are never clearly defined.

Safety Information Systems

Numerous reviews and independent assessments have noted that NASA’s safety system does not effectively manage risk. In particular, these reviews have observed that the processes in which NASA tracks and attempts to mitigate the risks posed by components on its Critical Items List is flawed. The Post Challenger Evaluation of Space Shuttle Risk Assessment and Management Report (1988) concluded that:

“The committee views NASA critical items list (CIL) waiver decision-making process as being subjective, with little in the way of formal and consistent criteria for approval or rejection of waivers. Waiver decisions appear to be driven almost exclusively by the design based Failure Mode Effects Analysis (FMEA)/CIL retention rationale, rather than being based on an integrated assessment of all inputs to risk management. The retention rationales appear biased toward proving that the design is “safe,” sometimes ignoring significant evidence to the contrary.

The report continues, “… the Committee has not found an independent, detailed analysis or assessment of the CIL retention rationale which considers all inputs to the risk assessment process.”33 Ten years later, the Shuttle Independent Assessment Team reported “Risk Management process erosion created by the desire to reduce costs … “ 34 The Shuttle Independent Assessment Team argued strongly that NASA Safety and Mission Assurance should be restored to its previous role of an independent oversight body, and Safety and Mission Assurance not be simply a “safety auditor.”

The Board found similar problems with integrated hazard analyses of debris strikes on the Orbiter. In addition, the information systems supporting the Shuttle – intended to be tools for decision-making – are extremely cumbersome and difficult to use at any level.

The following addresses the hazard tracking tools and major databases in the Shuttle Program that promote risk management.

• Hazard Analysis: A fundamental element of system safety is managing and controlling hazards. NASA’s only guidance on hazard analysis is outlined in the Methodology for Conduct of Space Shuttle Program Hazard Analysis, which merely lists tools available.35 Therefore, it is not surprising that hazard analysis processes are applied inconsistently across systems, subsystems, assemblies, and components.

United Space Alliance, which is responsible for both Orbiter integration and Shuttle Safety Reliability and Quality Assurance, delegates hazard analysis to Boeing. However, as of 2001, the Shuttle Program no longer requires Boeing to conduct integrated hazard analyses. Instead, Boeing now performs hazard analysis only at the sub-system level. In other words, Boeing analyzes hazards to components and elements, but is not required to consider the Shuttle as a whole. Since the current Failure Mode Effects Analysis/Critical Item List process is designed for bottom-up analysis at the component level, it cannot effectively support the kind of “top-down” hazard analysis that is needed to inform managers on risk trends and identify potentially harmful interactions between systems.

The Critical Item List (CIL) tracks 5,396 individual Shuttle hazards, of which 4,222 are termed “Critical-
ity 1/1R.” Of those, 3,233 have waivers. CRIT 1/1R component failures are defined as those that will result in loss of the Orbiter and crew. Waivers are granted whenever a Critical Item List component cannot be redesigned or replaced. More than 36 percent of these waivers have not been reviewed in 10 years, a sign that NASA is not aggressively monitoring changes in system risk.

It is worth noting that the Shuttle’s Thermal Protection System is on the Critical Item List, and an existing hazard analysis and hazard report deals with debris strikes. As discussed in Chapter 6, Hazard Report #37 is ineffective as a decision aid, yet the Shuttle Program never challenged its validity at the pivotal STS-113 Flight Readiness Review.

Although the Shuttle Program has undoubtedly learned a great deal about the technological limitations inherent in Shuttle operations, it is equally clear that risk – as represented by the number of critical items list and waivers – has grown substantially without a vigorous effort to assess and reduce technical problems that increase risk. An information system bulging with over 5,000 critical items and 3,200 waivers is exceedingly difficult to manage.

- **Hazard Reports:** Hazard reports, written either by the Space Shuttle Program or a contractor, document conditions that threaten the safe operation of the Shuttle. Managers use these reports to evaluate risk and justify flight. During mission preparations, contractors and Centers review all baseline hazard reports to ensure they are current and technically correct.

Board investigators found that a large number of hazard reports contained subjective and qualitative judgments, such as “believed” and “based on experience from previous flights this hazard is an ‘Accepted Risk.’” A critical ingredient of a healthy safety program is the rigorous implementation of technical standards. These standards must include more than hazard analysis or low-level technical activities. Standards must integrate project engineering and management activities. Finally, a mechanism for feedback on the effectiveness of system safety engineering and management needs to be built into procedures to learn if safety engineering and management methods are weakening over time.

- **Lessons Learned Information System:** The Lessons Learned Information System database is a much simpler system to use, and it can assist with hazard identification and risk assessment. However, personnel familiar with the Lessons Learned Information System indicate that design engineers and mission assurance personnel use it only on an ad hoc basis, thereby limiting its utility. The Board is not the first to note such deficiencies. Numerous reports, including most recently a General Accounting Office 2001 report, highlighted fundamental weaknesses in the collection and sharing of lessons learned by program and project managers.

**Conclusions**

Throughout the course of this investigation, the Board found that the Shuttle Program’s complexity demands highly effective communication. Yet integrated hazard reports and risk analyses are rarely communicated effectively, nor are the many databases used by Shuttle Program engineers and managers capable of translating operational experiences into effective risk management practices. Although the Space Shuttle system has conducted a relatively small number of missions, there is more than enough data to generate performance trends. As it is currently structured, the Shuttle Program does not use data-driven safety methodologies to their fullest advantage.

**7.5 ORGANIZATIONAL CAUSES: IMPACT OF A FLAWED SAFETY CULTURE ON STS-107**

In this section, the Board examines how and why an array of processes, groups, and individuals in the Shuttle Program failed to appreciate the severity and implications of the foam strike on STS-107. The Board believes that the Shuttle Program should have been able to detect the foam trend and
more fully appreciate the danger it represented. Recall that “safety culture” refers to the collection of characteristics and attitudes in an organization – promoted by its leaders and internalized by its members – that makes safety an overriding priority. In the following analysis, the Board outlines shortcomings in the Space Shuttle Program, Debris Assessment Team, and Mission Management Team that resulted from a flawed safety culture.

Shuttle Program Shortcomings

The flight readiness process, which involves every organization affiliated with a Shuttle mission, missed the danger signals in the history of foam loss.

Generally, the higher information is transmitted in a hierarchy, the more it gets “rolled-up,” abbreviated, and simplified. Sometimes information gets lost altogether, as weak signals drop from memos, problem identification systems, and formal presentations. The same conclusions, repeated over time, can result in problems eventually being deemed non-problems. An extraordinary example of this phenomenon is how Shuttle Program managers assumed the foam strike on STS-112 was not a warning sign (see Chapter 6).

During the STS-113 Flight Readiness Review, the bipod foam strike to STS-112 was rationalized by simply restating earlier assessments of foam loss. The question of why bipod foam would detach and strike a Solid Rocket Booster spawned no further analysis or heightened curiosity; nor did anyone challenge the weakness of External Tank Project Manager’s argument that backed launching the next mission. After STS-113’s successful flight, once again the STS-112 foam event was not discussed at the STS-107 Flight Readiness Review. The failure to mention an outstanding technical anomaly, even if not technically a violation of NASA’s own procedures, desensitized the Shuttle Program to the dangers of foam striking the Thermal Protection System, and demonstrated just how easily the flight preparation process can be compromised. In short, the dangers of bipod foam got “rolled-up,” which resulted in a missed opportunity to make Shuttle managers aware that the Shuttle required, and did not yet have a fix for the problem.

Once the Columbia foam strike was discovered, the Mission Management Team Chairperson asked for the rationale the STS-113 Flight Readiness Review used to launch in spite of the STS-112 foam strike. In her e-mail, she admitted that the analysis used to conclude flying was, in a word, “lousy” (Chapter 6). This admission – that the rationale to fly was rubber-stamped – is, to say the least, unsettling.

The Flight Readiness process is supposed to be shielded from outside influence, and is viewed as both rigorous and systematic. Yet the Shuttle Program is inevitably influenced by external factors, including, in the case of the STS-107, schedule demands. Collectively, such factors shape how the Program establishes mission schedules and sets budget priorities, which affects safety oversight, workforce levels, facility maintenance, and contractor workloads. Ultimately, external expectations and pressures impact even data collection, trend analysis, information development, and the reporting and disposition of anomalies. These realities contradict NASA’s optimistic belief that pre-flight reviews provide true safeguards against unacceptable hazards. The schedule pressure to launch International Space Station Node 2 is a powerful example of this point (Section 6.2).

