CHAPTER 7

The Accident's Organizational Causes

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."[1] 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.[2] 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.[3] 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, Reliability, 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.[4] The new office's Associate Administrator promptly initiated studies on Shuttle in-flight anomalies, overtime levels, the lack of spare parts, and landing and crew safety systems, among other issues.[5] 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."[6] 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."[7] 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].[8] 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."[9]

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.[10] 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. [11]

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.[12] Additionally, the Board held a forum, organized by the National Safety Council, to define the essential characteristics of a sound safety program.[13]

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.[14] 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.[15] 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.[16] 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.[17] 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.

7.3 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 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

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.[23] 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.[24] 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.[25]

- 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.[26]

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.[27]

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.[28] 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

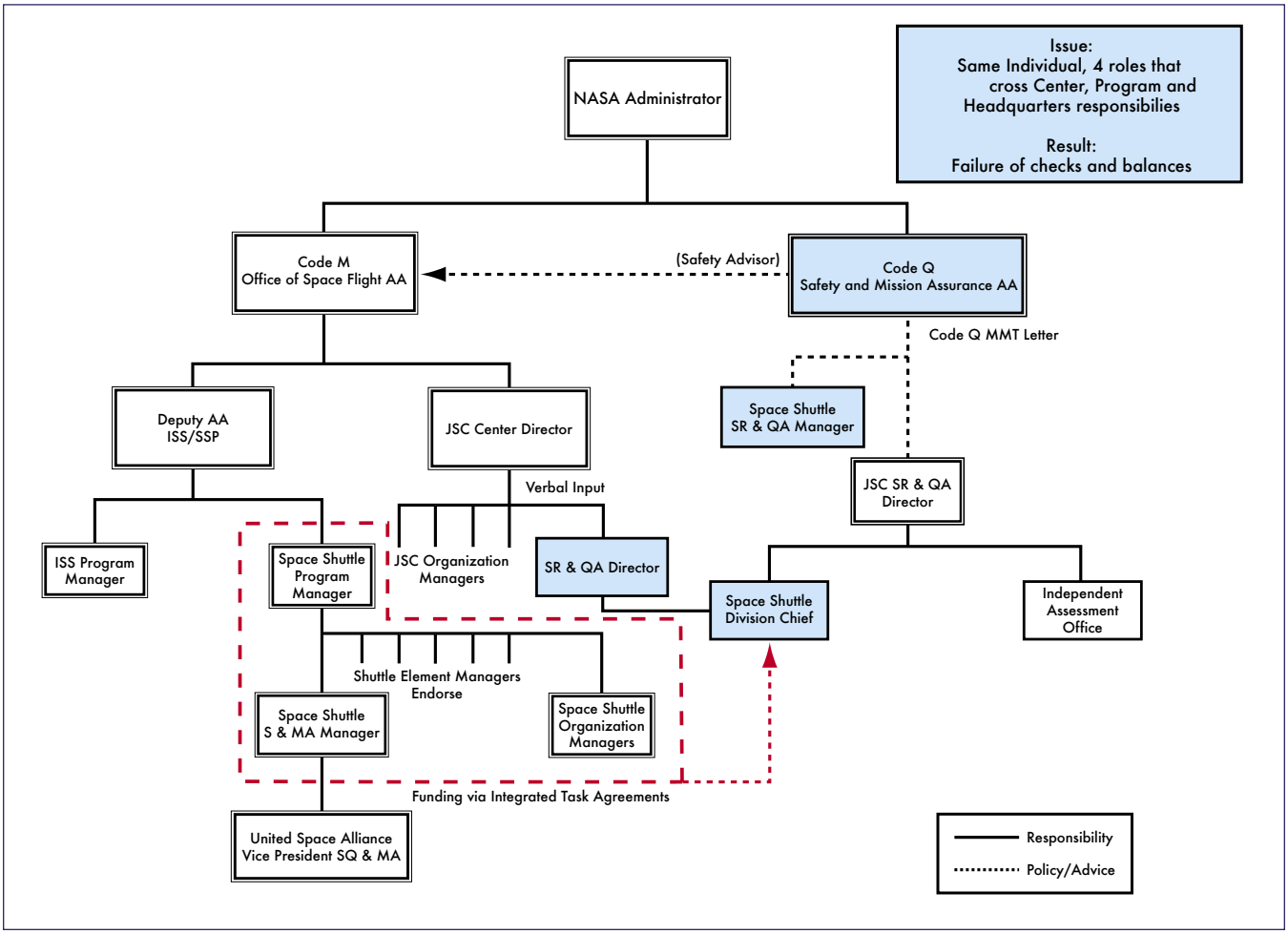


Figure 7.4-1. Independent safety checks and balance failure.

