

Chapter 5. Applying the Contemporary Paradigm - *Challenger*

As with the analysis presented in Chapter 3, those employing the contemporary paradigm must answer the same two fundamental questions:

- What caused the space shuttle *Challenger* to fail?
- What were the consequences of this system failure?

In addressing these questions, we must consider the total environment, in which the shuttle program was developed, including the vehicle's design history, the management of the program, and the operational record of the shuttle fleet. This environment extends to the political pressures that NASA faced and the very public expectations for the success of the program. In addition, NASA developed and placed on itself a series of demands not mandated by external sources. For example, NASA cannot be viewed as an indivisible whole, but rather is better understood by what Allison calls the "the governmental politics model" where:

The "Leaders" who sit on top of organizations are not a monolithic group. Rather, each individual in this group is in his own right, a player in a central, competitive game. The name of the game is politics: bargaining along regularized circuits among players positioned hierarchically with the government...players who make governmental decisions not by a single, rational choice but by the pulling and hauling that is politics.³¹⁹

The contemporary analysts also take advantage of the massive amount of information available about the failure, but view it from a different perspective. There is no assumption that the way to find the answers to the cause and consequence questions is to delve into data to uncover a previously undetected aspect of the failure. This approach uses a more holistic paradigm, which rather than exclusionary, includes initially all of the data to develop a more complete picture of the failure scenario. For example, instead of attempting to determine whether management error or a design flaw caused the accident, the analysis includes both in the paradigm and seeks to determine the relative contribution of each to the system failure.

In this analysis, it is not assumed that the path to the accident is linear and deterministic. There may be no path at all, but a cloud of factors each influencing the failure in ways difficult or impossible to determine. It is fruitless to attempt to resolve whether the accident was more dependent on the presence of political pressure or on the inability of the Thiokol engineers to convince their management to recommend against launching on a very cold morning. The analysis considers these factors among others in an attempt to determine some underlying structure to the accident. Building on the classical foundation, which is linear and deterministic, this structure incorporates the nonlinear elements that influenced the accident.

Effects may propagate through a system in ways not anticipated in advance. For example, a single failure mode may be caused in part by small changes that are not captured in the failure models. In the solid rocket booster system, NASA changed vendors for the thermal putty used to protect the O-rings. Although the old and the new vendors met all of the shuttle requirements, perhaps the requirements failed to capture what was needed to keep the joint safe. This apparently simple change never was provided as feedback up the NASA chain of command. The new putty was documented to perform differently, with leaks increasing after it was introduced. Was the communication among program elements structured poorly, preventing this possible linkage from being escalated to management?

The analyst does not expect the data to reveal a single cause of the failure. There is no need to hunt for the root cause, because one does not exist. The lesson to be learned is to understand how the various causes interacted to create a situation where the accident could occur. This unique situation is studied for two reasons. First, as with the classical paradigm, the specific failure mode should be understood so that the risk of this failure can be reduced or eliminated. Few expect another shuttle accident to occur because of problems with the O-ring seals in the solid rocket booster joints. This specific problem has been corrected using classical engineering techniques.

Second, the analyst uses the contemporary paradigm to reveal, to the extent possible, the interweaving of many factors that lead to multiple causes of the *Challenger* failure. The circumstances surrounding the failure are examined from a more holistic perspective than

³¹⁹ Allison, p. 144.

employed by the classical analysts. The accident is studied for what principles it can supply us for anticipating the behavior of complex systems. This investigation may uncover clues for recognizing similar situations in the future before the system failure occurs. In this way the *Challenger* becomes a case study for how all of the classical analysts' individual causes interact. The breadth of the analysis may be illustrated by some simple examples.