The premium placed on maintaining an operational schedule, combined with ever-decreasing resources, gradually led Shuttle managers and engineers to miss signals of potential danger. Foam strikes on the Orbiter’s Thermal Protection System, no matter what the size of the debris, were “normalized” and accepted as not being a “safety-of-flight risk.” Clearly, the risk of Thermal Protection damage due to such a strike needed to be better understood in quantifiable terms. External Tank foam loss should have been eliminated or mitigated with redundant layers of protection. If there was in fact a strong safety culture at NASA, safety experts would have had the authority to test the actual resilience of the leading edge Reinforced Carbon-Carbon panels, as the Board has done.

Debris Assessment Team Shortcomings

Chapter Six details the Debris Assessment Team’s efforts to obtain additional imagery of Columbia. When managers in the Shuttle Program denied the team’s request for imagery, the Debris Assessment Team was put in the untenable position of having to prove that a safety-of-flight issue existed without the very images that would permit such a determination. This is precisely the opposite of how an effective safety culture would act. Organizations that deal with high-risk operations must always have a healthy fear of failure – operations must be proved safe, rather than the other way around. NASA inverted this burden of proof.

Another crucial failure involves the Boeing engineers who conducted the Crater analysis. The Debris Assessment Team relied on the inputs of these engineers along with many others to assess the potential damage caused by the foam strike. Prior to STS-107, Crater analysis was the responsibility of a team at Boeing’s Huntington Beach facility in California, but this responsibility had recently been transferred to Boeing’s Houston office. In October 2002, the Shuttle Program completed a risk assessment that predicted the move of Boeing functions from Huntington Beach to Houston would increase risk to Shuttle missions through the end of 2003, because of the small number of experienced engineers who were willing to relocate. To mitigate this risk, NASA and United Space Alliance developed a transition plan to run through January 2003.

The Board has discovered that the implementation of the transition plan was incomplete and that training of replacement personnel was not uniform. STS-107 was the first mission during which Johnson-based Boeing engineers conducted analysis without guidance and oversight from engineers at Huntington Beach.

Even though STS-107’s debris strike was 400 times larger than the objects Crater is designed to model, neither Johnson engineers nor Program managers appealed for assistance from the more experienced Huntington Beach engineers,
The Debris Assessment Team presented its analysis in a formal briefing to the Mission Evaluation Room that relied on PowerPoint slides from Boeing. When engineering analyses and risk assessments are condensed to fit on a standard form or overhead slide, information is inevitably lost. In the process, the priority assigned to information can be easily misrepresented by its placement on a chart and the language that is used. Dr. Edward Tufte of Yale University, an expert in information presentation, who also researched communications failures in the Challenger accident, studied how the slides used by the Debris Assessment Team in their briefing to the Mission Evaluation Room misrepresented key information.38

The slide created six levels of hierarchy, signified by the title and the symbols to the left of each line. These levels prioritized information that was already contained in 11 simple sentences. Tufte also notes that the title is confusing. “Review of Test Data Indicates Conservatism” refers not to the predicted tile damage, but to the choice of test models used to predict the damage.

Only at the bottom of the slide do engineers state a key piece of information: that one estimate of the debris that struck Columbia was 640 times larger than the data used to calibrate the model on which engineers based their damage assessments. (Later analysis showed that the debris object was actually 400 times larger). This difference led Tufte to suggest that a more appropriate headline would be “Review of Test Data Indicates Irrelevance of Two Models.”39

Tufte also criticized the sloppy language on the slide. “The vaguely quantitative words ‘significant’ and ‘significantly’ are used 5 times on this slide,” he notes, “with de facto meanings ranging from ‘detectable in largely irrelevant calibration case study’ to ‘an amount of damage so that everyone dies’ to ‘a difference of 640-fold.’ ”40 Another example of sloppiness is that “cubic inches” is written inconsistently: “3cu. In,” “1920cu in,” and “3 cu in.” While such inconsistencies might seem minor, in highly technical fields like aerospace engineering a misrepresented decimal point or mistaken unit of measurement can easily engender inconsistencies and inaccuracies. In another phrase “Test results do show that it is possible at sufficient mass and velocity,” the word “it” actually refers to “damage to the protective tiles.”

As information gets passed up an organization hierarchy, from people who do analysis to mid-level managers to high-level leadership, key explanations and supporting information is filtered out. In this context, it is easy to understand how a senior manager might read this PowerPoint slide and not realize that it addresses a life-threatening situation.

At many points during its investigation, the Board was surprised to receive similar presentation slides from NASA officials in place of technical reports. The Board views the endemic use of PowerPoint briefing slides instead of technical papers as an illustration of the problematic methods of technical communication at NASA.

Review Of Test Data Indicates Conservatism for Tile Penetration

- The existing SOFI on tile test data used to create Crater was reviewed along with STS-107 Southwest Research data
  - Crater overpredicted penetration of tile coating significantly
    - Initial penetration to described by normal velocity
    - Varies with volume/mass of projectile(e.g., 200ft/sec for 3cu. In)
  - Significant energy is required for the softer SOFI particle to penetrate the relatively hard tile coating
    - Test results do show that insufficient mass and velocity
    - Convexly, once tile is penetrated SOFI can cause significant damage
      - Minor variations in total energy (above penetration level) can cause significant tile damage
  - Flight condition is significantly outside of test database
    - Volume of ramp is 1920cu in vs 3 cu in for test

The vaguely quantitative words “significant” and “significantly” are used 5 times on this slide, with de facto meanings ranging from ‘detectable in largely irrelevant calibration case study’ to “an amount of damage so that everyone dies’ to ‘a difference of 640-fold.’ ” None of these 5 usages appears to refer to the technical meaning of “statistical significance.”

The low resolution of PowerPoint slides promotes the use of compressed phrases like ‘Tile Penetration.’ As is the case here, such phrases may well be ambiguous. (The low resolution and large font generate 3 typographic orphans, lonely words dangling on a separate line.)

This vague pronoun reference “it” alludes to damage to the protective tiles, which caused the destruction of the Columbia. The slide weakens important material with ambiguous language (sentence fragments, passive voice, multiple meanings of “significant”). The 3 reports were created by engineers for high-level NASA officials who were deciding whether the threat of wing damage required further investigation before the Columbia attempted return. The officials were satisfied that the reports indicated that the Columbia was not in danger, and no attempts to further examine the threat were made. The slides were part of an oral presentation and also were circulated as e-mail attachments.

In this slide the same unit of measure for volume (cubic inches) is shown a different way every time

3cu. in 1920cu, in 3 cu in

rather than in clear and tidy exponential form 1920 in 3. Perhaps the available font cannot show exponents. Shakiness in units of measurement provokes concern. Slides that use hierarchical bullet-outlines here do not handle statistical data and scientific notation gracefully. If PowerPoint is a corporate-mandated format for all engineering reports, then some competent scientific typography (rather than the PP market-pitch style) is essential. In this slide, the typography is so choppy and clunky that it impedes understanding.

The analysis by Dr. Edward Tufte of the slide from the Debris Assessment Team briefing. [SOFI=Spray-On Foam Insulation]
who might have cautioned against using Crater so far outsidethe validated limits. Nor did safety personnelprovide any additional oversight. NASA failed to connect the dots:the engineers who misinterpreted Crater – a tool alreadyunsuited to the task at hand – were the very ones the ShuttleProgram identified as engendering the most risk in theirtransition from Huntington Beach. The Board views this exampleas characteristic of the greater turbulence the Shuttle Programexperienced in the decade before Columbia as aresult of workforce reductions and management reforms.

Mission Management Team Shortcomings

In the Board’s view, the decision to fly STS-113 without a compelling explanation for why bipod foam had separated on ascent during the preceding mission, combined with the low number of Mission Management Team meetings during STS-107, indicates that the Shuttle Program had become overconfident. Over time, the organization determined it did not need daily meetings during a mission, despite regulations that state otherwise.

Status update meetings should provide an opportunity to raisconcerns and hold discussions across structural and technical boundaries. The leader of such meetings must encourage participation and guarantee that problems are assessed and resolved fully. All voices must be heard, which can be difficult when facing a hierarchy. An employee’s location in the hierarchy can encourage silence. Organizations interested in safety must take steps to guarantee that all relevant information is presented to decision-makers. This did not happen in the meetings during the Columbia mission (see Chapter 6). For instance, e-mails from engineers at Johnson and Langley conveyed the depth of their concern about the foam strike, the questions they had about its implications, and the actions they wanted to take as a follow-up. However, these e-mails did not reach the Mission Management Team.

The failure to convey the urgency of engineering concerns was caused, at least in part, by organizational structure and spheres of authority. The Langley e-mails were circulated among co-workers at Johnson who explored the possible effects of the foam strike and its consequences for landing. Yet, like Debris Assessment Team Co-Chair Rodney Rocha, they kept their concerns within local channels and did not forward them to the Mission Management Team. They were separated from the decision-making process by distance and rank.