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.[29] 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.[30] 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."[31] 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.[32]

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-

pears 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-

Space Shuttle Safety Upgrade Program

NASA presented a Space Shuttle Safety Upgrade Initiative to Congress as part of its Fiscal Year 2001 budget in March 2000. This initiative sought to create a "Pro-active upgrade program to keep Shuttle flying safely and efficiently to 2012 and beyond to meet agency commitments and goals for human access to space."

The planned Shuttle safety upgrades included: Electric Auxiliary Power Unit, Improved Main Landing Gear Tire, Orbiter Cockpit/Avionics Upgrades, Space Shuttle Main Engine Advanced Health Management System, Block III Space Shuttle Main Engine, Solid Rocket Booster Thrust Vector Control/Auxiliary Power Unit Upgrades Plan, Redesigned Solid Rocket Motor – Propellant Grain Geometry Modification, and External Tank Upgrades – Friction Stir Weld. The plan called for the upgrades to be completed by 2008.

However, as discussed in Chapter 5, every proposed safety upgrade – with a few exceptions – was either not approved or was deferred.

The irony of the Space Shuttle Safety Upgrade Program was that the strategy placed emphasis on keeping the "Shuttle flying safely and efficiently to 2012 and beyond," yet the Space Flight Leadership Council accepted the upgrades **only as long as they were financially feasible**. *Funding a safety upgrade in order to fly safely, and then canceling it for budgetary reasons, makes the concept of mission safety rather hollow.*

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 ineffectual 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.[36] 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.

Dysfunctional Databases

In its investigation, the Board found that the information systems that support the Shuttle program are extremely cumbersome and difficult to use in decision-making at any level. For obvious reasons, these shortcomings imperil the Shuttle Program's ability to disseminate and share critical information among its many layers. This section explores the report databases that are crucial to effective risk management.

- **Problem Reporting and Corrective Action:** The Problem Reporting and Corrective Action database records any non-conformances (instances in which a requirement is not met). Formerly, different Centers and contractors used the Problem Reporting and Corrective Action database differently, which prevented comparisons across the database. NASA recently initiated an effort to integrate these databases to permit anyone in the agency to access information from different Centers. This system, Web Program Compliance Assurance and Status System (WEBPCASS), is supposed to provide easier access to consolidated information and facilitates higher-level searches.

  However, NASA safety managers have complained that the system is too time-consuming and cumbersome. Only employees trained on the database seem capable of using WEBPCASS effectively. One particularly frustrating aspect of which the Board is acutely aware is the database's waiver section. It is a critical information source, but only the most expert users can employ it effectively. The database is also incomplete. For instance, in the case of foam strikes on the Thermal Protection System, only strikes that were declared "In-Fight Anomalies" are added to the Problem Reporting and Corrective Action database, which masks the full extent of the foam debris trends.

- **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.[37]

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 continue 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,

Engineering by Viewgraphs

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]

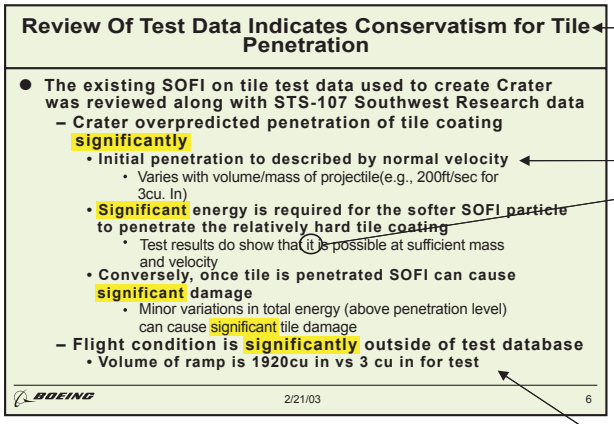
The slide created six levels of hierarchy, signified by the title and the symbols to the left of each line. These levels prioritized information that was already contained in 11 simple sentences. Tufte also notes that the title is confusing. "Review of Test Data Indicates Conservatism" refers not to 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 misplaced 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.



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 ambiquous. (The low resolution and large font generate 3 typographic orphans, lonely words dangling on a seperate 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 ambiquous 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 outside its validated limits. Nor did safety personnel provide any additional oversight. NASA failed to connect the dots: the engineers who misinterpreted Crater – a tool already unsuited to the task at hand – were the very ones the Shuttle Program identified as engendering the most risk in their transition from Huntington Beach. The Board views this example as characteristic of the greater turbulence the Shuttle Program experienced in the decade before *Columbia* as a result 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 raise concerns 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.