Was it just the cold weather to blame? The tremendous focus on this single element overlooks many other contributors to accident. First, although the cold weather undoubtedly had an effect on the performance of the solid rocket booster joint seals, erosion had been seen at higher temperatures. The accident might have occurred even in warmer temperatures. The understanding of the system failure extends far beyond determining the minimum temperature at which it is safe to launch the vehicle. It includes determining how the situation developed to the point where such a launch would be attempted without an understanding of the risk factors involved.

What about the management crisis within Thiokol which led the company to reverse its "no go" decision at the eleventh hour? There is little doubt that the decision process was flawed and should be considered one of the causes of the accident. However, the focus for preventing future system failures should not be on the particular decision made, but on the process used to make the decision. Boisjoly illustrates this approach in his testimony before the Presidential Commission:

One of my colleagues that was in the meeting [to recommend launching] summed it up best. This was a meeting where the determination was to launch, and it was up to us to prove beyond a shadow of a doubt that it was not safe to do so. This is a total reverse to what the position usually is in a preflight conversation or a flight readiness review. It is usually exactly opposite that.³²⁰

The contemporary paradigm also does not call for a key consequence, but attempts to document the interaction among the multiple consequences that arose from the loss of the shuttle. This task does not simply list the consequences, but attempts to reconcile how each consequence came about based on the failure. For example, what makes the loss of the crew a consequence that would cripple the space agency for years? The crew, including the "guest" astronauts, was

³²⁰ Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, p. 93.

fully aware of the risks involved in launching the shuttle. They were involved in a research and development program and were lost in what was essentially an industrial accident. This particular accident was more dramatic because it was filmed, but it should be placed in proper perspective.

Wasn't the loss of the *Challenger* vehicle itself equally as significant when viewed in its impact to the national agenda? The shuttle fleet was reduced by 25 percent, severely impacting the nation's launch capability. National defense payloads had to be re-manifested on other launchers and the ability to provide critical surveillance was impacted during this period. With the decision to replace *Challenger*, the Congress was forced to appropriate almost \$3 billion in unanticipated funds over a two-year period. Other planned scientific investigations also were delayed or scrapped, creating an immeasurable loss to our economy.

After a failure such as the *Challenger* accident, the classical paradigm anticipates and sees a static world in which events unfold like the end game on a familiar chessboard. The contemporary analyst sees no such inevitability and works to understand how participants' actions could influence the outcome of the match. These actions are not a coordinated set of responses to the failure, but are based on the perspectives of the people taking them. They may alter the consequences of the failure or may interact with actions taken by others. For example, following the accident, the companies making expendable rockets renewed their call for the country to develop and maintain a mixed fleet of such rockets as an alternative to the space shuttle. Certainly these efforts had some influence in developing the national space policy restricting the types of payloads which may be flown on the shuttle. Using this approach, several questions arise about the actions of NASA in response to the accident.

Were they prepared for the accident? NASA had an extensive set of failure procedures that were executed immediately after the accident. These procedures were used to capture the data related to the accident and to preserve it for later examination. However, there was no catastrophic mishap plan in place that addressed who would lead a system-wide investigation, make statements to the press, coordinate an agency response with its contractors, and work with

other government agencies involved in the recovery effort.³²¹ This lack of preparation severely affected the quality of NASA's response and the eventual consequences of the failure.³²²

What was the response of the organization in the aftermath of the failure? NASA demonstrably was in disarray in the days following the accident. This behavior led many to question whether NASA was capable of conducting the investigation or perhaps was not telling all the facts to the American public. The Presidential Commission discusses this situation in the preface of its report:

For the first several days after the accident - possibly because of the trauma resulting from the accident - NASA appeared to be withholding information about the accident from the public. After the Commission began its work, and at its suggestion, NASA began releasing a great deal of information that helped to reassure the public that all aspects of the accident were being investigated and that the full story was being told in an orderly and thorough manner. Following the suggestion of the Commission, NASA established several teams of persons not involved in the mission 51-L launch process to support the Commission and its panels.³²³

How did NASA recover and move forward? From an engineering perspective, NASA responded thoroughly to the accident. The solid rocket booster joints were redesigned to eliminate the type of failure that occurred with the *Challenger*. The agency made several other systems changes in an attempt to lower the overall risk of the flying the shuttle. NASA's strategic moves are more difficult to gauge. The long grounding of the fleet forced rescheduling of many experiments. Some completely constructed spacecraft were placed in storage and ultimately never flew. The four planned orbiting observatories were delayed, with one ultimately canceled. Today, only one, the Hubble Space Telescope, has been launched.