Similarly, Mission Management Team participants felt pressured to remain quiet unless discussion turned to their particular area of technological or system expertise, and, even then, to be brief. The initial damage assessment briefing prepared for the Mission Evaluation Room was cut down considerably in order to make it “fit” the schedule. Even so, it took 40 minutes. It was cut down further to a three-minute discussion topic at the Mission Management Team. Tapes of STS-107 Mission Management Team sessions reveal a noticeable “rush” by the meeting’s leader to the preconceived bottom line that there was “no safety-of-flight” issue (see Chapter 6). Program managers created huge barriers against dissenting opinions by stating preconceived conclusions based on subjective knowledge and experience, rather than on solid data. Managers demonstrated little concern for mission safety.

Organizations with strong safety cultures generally acknowledge that a leader’s best response to unanimous consent is to play devil’s advocate and encourage an exhaustive debate. Mission Management Team leaders failed to seek out such minority opinions. Imagine the difference if any Shuttle manager had simply asked, “Prove to me that Columbia has not been harmed.”

Similarly, organizations committed to effective communication seek avenues through which unidentified concerns and dissenting insights can be raised, so that weak signals are not lost in background noise. Common methods of bringing minority opinions to the fore include hazard reports, suggestion programs, and empowering employees to call “time out” (Chapter 10). For these methods to be effective, they must mitigate the fear of retribution, and management and technical staff must pay attention. Shuttle Program hazard reporting is seldom used, safety time outs are at times disregarded, and informal efforts to gain support are squelched. The very fact that engineers felt inclined to conduct simulated blown tire landings at Ames “after hours,” indicates their reluctance to bring the concern up in established channels.

Safety Shortcomings

The Board believes that the safety organization, due to a lack of capability and resources independent of the Shuttle Program, was not an effective voice in discussing technical issues or mission operations pertaining to STS-107. The safety personnel present in the Debris Assessment Team, Mission Evaluation Room, and on the Mission Management Team were largely silent during the events leading up to the loss of Columbia. That silence was not merely a failure of safety, but a failure of the entire organization.

7.6 Findings and Recommendations

The evidence that supports the organizational causes also led the Board to conclude that NASA’s current organization, which combines in the Shuttle Program all authority and responsibility for schedule, cost, manifest, safety, technical requirements, and waivers to technical requirements, is not an effective check and balance to achieve safety and mission assurance. Further, NASA’s Office of Safety and Mission Assurance does not have the independence and authority that the Board and many outside reviews believe is necessary. Consequently, the Space Shuttle Program does not consistently demonstrate the characteristics of organizations that effectively manage high risk. Therefore, the Board offers the following Findings and Recommendations:

Findings:

F7.1-1 Throughout its history, NASA has consistently struggled to achieve viable safety programs and adjust them to the constraints and vagaries of changing budgets. Yet, according to multiple high level independent reviews, NASA’s safety system has fallen short of the mark.
The Associate Administrator for Safety and Mission Assurance is not responsible for safety and mission assurance execution, as intended by the Rogers Commission, but is responsible for Safety and Mission Assurance policy, advice, coordination, and budgets. This view is consistent with NASA's recent philosophy of management at a strategic level at NASA Headquarters but contrary to the Rogers' Commission recommendation.

Safety and Mission Assurance organizations supporting the Shuttle Program are largely dependent upon the Program for funding, which hampers their status as independent advisors.

Over the last two decades, little to no progress has been made toward attaining integrated, independent, and detailed analyses of risk to the Space Shuttle system.

System safety engineering and management is separated from mainstream engineering, is not vigorous enough to have an impact on system design, and is hidden in the other safety disciplines at NASA Headquarters.

Risk information and data from hazard analyses are not communicated effectively to the risk assessment and mission assurance processes. The Board could not find adequate application of a process, database, or metric analysis tool that took an integrated, systemic view of the entire Space Shuttle system.

The Space Shuttle Systems Integration Office handles all Shuttle systems except the Orbiter. Therefore, it is not a true integration office.

When the Integration Office convenes the Integration Control Board, the Orbiter Office usually does not send a representative, and its staff makes verbal inputs only when requested.

The Integration office did not have continuous responsibility to integrate responses to bipod foam shedding from various offices. Sometimes the Orbiter Office had responsibility, sometimes the External Tank Office at Marshall Space Flight Center had responsibility, and sometime the bipod shedding did not result in any designation of an In-Flight Anomaly. Integration did not occur.

NASA information databases such as The Problem Reporting and Corrective Action and the Web Program Compliance Assurance and Status System are marginally effective decision tools.

Senior Safety, Reliability & Quality Assurance and element managers do not use the Lessons Learned Information System when making decisions. NASA subsequently does not have a constructive program to use past lessons to educate engineers, managers, astronauts, or safety personnel.

The Space Shuttle Program has a wealth of data tucked away in multiple databases without a convenient way to integrate and use the data for management, engineering, or safety decisions.

The dependence of Safety, Reliability & Quality Assurance personnel on Shuttle Program support limits their ability to oversee operations and communicate potential problems throughout the organization.

There are conflicting roles, responsibilities, and guidance in the Space Shuttle safety programs. The Safety & Mission Assurance Pre-Launch Assessment Review process is not recognized by the Space Shuttle Program as a requirement that must be followed (NSTS 22778). Failure to consistently apply the Pre-Launch Assessment Review as a requirements document creates confusion about roles and responsibilities in the NASA safety organization.

Recommendations:

Establish an independent Technical Engineering Authority that is responsible for technical requirements and all waivers to them, and will build a disciplined, systematic approach to identifying, analyzing, and controlling hazards throughout the life cycle of the Shuttle System.

The independent technical authority does the following as a minimum:

- Develop and maintain technical standards for all Space Shuttle Program projects and elements
- Be the sole waiver-granting authority for all technical standards
- Conduct trend and risk analysis at the subsystem, system, and enterprise levels
- Own the failure mode, effects analysis and hazard reporting systems
- Conduct integrated hazard analysis
- Decide what is and is not an anomalous event
- Independently verify launch readiness
- Approve the provisions of the recertification program called for in Recommendation R9.1-1

The Technical Engineering Authority should be funded directly from NASA Headquarters, and should have no connection to or responsibility for schedule or program cost.

NASA Headquarters Office of Safety and Mission Assurance should have direct line authority over the entire Space Shuttle Program safety organization and should be independently resourced.

Reorganize the Space Shuttle Integration Office to make it capable of integrating all elements of the Space Shuttle Program, including the Orbiter.
ENDNOTES FOR CHAPTER 7

The citations that contain a reference to “CAIB document” with CAB or CTF followed by seven to eleven digits, such as CABD001-0010, refer to a document in the Columbia Accident Investigation Board database maintained by the Department of Justice and archived at the National Archives.


8 The quotes are from the Executive Summary of National Aeronautics and Space Administration Space Shuttle Independent Assessment Team, “Report to Associate Administrator, Office of Space Flight,” October-December 1999. CAIB document CTF017-0169.

9 Harry McDonald, “SIAT Space Shuttle Independent Assessment Team Report.”


12 Dr. Karl Weick, University of Michigan; Dr. Karlene Roberts, University of California-Berkley; Dr. Howard McCurdy, American University; and Dr. Diane Vaughn, Boston College.

13 Dr. David Woods, Ohio State University; Dr. Nancy G. Leveson, Massachusetts Institute of Technology; Mr. James Wick, Intel Corporation; Ms. Deborah L. Grubbe, DuPont Corporation; Dr. M. Sam Mannan, Texas A&M University; Douglas A. Wiegmann, University of Illinois at Urbana-Champaign; and Mr. Alan C. McMillan, President and Chief Executive Officer, National Safety Council.


15 Dr. Diane Vaughn, Boston College; Dr. David Woods, Ohio State University; Dr. Howard E. McCurdy, American University; Dr. Karl E. Weick, University of Michigan; Dr. Karlene H. Roberts; Dr. M. Elisabeth Paté-Cornell; Dr. Douglas A. Wiegmann, University of Illinois at Urbana-Champaign; Dr. Nancy G. Leveson, Massachusetts Institute of Technology; Mr. James Wick, Intel Corporation; Ms. Deborah L. Grubbe, DuPont Corporation; Dr. M. Sam Mannan, Texas A&M University; and Mr. Alan C. McMillan, President and Chief Executive Officer, National Safety Council.

16 Dr. David Woods of Ohio State University speaking to the Board on Hind-Sight Bias. April 28, 2003.


18 LaPorte and Consolini, “Working In Practice.”


21 Rockwell, Rickover, p. 320.

22 For more information, see Dr. Diane Vaught, The Challenger Launch Decision, Risky Technology, Culture, and Deviance at NASA (Chicago: University of Chicago Press, 1996).