F7.4-1 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.

F7.4-2 Safety and Mission Assurance organizations supporting the Shuttle Program are largely dependent upon the Program for funding, which hampers their status as independent advisors.

F7.4-3 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.

F7.4-4 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.

F7.4-5 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.

F7.4-6 The Space Shuttle Systems Integration Office handles all Shuttle systems except the Orbiter. Therefore, it is not a true integration office.

F7.4-7 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.

F7.4-8 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.

F7.4-9 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.

F7.4-10 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.

F7.4-11 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.

F7.4-12 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.

F7.4-13 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:

R7.5-1 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.

R7.5-2 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.

R7.5-3 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 CAB001-0010, refer to a document in the Columbia Accident Investigation Board database maintained by the Department of Justice and archived at the National Archives.

1 Sylvia Kramer, "History of NASA Safety Office from 1958-1980's," NASA History Division Record Collection, 1986, p. 1. CAIB document CAB065-0358.

2 Ralph M. Miles Jr. "Introduction." In Ralph M. Miles Jr., editor, *System Concepts: Lectures on Contemporary Approaches to Systems*, p. 1-12 (New York: John F. Wiley & Sons, 1973).

3 "The Aerospace Safety Advisory Panel, " NASA History Office, July 1, 1987, p. 1.

4 On Rodney's appointment, see *NASA Management Instruction* 1103.39, July 3, 1986, and NASA News July 8, 1986.

5 *NASA Facts*, "Brief Overview, Office of Safety, Reliability, Maintainability and Quality Assurance," circa 1987.

6 "Space Program Safety: Funding for NASA's Safety Organizations Should Be Centralized," General Accounting Office Report, NSIAD-90-187, 1990.

7 "Aerospace Safety Advisory Panel Annual Report," 1996.

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."

10 NASA Chief Engineer and NASA Integrated Action Team, "Enhancing Mission Success – A Framework for the Future," December 21, 2000.

11 The information in this section is derived from a briefing titled, "Draft Final Report of the Space Shuttle Competitive Source Task Force," July 12, 2002. Mr. Liam Sarsfield briefed this report to NASA Headquarters.

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

14 Todd R. La Porte and Paula M. Consolini, "Working in Practice but Not in Theory," *Journal of Public Administration Research and Theory*, 1 (1991) pp. 19-47.

15 Scott Sagan, *The Limits of Safety* (Princeton: Princeton University Press, 1995).

16 Dr. Diane Vaughan, 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.

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

18 Sagan, The Limits of Safety, p.258.

19 LaPorte and Consolini, "Working In Practice."

20 Notes from "NASA/Navy Benchmarking Exchange (NNBE), Interim Report, Observations & Opportunities Concerning Navy Submarine Program Safety Assurance," Joint NASA and Naval Sea Systems Command NNBE Interim Report, December 20, 2002.

21 Theodore Rockwell, *The Rickover Effect, How One Man Made a Difference*. (Annapolis, Maryland: Naval Institute Press, 1992), p. 318.

22 Rockwell, *Rickover*, p. 320.

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

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

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

26 Aerospace's Launch Verification Process and its Contribution to Titan Risk Management, Briefing given to Board, May 21, 2003, Mr. Ken Holden, General Manager, Launch Verification Division.

27 Joe Tomei, "ELV Launch Risk Assessment Briefing," 3rd Government/ Industry Mission Assurance Forum, Aerospace Corporation, September 24, 2002.

28 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).

29 Charles B. Perrow. *Normal Accidents* (New York: Basic Books, 1984).

30 A. Shenhar, "Project management style and the space shuttle program (part 2): A retrospective look," *Project Management Journal*, 23 (1), pp. 32-37.

31 Harry McDonald, "SIAT Space Shuttle Independent Assessment Team Report."

32 Ibid.

33 "Post Challenger Evaluation of Space Shuttle Risk Assessment and Management Report, National Academy Press 1988," section 5.1, pg. 40.

34 Harry McDonald, "SIAT Space Shuttle Independent Assessment Team Report."

35 NSTS-22254 Rev B.

36 Ibid.

37 GAO Report, "Survey of NASA Lessons Learned," GAO-01-1015R, September 5, 2001.

38 E. Tufte, *Beautiful Evidence* (Cheshire, CT: Graphics Press). [in press.]

39 Ibid., Edward R. Tufte, "The Cognitive Style of PowerPoint," (Cheshire, CT: Graphics Press, May 2003).

40 Ibid.