The contemporary paradigm brings a structured approach to developing comprehensive answers to these questions. The factors identified in the classical paradigm are included. These include the standard analyses that determine the proximate cause of the accident, the causes that led to this proximate cause, and the various consequences that have been identified. However, absent are any judgments regarding whether one of the factors is the "correct" answer.

³²¹ Collins, p. 36

³²² Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, p. 1.

³²³ Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, p. 1.

The contemporary paradigm expands the view to take advantage of probabilistic risk analysis. These analyses take into account not only the consequences, which result from a system failure, but also the likelihood that they will occur. As with the classical paradigm, the organization focuses first on the potential failures that have the highest consequences. However, these consequences then are reconsidered in light of the probability they will occur. For example, NASA has documented the loss of an orbiter wing as a catastrophic failure resulting in the destruction of the entire vehicle and death of the crew. This failure scenario is documented as of very low likelihood. Small but unexpected cracks might appear in the wing root where it joins the fuselage. Although not considered a problem, they would be investigated to determine why they appeared in the first place. The contemporary organization would accept this finding, but would devote a portion of its energy searching for changes in the way the wing performed or was maintained to look for unknown issues,

The new paradigms also considers factors which are difficult to measure. In these cases, the factors may not be observable directly, but they can be detected through the effects they create. For example, components in the complex shuttle thermal system may create unanticipated “hot spots” in some areas of the shuttle and their existence only surfaces in a rise in overall temperature in the cooling system. In the management arena, changes in managers and organizational structure have a bearing on the probability that a failure will occur. However, this bearing cannot be reduced to simple measurements.

Finally it provides a glimpse into how students and practitioners would benefit from incorporating the contemporary concepts into their work. This paradigm provides the rudimentary structure for managing a complex system, which will never exhibit the stability, required by the classical paradigm. This structure acknowledges the factors affecting system performance that may never be quantifiable and illustrates how the system risks can be managed despite this lack of knowledge.

5.1 It's the O-Rings Dummy.... Or Was It?

There is little, if any doubt that the O-rings failed and destroyed the seal in the solid rocket booster. The failed seal triggered the destruction of the *Challenger*. This conclusion was

reached only after considering a number of alternative causes. The Presidential Commission investigated whether the shuttle external tank had been destroyed by an accidental detonation of the range safety system which ignited the propellants in the hydrogen and oxygen tanks. Another possibility was a flaw in the tank structure that caused it to fail. Nothing was found to indicate the tank played any role in causing the failure. The shuttle main engines were retrieved and examined to ensure all three were operating properly when they were shut down. The orbiter itself and the payloads were analyzed to determine if there was any possible failure that could have created the accident. The Presidential Commission concluded that the solid rockets were at fault:

In view of these findings, the Commission concluded that the cause of the *Challenger* accident was the failure of the pressure seal in the aft field joint of the right solid rocket motor.³²⁴

Can we really be one hundred percent sure, however, that the O-rings failed because of cold weather? What most analysts do not realize or fail to forget is that the Presidential Commission never drew a direct correlation between the cold temperatures and the failure of the O-rings. Although the Presidential Commission devotes several pages (Figures 5-1, 5-2) to the cold weather and asserts “O-ring resiliency is directly related to its temperature,” the implication being that this was the proximate cause, the Commission actually stops short of naming this as the proximate cause. Instead the Presidential Commission hedges in concluding temperature was the only contributor, stating “As a result it is probable [emphasis added] that the O-rings in the right solid booster aft field joint were not following the opening of the gap between the tang and clevis at time of ignition.”³²⁵

³²⁴ Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, p. 72.