23 Presentation to the Board by Admiral Walter Cantrell, Aerospace Advisory Panel member, April 7, 2003.

24 Presentation to the Board by Admiral Walter Cantrell, Aerospace Advisory Panel member, April 7, 2003.


27 NASA Policy Directive 8700.1A, “NASA Policy for Safety and Mission Success”, Para 1.b, 5.b(1), 5.e(1), and 5.f(1).


30 Harry McDonald, “SIAT Space Shuttle Independent Assessment Team Report.”

31 Ibid.


33 Harry McDonald, “SIAT Space Shuttle Independent Assessment Team Report.”

34 NSTS-2254 Rev B.

35 Ibid.

36 Ibid.


40 Ibid.
The Board began its investigation with two central questions about NASA decisions. Why did NASA continue to fly with known foam debris problems in the years preceding the Columbia launch, and why did NASA managers conclude that the foam debris strike 81.9 seconds into Columbia’s flight was not a threat to the safety of the mission, despite the concerns of their engineers?

### 8.1 Echoes of Challenger

As the investigation progressed, Board member Dr. Sally Ride, who also served on the Rogers Commission, observed that there were “echoes” of Challenger in Columbia. Ironically, the Rogers Commission investigation into Challenger started with two remarkably similar central questions: Why did NASA continue to fly with known O-ring erosion problems in the years before the Challenger launch, and why, on the eve of the Challenger launch, did NASA managers decide that launching the mission in such cold temperatures was an acceptable risk, despite the concerns of their engineers?

The echoes did not stop there. The foam debris hit was not the single cause of the Columbia accident, just as the failure of the joint seal that permitted O-ring erosion was not the single cause of Challenger. Both Columbia and Challenger were lost also because of the failure of NASA’s organizational system. Part Two of this report cites failures of the three parts of NASA’s organizational system. This chapter shows how previous political, budgetary, and policy decisions by leaders at the White House, Congress, and NASA (Chapter 5) impacted the Space Shuttle Program’s structure, culture, and safety system (Chapter 7), and how these in turn resulted in flawed decision-making (Chapter 6) for both accidents. The explanation is about system effects: how actions taken in one layer of NASA’s organizational system impact other layers. History is not just a backdrop or a scene-setter. History is cause. History set the Columbia and Challenger accidents in motion. Although Part Two is separated into chapters and sections to make clear what happened in the political environment, the organization, and managers’ and engineers’ decision-making, the three worked together. Each is a critical link in the causal chain.

This chapter shows that both accidents were “failures of foresight” in which history played a prominent role. 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. The final section compares the two critical decision sequences immediately before the loss of both Orbiters – the pre-launch teleconference for Challenger and the post-launch foam strike discussions for Columbia. It shows history again at work: how past definitions of risk combined with systemic problems in the NASA organization caused both accidents.

Connecting the parts of NASA’s organizational system and drawing the parallels with Challenger demonstrate three things. First, despite all the post-Challenger changes at NASA and the agency’s notable achievements since, the causes of the institutional failure responsible for Challenger have not been fixed. Second, the Board strongly believes that if these persistent, systemic flaws are not resolved, the scene is set for another accident. Therefore, the recommendations for change are not only for fixing the Shuttle’s technical system, but also for fixing each part of the organizational system that produced Columbia’s failure. Third, the Board’s focus on the context in which decision making occurred does not mean that individuals are not responsible and accountable. To the contrary, individuals always must assume responsibility for their actions. What it does mean is that NASA’s problems cannot be solved simply by retirements, resignations, or transferring personnel.

The constraints under which the agency has operated throughout the Shuttle Program have contributed to both
Shuttle accidents. Although NASA leaders have played an important role, these constraints were not entirely of NASA's own making. The White House and Congress must recognize the role of their decisions in this accident and take responsibility for safety in the future.

8.2 Failures of Foresight: Two Decision Histories and the Normalization of Deviance

Foam loss may have occurred on all missions, and left bipod ramp foam loss occurred on 10 percent of the flights for which visible evidence exists. The Board had a hard time understanding how, after the bitter lessons of Challenger, NASA could have failed to identify a similar trend. Rather than view the foam decision only in hindsight, the Board tried to see the foam incidents as NASA engineers and managers saw them as they made their decisions. This section gives an insider perspective: how NASA defined risk and how those definitions changed over time for both foam debris hits and O-ring erosion. In both cases, engineers and managers conducting risk assessments continually normalized the technical deviations they found. In all official engineering analyses and launch recommendations prior to the accidents, evidence that the design was not performing as expected was reinterpreted as acceptable and non-deviant, which diminished perceptions of risk throughout the agency.

The initial Shuttle design predicted neither foam debris problems nor poor sealing action of the Solid Rocket Booster joints. To experience either on a mission was a violation of design specifications. These anomalies were signals of potential danger, not something to be tolerated, but in both cases after the first incident the engineering analysis concluded that the design could tolerate the damage. These engineers decided to implement a temporary fix and/or accept the risk, and fly. For both O-rings and foam, that first decision was a turning point. It established a precedent for accepting, rather than eliminating, these technical deviations. As a result of this new classification, subsequent incidents of O-ring erosion or foam debris strikes were not defined as signals of danger, but as evidence that the design was now acting as predicted. Engineers and managers incorporated worsening anomalies into the engineering experience base, which functioned as an elastic waistband, expanding to hold larger deviations from the original design. Anomalies that did not lead to catastrophic failure were treated as a source of valid engineering data that justified further flights. These anomalies were translated into a safety margin that was extremely influential, allowing engineers and managers to add incrementally to the amount and seriousness of damage that was acceptable. Both O-ring erosion and foam debris events were repeatedly “addressed” in NASA's Flight Readiness Reviews but never fully resolved. In both cases, the engineering analysis was incomplete and inadequate. Engineers understood what was happening, but they never understood why. NASA continued to implement a series of small corrective actions, living with the problems until it was too late.

NASA documents show how official classifications of risk were downgraded over time. Program managers designated both the foam problems and O-ring erosion as “acceptable risks” in Flight Readiness Reviews. NASA managers also assigned each bipod foam event In-Flight Anomaly status, and then removed the designation as corrective actions were implemented. But when major bipod foam-shedding occurred on STS-112 in October 2002, Program management did not assign an In-Flight Anomaly. Instead, it downgraded the problem to the lower status of an “action” item. Before Challenger, the problematic Solid Rocket Booster joint had been elevated to a Criticality 1 item on NASA's Critical Items List, which ranked Shuttle components by failure consequences and noted why each was an acceptable risk. The joint was later demoted to a Criticality 1-R (redundant), and then in the month before Challenger's launch was “closed out” of the problem-reporting system. Prior to both accidents, this demotion from high-risk item to low-risk item was very similar, but with some important differences. Damaging the Orbiter's Thermal Protection System, especially its fragile tiles, was normalized even before Shuttle launches began: it was expected due to forces at launch, orbit, and re-entry. So normal was replacement of Thermal Protection System materials that NASA managers budgeted for tile cost and turnaround maintenance time from the start.

It was a small and logical next step for the discovery of foam debris damage to the tiles to be viewed by NASA as part of an already existing maintenance problem, an assessment based on experience, not on a thorough hazard analysis. Foam debris anomalies came to be categorized by the reassuring term “in-family,” a formal classification indicating that new occurrences of an anomaly were within the engineering experience base. “In-family” was a strange term indeed for a violation of system requirements. Although “in-family” was a designation introduced post-Challenger to separate problems by seriousness so that “out-of-family” problems got more attention, by definition the problems that were shifted into the lesser “in-family” category got less attention. The Board’s investigation uncovered no paper trail showing escalating concern about the foam problem like the one that Solid Rocket Booster engineers left prior to Challenger. So ingrained was the agency’s belief that foam debris was not a threat to flight safety that in press briefings after the Columbia accident, the Space Shuttle Program Manager still discounted the foam as a probable cause, saying that Shuttle managers were “comfortable” with their previous risk assessments.

From the beginning, NASA’s belief about both these problems was affected by the fact that engineers were evaluating them in a work environment where technical problems were normal. Although management treated the Shuttle as operational, it was in reality an experimental vehicle. Many anomalies were expected on each mission. Against this backdrop, an anomaly was not in itself a warning sign of impending catastrophe. Another contributing factor was that both foam debris strikes and O-ring erosion events were examined separately, one at a time. Individual incidents were not read by engineers as strong signals of danger. What NASA engineers and managers saw were pieces of ill-structured problems. An incident of O-ring erosion or foam bipod debris would be followed by several launches where the machine behaved properly, so that signals of danger
were followed by all-clear signals – in other words, NASA managers and engineers were receiving mixed signals. Some signals defined as weak at the time were, in retrospect, warnings of danger. Foam debris damaged tile was assumed (erroneously) not to pose a danger to the wing. If a primary O-ring failed, the secondary was assumed (erroneously) to provide a backup. Finally, because foam debris strikes were occurring frequently, like O-ring erosion in the years before Challenger, foam anomalies became routine signals – a normal part of Shuttle operations, not signals of danger. Other anomalies gave signals that were strong, like wiring malfunctions or the cracked balls in Strut Tie Rod Assemblies, which had a clear relationship to a “loss of mission.” On those occasions, NASA stood down from launch, sometimes for months, while the problems were corrected. In contrast, foam debris and eroding O-rings were defined as nagging issues of seemingly little consequence. Their significance became clear only in retrospect, after lives had been lost.

History became cause as the repeating pattern of anomalies was ratified as safe in Flight Readiness Reviews. The official definitions of risk assigned to each anomaly in Flight Readiness Reviews limited the actions taken and the resources spent on these problems. Two examples of the road not taken and the devastating implications for the future occurred close in time to both accidents. On the October 2002 launch of STS-112, a large piece of bipod ramp foam hit and damaged the External Tank Attachment ring on the Solid Rocket Booster skirt, a strong signal of danger 10 years after the last known bipod ramp foam event. Prior to Challenger, there was a comparable surprise. After a January 1985 launch, for which the Shuttle sat on the launch pad for three consecutive nights of unprecedented cold temperatures, engineers observed the Scorched putty in between – an indication that the joint nearly failed. But accidents are not always preceded by a wake-up call.

In 1985, engineers realized they needed data on the relationship between cold temperatures and O-ring erosion. However, the task of getting better temperature data stayed on the back burner because of the definition of risk: the primary erosion was within the experience base; the secondary O-ring (thought to be redundant) was not damaged and, significantly, there was a low probability that such cold Florida temperatures would recur. The scorched putty, initially a strong signal, was redefined after analysis as weak. On the eve of the Challenger launch, when cold temperature became a concern, engineers had no test data on the effect of cold temperatures on O-ring erosion. Before Columbia, engineers concluded that the damage from the STS-112 foam hit in October 2002 was not a threat to flight safety. After analysis, the biggest foam hit to date was redefined as a weak signal. Similar self-defeating actions and inactions followed. Engineers were again dealing with the poor quality of tracking camera images of strikes during ascent. Yet NASA took no steps to improve imagery and took no immediate action to reduce the risk of bipod and foam shedding and potential damage to the Orbiter before Columbia. Furthermore, NASA performed no tests on what would happen if a wing leading edge were struck by bipod foam, even though foam had repeatedly separated from the External Tank.

During the Challenger investigation, Rogers Commission member Dr. Richard Feynman famously compared launching Shuttles with known problems to playing Russian roulette. But that characterization is only possible in hindsight. It is not how NASA personnel perceived the risks as they were being assessed, one launch at a time. Playing Russian roulette implies that the pistol-holder realizes that death might be imminent and still takes the risk. For both foam debris and O-ring erosion, fixes were in the works at the time of the accidents, but there was no rush to complete them because neither problem was defined as a show-stopper. Each time an incident occurred, the Flight Readiness process declared it safe to continue flying. Taken one at a time, each decision seemed correct. The agency allocated attention and resources to these two problems accordingly. The consequences of living with both of these anomalies were, in its view, minor. Not all engineers agreed in the months immediately preceding Challenger, but the dominant view at NASA – the managerial view – was, as one manager put it, “we were just eroding rubber O-rings,” which was a low-cost problem. The financial consequences of foam debris also were relatively low; replacing tiles extended the turnaround time between launches. In both cases, NASA was comfortable with its analyses. Prior to each accident, the agency saw no greater consequences on the horizon.

### 8.3 System Effects: The Impact of History and Politics on Risky Work

The series of engineering decisions that normalized technical deviations shows one way that history became cause in both accidents. But NASA’s own history encouraged this pattern of flying with known flaws. Seventeen years separated the two accidents. NASA Administrators, Congresses, and political administrations changed. However, NASA’s political and budgetary situation remained the same in principle as it had been since the inception of the Shuttle Program. NASA remained a politicized and vulnerable agency, dependent on key political players who accepted NASA’s ambitious proposals and then imposed strict budget limits. Post-Challenger policy decisions made by the White House, Congress, and NASA leadership resulted in the agency reproducing many of the failings identified by the Rogers Commission. Policy constraints affected the Shuttle Program’s organization culture, its structure, and the structure of the safety system. The three combined to keep NASA on its slippery slope toward Challenger and Columbia. NASA culture allowed flying with flaws when problems were defined as normal and routine; the structure of NASA’s Shuttle Program blocked the flow of critical information up the hierarchy, so definitions of risk continued unaltered. Finally, a perennially weakened safety system, unable to critically analyze and intervene, had no choice but to ratify the existing risk assessments on these two problems. The following comparison shows that these system effects persisted through time, and affected engineering decisions in the years leading up to both accidents.
The Board found that dangerous aspects of NASA’s 1986 culture, identified by the Rogers Commission, remained unchanged. The Space Shuttle Program had been built on compromises hammered out by the White House and NASA headquarters.\textsuperscript{14} As a result, NASA was transformed from a research and development agency to more of a business, with schedules, production pressures, deadlines, and cost efficiency goals elevated to the level of technical innovation and safety goals.\textsuperscript{15} The Rogers Commission dedicated an entire chapter of its report to production pressures.\textsuperscript{16} Moreover, the Rogers Commission, as well as the 1990 Augustine Committee and the 1999 Shuttle Independent Assessment Team, criticized NASA for treating the Shuttle as if it were an operational vehicle. Launching on a tight schedule, which the agency had pursued as part of its initial bargain with the White House, was not the way to operate what was in fact an experimental vehicle. The Board found that prior to Columbia, a budget-limited Space Shuttle Program, forced again and again to refashion itself into an efficiency model because of repeated government cutbacks, was beset by these same ills. The harmful effects of schedule pressure identified in previous reports had returned.

Prior to both accidents, NASA was scrambling to keep up. Not only were schedule pressures impacting the people who worked most closely with the technology—technicians, mission operators, flight crews, and vehicle processors—engineering decisions also were affected.\textsuperscript{17} For foam debris and O-ring erosion, the definition of risk established during the Flight Readiness process determined actions taken and not taken, but the schedule and shoestring budget were equally influential. NASA was cutting corners. Launches proceeded with incomplete engineering work on these flaws. Challenger-era engineers were working on a permanent fix for the booster joints while launches continued.\textsuperscript{18} After the major foam bipod hit on STS-112, management made the deadline for corrective action on the foam problem after the next launch, STS-113, and then slipped it again until after the flight of STS-107. Delays for flowliner and Ball Strut Tie Rod Assembly problems left no margin in the schedule between February 2003 and the management-imposed February 2004 launch date for the International Space Station Node 2. Available resources—including time out of the schedule for research and hardware modifications—went to the problems that were designated as serious—those most likely to bring down a Shuttle. The NASA culture encouraged flying with flaws because the schedule could not be held up for routine problems that were not defined as a threat to mission safety.\textsuperscript{19}

The question the Board had to answer was why, since the foam debris anomalies went on for so long, had no one recognized the trend and intervened? The O-ring history prior to Challenger had followed the same pattern. This question pointed the Board’s attention toward the NASA organization structure and the structure of its safety system. Safety-oriented organizations often build in checks and balances to identify and monitor signals of potential danger. If these checks and balances were in place in the Shuttle Program, they weren’t working. Again, past policy decisions produced system effects with implications for both Challenger and Columbia.

Prior to Challenger, Shuttle Program structure had hindered information flows, leading the Rogers Commission to conclude that critical information about technical problems was not conveyed effectively through the hierarchy.\textsuperscript{20} The Space Shuttle Program had altered its structure by outsourcing to contractors, which added to communication problems. The Commission recommended many changes to remedy these problems, and NASA made many of them. However, the Board found that those post-Challenger changes were undone over time by management actions.\textsuperscript{21} NASA administrators, reacting to government pressures, transferred more functions and responsibilities to the private sector. The change was cost-efficient, but personnel cuts reduced oversight of contractors at the same time that the agency’s dependence upon contractor engineering judgment increased. When high-risk technology is the product and lives are at stake, safety, oversight, and communication flows are critical. The Board found that the Shuttle Program’s normal chain of command and matrix system did not perform a check-and-balance function on either foam or O-rings.

The Flight Readiness Review process might have reversed the disastrous trend of normalizing O-ring erosion and foam debris hits, but it didn’t. In fact, the Rogers Commission found that the Flight Readiness process only affirmed the pre-Challenger engineering risk assessments.\textsuperscript{22} Equally troubling, the Board found that the Flight Readiness process, which is built on consensus verified by signatures of all responsible parties, in effect renders no one accountable. Although the process was altered after Challenger, these changes did not erase the basic problems that were built into the structure of the Flight Readiness Review.\textsuperscript{23} Managers at the top were dependent on engineers at the bottom for their engineering analysis and risk assessments. Information was lost as engineering risk analyses moved through the process. At succeeding stages, management awareness of anomalies, and therefore risks, was reduced either because of the need to be increasingly brief and concise as all the parts of the system came together, or because of the need to produce consensus decisions at each level. The Flight Readiness process was designed to assess hardware and take corrective actions that would transform known problems into acceptable flight risks, and that is precisely what it did. The 1986 House Committee on Science and Technology concluded during its investigation into Challenger that Flight Readiness Reviews had performed exactly as they were designed, but that they could not be expected to replace engineering analysis, and therefore they “cannot be expected to prevent a flight because of a design flaw that Project management had already determined an acceptable risk.”\textsuperscript{24} Those words, true for the history of O-ring erosion, also hold true for the history of foam debris.

The last line of defense against errors is usually a safety system. But the previous policy decisions by leaders described in Chapter 5 also impacted the safety structure and contributed to both accidents. Neither in the O-ring erosion nor the foam debris problems did NASA’s safety system attempt to reverse the course of events. In 1986, the Rogers Commission called it “The Silent Safety System.”\textsuperscript{25} Pre-Challenger budget shortages resulted in safety personnel cutbacks. Without clout or independence, the
safety personnel who remained were ineffective. In the case of Columbia, the Board found the same problems were reproduced and for an identical reason: when pressed for cost reduction, NASA attacked its own safety system. The faulty assumption that supported this strategy prior to Columbia was that a reduction in safety staff would not result in a reduction of safety, because contractors would assume greater safety responsibility. The effectiveness of those remaining staff safety engineers was blocked by their dependence on the very Program they were charged to supervise. Also, the Board found many safety units with unclear roles and responsibilities that left crucial gaps. Post-Challenger NASA still had no systematic procedure for identifying and monitoring trends. The Board was surprised at how long it took NASA to put together trend data in response to Board requests for information. Problem reporting and tracking systems were still overloaded or underused, which undermined their very purpose. Multiple job titles disguised the true extent of safety personnel shortages. The Board found cases in which the same person was occupying more than one safety position – and in one instance at least three positions – which compromised any possibility of safety organization independence because the jobs were established with built-in conflicts of interest.

9.4 Organization, Culture, and Unintended Consequences

A number of changes to the Space Shuttle Program structure made in response to policy decisions had the unintended effect of perpetuating dangerous aspects of pre-Challenger culture and continued the pattern of normalizing things that were not supposed to happen. At the same time that NASA leaders were emphasizing the importance of safety, their personnel cutbacks sent other signals. Streamlining and downsizing, which scarcely go unnoticed by employees, convey a message that efficiency is an important goal. The Shuttle/Space Station partnership affected both programs. Working evenings and weekends just to meet the International Space Station Node 2 deadline sent a signal to employees that schedule is important. When paired with the “faster, better, cheaper” NASA motto of the 1990s and cuts that dramatically decreased safety personnel, efficiency becomes a strong signal and safety a weak one. This kind of doublespeak by top administrators affects people’s decisions and actions without them even realizing it.

Changes in Space Shuttle Program structure contributed to the accident in a second important way. Despite the constraints that the agency was under, prior to both accidents NASA appeared to be immersed in a culture of invincibility, in stark contradiction to post-accident reality. The Rogers Commission found a NASA blinded by its “Can-Do” attitude, a cultural artifact of the Apollo era that was inappropriate in a Space Shuttle Program so strapped by schedule pressures and shortages that spare parts had to be cannibalized from one vehicle to launch another. This can-do attitude bolstered administrators’ belief in an achievable launch rate, the belief that they had an operational system, and an unwillingness to listen to outside experts. The Aerospace Safety and Advisory Panel in a 1985 report told NASA that the vehicle was not operational and NASA should stop treating it as if it were. The Board found that even after the loss of Challenger, NASA was guilty of treating an experimental vehicle as if it were operational and of not listening to outside experts. In a repeat of the pre-Challenger warning, the 1999 Shuttle Independent Assessment Team report reiterated that “the Shuttle was not an ‘operational’ vehicle in the usual meaning of the term.” Engineers and program planners were also affected by “Can-Do,” which, when taken too far, can create a reluctance to say that something cannot be done.

How could the lessons of Challenger have been forgotten so quickly? Again, history was a factor. First, if success is measured by launches and landings, the machine appeared to be working successfully prior to both accidents. Challenger was the 25th launch. Seventeen years and 87 missions passed without major incident. Second, previous policy decisions again had an impact. NASA’s Apollo-era research and development culture and its prized deference to the technical expertise of its working engineers was overridden in the Space Shuttle era by “bureaucratic accountability” – an allegiance to hierarchy, procedure, and following the chain of command. Prior to Challenger, the can-do culture was a result not just of years of apparently successful launches, but of the cultural belief that the Shuttle Program’s many structures, rigorous procedures, and detailed system of rules were responsible for those successes. The Board noted that the pre-Challenger layers of processes, boards, and panels that had produced a false sense of confidence in the system and its level of safety returned in full force prior to Columbia. NASA made many changes to the Space Shuttle Program structure after Challenger. The fact that many changes had been made supported a belief in the safety of the system, the invincibility of organizational and technical systems, and ultimately, a sense that the foam problem was understood.

8.5 History as Cause: Two Accidents

Risk, uncertainty, and history came together when unprecedented circumstances arose prior to both accidents. For Challenger, the weather prediction for launch time the next day was for cold temperatures that were out of the engineering experience base. For Columbia, a large foam hit – also outside the experience base – was discovered after launch. For the first case, all the discussion was pre-launch; for the second, it was post-launch. This initial difference determined the shape these two decision sequences took, the number of people who had information about the problem, and the locations of the involved parties.

For Challenger, engineers at Morton-Thiokol, the Solid Rocket Motor contractor in Utah, were concerned about the effect of the unprecedented cold temperatures on the rubber O-rings. Because launch was scheduled for the next morning, the new condition required a reassessment of the engineering analysis presented at the Flight Readiness Review two weeks prior. A teleconference began at 8:45 p.m. Eastern Standard Time (EST) that included 34 people in three locations: Morton-Thiokol in Utah, Marshall, and Kennedy. Thiokol engineers were recommending a launch delay. A reconsideration of a Flight Readiness Review risk
assessment the night before a launch was as unprecedented as the predicted cold temperatures. With no ground rules or procedures to guide their discussion, the participants automatically reverted to the centralized, hierarchical, tightly structured, and procedure-bound model used in Flight Readiness Reviews. The entire discussion and decision to launch began and ended with this group of 34 engineers. The phone conference linking them together concluded at 11:15 p.m. EST after a decision to accept the risk and fly.

For Columbia, information about the foam debris hit was widely distributed the day after launch. Time allowed for videos of the strike, initial assessments of the size and speed of the foam, and the approximate location of the impact to be dispersed throughout the agency. This was the first debris impact of this magnitude. Engineers at the Marshall, Johnson, Kennedy, and Langley centers showed initiative and jumped on the problem without direction from above. Working groups and e-mail groups formed spontaneously. The size of Johnson’s Debris Assessment Team alone neared and in some instances exceeded the total number of participants in the 1986 Challenger teleconference. Rather than a tightly constructed exchange of information completed in a few hours, time allowed for the development of ideas and free-wheeling discussion among the engineering ranks. The early post-launch discussion among engineers and all later decision-making at management levels were decentralized, loosely organized, and with little form. While the spontaneous and decentralized exchanging of information was evidence that NASA’s original technical culture was alive and well, the diffuse form and lack of structure in the rest of the proceedings would have several negative consequences.

In both situations, all new information was weighed and interpreted against past experience. Formal categories and cultural beliefs provide a consistent frame of reference in which people view and interpret information and experiences. Pre-existing definitions of risk shaped the actions taken and not taken. Worried engineers in 1986 and again in 2003 found it impossible to reverse the Flight Readiness Review risk assessments that foam and O-rings did not pose safety-of-flight concerns. These engineers could not prove that foam strikes and cold temperatures were unsafe, even though the previous analyses that declared them safe had been incomplete and were based on insufficient data and testing. Engineers’ failed attempts were not just a matter of psychological frames and interpretations. The obstacles these engineers faced were political and organizational. They were rooted in NASA history and the decisions of leaders that had altered NASA culture, structure, and the structure of the safety system and affected the social context of decision-making for both accidents. In the following comparison of these critical decision scenarios for Columbia and Challenger, the systemic problems in the NASA organization are in italics, with the system effects on decision-making following.

NASA had conflicting goals of cost, schedule, and safety. Safety lost out as the mandates of an “operational system” increased the schedule pressure. Scarce resources went to problems that were defined as more serious, rather than to foam strikes or O-ring erosion.

In both situations, upper-level managers and engineering teams working the O-ring and foam strike problems held opposing definitions of risk. This was demonstrated immediately, as engineers reacted with urgency to the immediate safety implications: Thiokol engineers scrambled to put together an engineering assessment for the teleconference, Langley Research Center engineers initiated simulations of landings that were run after hours at Ames Research Center, and Boeing analysts worked through the weekend on the debris impact analysis. But key managers were responding to additional demands of cost and schedule, which competed with their safety concerns. NASA’s conflicting goals put engineers at a disadvantage before these new situations even arose. In neither case did they have good data as a basis for decision-making. Because both problems had been previously normalized, resources sufficient for testing or hardware were not dedicated. The Space Shuttle Program had not produced good data on the correlation between cold temperature and O-ring resilience or good data on the potential effect of bipod ramp foam debris hits.

Cultural beliefs about the low risk O-rings and foam debris posed, backed by years of Flight Readiness Review decisions and successful missions, provided a frame of reference against which the engineering analyses were judged. When confronted with the engineering risk assessments, top Shuttle Program managers held to the previous Flight Readiness Review assessments. In the Challenger teleconference, where engineers were recommending that NASA delay the launch, the Marshall Solid Rocket Booster Project manager, Lawrence Mulloy, repeatedly challenged the contractor’s risk assessment and restated Thiokol’s engineering rationale for previous flights.

STS-107 Mission Management Team Chair Linda Ham made many statements in meetings reiterating her understanding that foam was a maintenance problem and a turnaround issue, not a safety-of-flight issue.

The effects of working as a manager in a culture with a cost/efficiency/safety conflict showed in managerial responses. In both cases, managers’ techniques focused on the information that tended to support the expected or desired result at that time. In both cases, believing the safety of the mission was not at risk, managers drew conclusions that minimized the risk of delay. At one point, Marshall’s Mulloy, believing in the previous Flight Readiness Review assessments, unconvinced by the engineering analysis, and concerned about the schedule implications of the 53-degree temperature limit on launch the engineers proposed, said, “My God, Thiokol, when do you want me to launch, next April?” Reflecting the overall goal of keeping to the Node 2 launch schedule, Ham’s priority was to avoid the delay of STS–114, the next mission after STS–107. Ham was slated as Manager of Launch Integration for STS–114 – a dual role promoting a conflict of interest and a single-point failure, a situation that should be avoided in all organizational as well as technical systems.

NASA’s culture of bureaucratic accountability emphasized chain of command, procedure, following the rules, and going by the book. While rules and procedures were essential for coordination, they had an unintended but negative effect. Allegiance to hierarchy and procedure had replaced deference to NASA engineers’ technical expertise.
In both cases, engineers initially presented concerns as well as possible solutions – a request for images, a recommendation to place temperature constraints on launch. Management did not listen to what their engineers were telling them. Instead, rules and procedures took priority. For Columbia, program managers turned off the Kennedy engineers’ initial request for Department of Defense imagery, with apologies to Defense Department representatives for not having followed “proper channels.” In addition, NASA administrators asked for and promised corrective action to prevent such a violation of protocol from recurring. Debris Assessment Team analysts at Johnson were asked by managers to demonstrate a “mandatory need” for their imagery request, but were not told how to do that. Both Challenger and Columbia engineering teams were held to the usual quantitative standard of proof. But it was a reverse of the usual circumstance: instead of having to prove it was safe to fly, they were asked to prove that it was unsafe to fly.

In the Challenger teleconference, a key engineering chart presented a qualitative argument about the relationship between cold temperatures and O-ring erosion that engineers were asked to prove. Thiokol’s Roger Boisjoly said, “I had no data to quantify it. But I did say I knew it was away from goodness in the current data base.” Similarly, the Debris Assessment Team was asked to prove that the foam hit was a threat to flight safety, a determination that only the imagery they were requesting could help them make. Ignored by management was the qualitative data that the engineering teams did have: both instances were outside the experience base. In stark contrast to the requirement that engineers adhere to protocol and hierarchy was management’s failure to apply this criterion to their own activities. The Mission Management Team did not meet on a regular schedule during the mission, proceeded in a loose format that allowed informal influence and status differences to shape their decisions, and allowed unchallenged opinions and assumptions to prevail, all the while holding the engineers who were making risk assessments to higher standards. In highly uncertain circumstances, when lives were immediately at risk, management failed to defer to its engineers and failed to recognize that different data standards – qualitative, subjective, and intuitive – and different processes – democratic rather than protocol and chain of command – were more appropriate.

The organizational structure and hierarchy blocked effective communication of technical problems. Signals were overlooked, people were silenced, and useful information and dissenting views on technical issues did not surface at higher levels. What was communicated to parts of the organization was that O-ring erosion and foam debris were not problems.

Structure and hierarchy represent power and status. For both Challenger and Columbia, employees’ positions in the organization determined the weight given to their information, by their own judgment and in the eyes of others. As a result, many signals of danger were missed. Relevant information that could have altered the course of events was available but was not presented.

Early in the Challenger teleconference, some engineers who had important information did not speak up. They did not define themselves as qualified because of their position: they were not in an appropriate specialization, had not recently worked the O-ring problem, or did not have access to the “good data” that they assumed others more involved in key discussions would have. Geographic locations also resulted in missing signals. At one point, in light of Marshall’s objections, Thiokol managers in Utah requested an “off-line caucus” to discuss their data. No consensus was reached, so a “management risk decision” was made. Managers voted and engineers did not. Thiokol managers came back on line, saying they had reversed their earlier NO-GO recommendation, decided to accept risk, and would send new engineering charts to back their reversal. When a Marshall administrator asked, “Does anyone have anything to add to this?,” no one spoke. Engineers at Thiokol who still objected to the decision later testified that they were intimidated by management authority, were accustomed to turning their analysis over to managers and letting them decide, and did not have the quantitative data that would empower them to object further.

In the more decentralized decision process prior to Columbia’s re-entry, structure and hierarchy again were responsible for an absence of signals. The initial request for imagery came from the “low status” Kennedy Space Center, bypassed the Mission Management Team, and went directly to the Department of Defense separate from the all-powerful Shuttle Program. By using the Engineering Directorate avenue to request imagery, the Debris Assessment Team was working at the margins of the hierarchy. But some signals were missing even when engineers traversed the appropriate channels. The Mission Management Team Chair’s position in the hierarchy governed what information she would or would not receive. Information was lost as it traveled up the hierarchy. A demoralized Debris Assessment Team did not include a slide about the need for better imagery in their presentation to the Mission Evaluation Room. Their presentation included the Crater analysis, which they reported as incomplete and uncertain. However, the Mission Evaluation Room manager perceived the Boeing analysis as rigorous and quantitative. The choice of headings, arrangement of information, and size of bullets on the key chart served to highlight what management already believed. The uncertainties and assumptions that signaled danger dropped out of the information chain when the Mission Evaluation Room manager condensed the Debris Assessment Team’s formal presentation to an informal verbal briefing at the Mission Management Team meeting.

As what the Board calls an “informal chain of command” began to shape STS-107’s outcome, location in the structure empowered some to speak and silenced others. For example, a Thermal Protection System tile expert, who was a member of the Debris Assessment Team but had an office in the more prestigious Shuttle Program, used his personal network to shape the Mission Management Team view and snuff out dissent. The informal hierarchy among and within Centers was also influential. Early identifications of problems by Marshall and Kennedy may have contributed to the Johnson-based Mission Management Team’s indifference to concerns about the foam strike. The engineers and managers circulating e-mails at Langley were peripheral to the Shuttle Program, not structurally connected to the proceedings, and...
therefore of lower status. When asked in a post-accident press conference why they didn’t voice their concerns to Shuttle Program management, the Langley engineers said that people “need to stick to their expertise.” Status mattered. In its absence, numbers were the great equalizer. One striking exception: the Debris Assessment Team tile expert was so influential that his word was taken as gospel, though he lacked the requisite expertise, data, or analysis to evaluate damage to RCC. For those with lesser standing, the requirement for data was stringent and inhibiting, which resulted in information that warned of danger not being passed up the chain. As in the teleconference, Debris Assessment Team engineers did not speak up when the Mission Management Team Chair asked if anyone else had anything to say. Not only did they not have the numbers, they also were intimidated by the Mission Management Team Chair’s position in the hierarchy and the conclusions she had already made. Debris Assessment Team members signed off on the Crater analysis, even though they had trouble understanding it. They still wanted images of Columbia’s left wing.

In neither impending crisis did management recognize how structure and hierarchy can silence employees and follow through by polling participants, soliciting opinions, or bringing in outsiders who might have a different perspective or useful information. Perhaps the ultimate example of engineering concerns not making their way upstream, Challenger astronauts were told that the cold temperature was not a problem, and Columbia astronauts were told that the foam strike was not a problem.

**NASA structure changed as roles and responsibilities were transferred to contractors, which increased the dependence on the private sector for safety functions and risk assessment while simultaneously reducing the in-house capability to spot safety issues.**

A critical turning point in both decisions hung on the discussion of contractor risk assessments. Although both Thiokol and Boeing engineering assessments were replete with uncertainties, NASA ultimately accepted each. Thiokol’s initial recommendation against the launch of Challenger was at first criticized by Marshall as flawed and unacceptable. Thiokol was recommending an unheard-of delay on the eve of a launch, with schedule ramifications and NASA-contractor relationship repercussions. In the Thiokol off-line caucus, a senior vice president who seldom participated in these engineering discussions championed the Marshall engineering rationale for flight. When he told the managers present to “Take off your engineering hat and put on your management hat,” they reversed the position their own engineers had taken. Marshall engineers then accepted this assessment, deferring to the expertise of the contractor. NASA was dependent on Thiokol for the risk assessment, but the decision process was affected by the contractor’s dependence on NASA. Not willing to be responsible for a delay, and swayed by the strength of Marshall’s argument, the contractor did not act in the best interests of safety. Boeing’s Crater analysis was performed in the context of the Debris Assessment Team, which was a collaborative effort that included Johnson, United Space Alliance, and Boeing. In this case, the decision process was also affected by NASA’s dependence on the contractor. Unfamiliar with Crater, NASA engineers and managers had to rely on Boeing for interpretation and analysis, and did not have the training necessary to evaluate the results. They accepted Boeing engineers’ use of Crater to model a debris impact 400 times outside validated limits.

**NASA’s safety system lacked the resources, independence, personnel, and authority to successfully apply alternate perspectives to developing problems. Overlapping roles and responsibilities across multiple safety offices also undermined the possibility of a reliable system of checks and balances.**

NASA’s “Silent Safety System” did nothing to alter the decision-making that immediately preceded both accidents. No safety representatives were present during the Challenger teleconference — no one even thought to call them. In the case of Columbia, safety representatives were present at Mission Evaluation Room, Mission Management Team, and Debris Assessment Team meetings. However, rather than critically question or actively participate in the analysis, the safety representatives simply listened and concurred.

### 8.6 Changing NASA’s Organizational System

The echoes of Challenger in Columbia identified in this chapter have serious implications. These repeating patterns mean that flawed practices embedded in NASA’s organizational system continued for 20 years and made substantial contributions to both accidents. The Columbia Accident Investigation Board noted the same problems as the Rogers Commission. An organization system failure calls for corrective measures that address all relevant levels of the organization, but the Board’s investigation shows that for all its cutting-edge technologies, “diving-catch” rescues, and imaginative plans for the technology and the future of space exploration, NASA has shown very little understanding of the inner workings of its own organization.

NASA managers believed that the agency had a strong safety culture, but the Board found that the agency had the same conflicting goals that it did before Challenger, when schedule concerns, production pressure, cost-cutting and a drive for ever-greater efficiency — all the signs of an “operational” enterprise — had eroded NASA’s ability to assure mission safety. The belief in a safety culture has even less credibility in light of repeated cuts of safety personnel and budgets — also conditions that existed before Challenger. NASA managers stated confidently that everyone was encouraged to speak up about safety issues and that the agency was responsive to those concerns, but the Board found evidence to the contrary in the responses to the Debris Assessment Team’s request for imagery, to the initiation of the imagery request from Kennedy Space Center, and to the “we were just ‘what-iffing’” e-mail concerns that did not reach the Mission Management Team. NASA’s bureaucratic structure kept important information from reaching engineers and managers alike. The same NASA whose engineers showed initiative and a solid working knowledge of how to get things done fast had a managerial culture with an allegiance to bureaucracy and cost-efficiency that squelched
the engineers’ efforts. When it came to managers’ own actions, however, a different set of rules prevailed. The Board found that Mission Management Team decision-making operated outside the rules even as it held its engineers to a stifling protocol. Management was not able to recognize that in unprecedented conditions, when lives are on the line, flexibility and democratic process should take priority over bureaucratic response.47

During the Columbia investigation, the Board consistently searched for causal principles that would explain both the technical and organizational system failures. These principles were needed to explain Columbia and its echoes of Challenger. They were also necessary to provide guidance for NASA. The Board’s analysis of organizational causes in Chapters 5, 6, and 7 supports the following principles that should govern the changes in the agency’s organizational system. The Board’s specific recommendations, based on these principles, are presented in Part Three.

Leaders create culture. It is their responsibility to change it. Top administrators must take responsibility for risk, failure, and safety by remaining alert to the effects their decisions have on the system. Leaders are responsible for establishing the conditions that lead to their subordinates’ successes or failures. 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. The measure of NASA’s success became how much costs were reduced and how efficiently the schedule was met. But the Space Shuttle is not now, nor has it ever been, an operational vehicle. We cannot explore space on a fixed-cost basis. Nevertheless, due to International Space Station needs and scientific experiments that require particular timing and orbits, the Space Shuttle Program seems likely to continue to be schedule-driven. National leadership needs to recognize that NASA must fly only when it is ready. As the White House, Congress, and NASA Headquarters plan the future of human space flight, the goals and the resources required to achieve them safely must be aligned.

Changes in organizational structure should be made only with careful consideration of their effect on the system and their possible unintended consequences. Changes that make the organization more complex may create new ways that it can fail.48 When changes are put in place, the risk of error initially increases, as old ways of doing things compete with new. Institutional memory is lost as personnel and records are moved and replaced. Changing the structure of organizations is complicated by external political and budgetary constraints, the inability of leaders to conceive of the full ramifications of their actions, the vested interests of insiders, and the failure to learn from the past.49

Nonetheless, changes must be made. The Shuttle Program’s structure is a source of problems, not just because of the way it impedes the flow of information, but because it has had effects on the culture that contradict safety goals. NASA’s blind spot is it believes it has a strong safety culture. Program history shows that the loss of a truly indepen-

Strategies must increase the clarity, strength, and presence of signals that challenge assumptions about risk. Twice in NASA history, the agency embarked on a slippery slope that resulted in catastrophe. Each decision, taken by itself, seemed correct, routine, and indeed, insignificant and unremarkable. Yet in retrospect, the cumulative effect was stunning. In both pre-accident periods, events unfolded over a long time and in small increments rather than in sudden and dramatic occurrences. NASA’s challenge is to design systems that maximize the clarity of signals, amplify weak signals so they can be tracked, and account for missing signals. For both accidents there were moments when management definitions of risk might have been reversed were it not for the many missing signals – an absence of trend analysis, imagery data not obtained, concerns not voiced, information overlooked or dropped from briefings. A safety team must have equal and independent representation so that managers are not again lulled into complacency by shifting definitions of risk. It is obvious but worth acknowledging that people who are marginal and powerless in organizations may have useful information or opinions that they don’t express. Even when these people are encouraged to speak, they find it intimidating to contradict a leader’s strategy or a group consensus. Extra effort must be made to contribute all relevant information to discussions of risk. These strategies are important for all safety aspects, but especially necessary for ill-structured problems like O-rings and foam debris. Because ill-structured problems are less visible and therefore invite the normalization of deviance, they may be the most risky of all.

Challenger launches on the ill-fated STS-33/51-L mission on January 28, 1986. The Orbiter would be destroyed 73 seconds later.
ENDNOTES FOR CHAPTER 8

The citations that contain a reference to “CAIB document” with CABI or CTF followed by seven to eleven digits, such as CABI001-0010, refer to a document in the Columbia Accident Investigation Board database maintained by the Department of Justice and archived at the National Archives.

1 Turner studied 85 different accidents and disasters, noting a common pattern: each had a long incubation period in which hazards and warning signs prior to the accident were either ignored or misinterpreted. He called these “failures of foresight.” Barry Turner, Man-made Disasters, (London: Wykeham, 1978); Barry Turner and Nick Pidgeon, Man-made Disasters, 2nd ed. (Oxford: Butterworth Heinemann, 1997).

2 Changing personnel is a typical response after an organization has some kind of harmful outcome. It has great symbolic value. A change in personnel points to individuals as the cause and removing them gives the false impression that the problems have been solved, leaving unresolved organizational system problems. See Scott Sagan, The Limits of Safety. Princeton: Princeton University Press, 1993.


8 Turner, Man-made Disasters.


10 Turner, Man-made Disasters.


21 Harry McDonald, Report of the Shuttle Independent Assessment Team.


30 Harry McDonald, Report of the Shuttle Independent Assessment Team.


34 Morton subsequently sold its propulsion division of Alcoa, and the company is now known as ATK Thiokol Propulsion.

35 Report of the Presidential Commission, pp. 82-118.


47 Weick argues that in a risky situation, people need to learn how to “drop their tools,” learn to recognize when they are in unprecedented situations in which following the rules can be disastrous. See Karl E. Weick, “The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster.” Administrative Science Quarterly 38, 1993, pp. 628-652.