³²⁵ Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, p. 71.



Above, Shuttle 51-L on Kennedy Space Center Pad 39B in the early morning of launch day. Temperatures were well below freezing, as indicated by the lower left photo, which shows thick ice in a water trough despite use of an anti-freeze solution.

Figure 5-1 - Early Morning of Launch Day³²⁶

³²⁶ Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, pp. 112.



Figure 5-2 - Foot-long Icicles on Fixed Service Structure³²⁷

The Commission stopped short of concluding that the seal failure was directly related to temperature. Instead, they identify a number of factors that could have contributed to the failure:

The failure was due to a faulty design unacceptably sensitive to a number of factors. These factors were the effects of temperature, physical dimensions, the character of materials, the effects of reusability, processing, and the reaction of the joints to dynamic loading.³²⁸

Although temperature receives virtually all the attention in the classical literature on cause of the accident, these other factors are of great importance to understanding how the failure developed and to construct a paradigm of how the factors interacted. For example, some have speculated that the *Challenger's* O-rings may have damaged during assembly at the Kennedy Space Center.³²⁹ The O-rings are impossible to inspect directly after they have been installed. The Presidential Commission points out that the two solid rocket booster segments abutting the joint that failed had been flown on past missions. These segments were considerably out-of-round, affecting the gap in the joint that the O-rings would have to seal.³³⁰ Following assembly, the joint was tested using a standard test procedure. Although the seals passed the leak test, these tests may have failed to detect improperly installed O-rings. The seals could have passed the test because the putty that was also in the joint temporarily kept them in place or the out-of-round condition of the segments held the seals in place under test conditions.

Other analysts contend the O-rings leaked at solid rocket booster ignition but sealed again until later in the flight.³³¹ Tufte, for example, asserts the initial leak that occurred at solid rocket booster ignition lasted only two seconds and was plugged by the putty or other insulation. Only later, at approximately a minute into the flight did the flames become visible as the solid rocket booster casing was breached.

Although the cold temperature is cited frequently as the critical weather element on that January day, it was not the only departure from the typical Florida environment. The seas were incredibly rough from the winter storm that had moved through the Cocoa Beach area.

³²⁷ Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, pp. 113.

³²⁸ Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, p. 72.

³²⁹ Collins, p. 236.

³³⁰ Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, p. 70.

Operations personnel voiced concerns that the sea condition would prevent the recovery ships from snaring the solid rocket boosters. If this occurred, the boosters would sink and be lost to the program. NASA managers discussed this concern during preflight briefings on the weather in the area. The discussion, however, did not extend to looking at the various weather conditions as part of a larger issue. Using the contemporary paradigm, these conditions would be seen as the visible components of a problem that might have other, less visible, aspects. In fact, prelaunch inspection teams did not measure the temperature of the solid rocket boosters because it was not a part of mandated procedures. No one thought to step back and look at the bigger picture. The decision still may have been to launch, but the managers would have recognized the uncertainty introduced by these never before experienced conditions.

The same storm brought high winds and unusual wind patterns in the launch area. Telemetry data transmitted from the shuttle computers prior to the explosion indicate that the vehicle encountered the highest winds aloft ever experienced by a shuttle in the program's history. Some analysts attribute the reappearance of the smoke from the burning O-rings late in the flight to the flexing of the multistory solid rocket boosters in the blustery winds. McConnell provides a graphic description of this possibility:

Challenger slammed through the most violent wind ever encountered on a space shuttle mission. To keep the vehicle's mass aligned with the flight vector and reduce aerodynamic stress, the shuttle's computers issued an almost continuous stream of commands to the Orbiter's aerosurfaces and the gimballed nozzles of the main engines and of the solid rocket boosters...The jolting stress of these aerodynamic forces [when the joint failed] was the final sinister element in the evolution of the accident. Had there been no high-altitude wind shear, the field joint might have maintained its precarious seal all the way to booster burnout.³³²

Post-failure analyses show conclusively that the O-rings did not perform as anticipated in the presence of cold temperatures. A chart of the seal erosion and blow-by for each flight plotted against temperature clearly indicate a correlation between temperature and blow-by (Figure 5-3). The correlation, however, is not 100 percent. Three missions experience leaks at temperatures solidly within the normal launch constraints. These analyses do not tell us how cold it would

³³¹ Tufte, p. 16.

³³² McConnell, p. 243.

have to be before they would not seal sufficiently to allow the boosters to burn for the required 2¼ minutes.

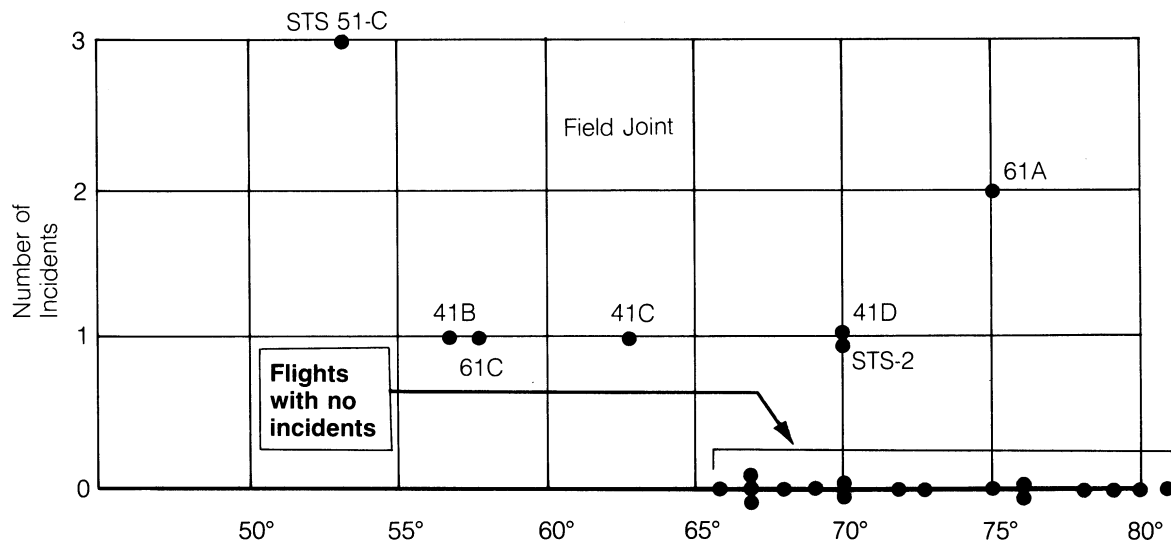


Figure 5-3 - Plot of flights with and without incidents of O-ring thermal distress³³³

Apparently, temperature was not the only factor at work here. Even in the extremely cold weather, the seal did not fail until over a minute into the flight. The O-ring performance may have been affected by all of the factors above and the vehicle might have survived if only one had been absent.

5.2 With Complexity, Delays, and Politics -- How Do We Isolate the Cause?

The story begins with the inception of the space shuttle program. It is the early 1970's and NASA is trying to salvage its human space flight program by identifying a new goal, one that will build on the technical knowledge of the Apollo program. The proposed costs for continuing solar system exploration, building an orbiting space station, and developing a space shuttle continue to rise. When budgetary constraints force NASA to abandon or delay other programs and concentrate on the shuttle, agency managers recognize the days of unlimited funding as seen

³³³ Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, p. 146.

in Apollo are a thing of the past. They turn then to focus on translating human space flights from newsworthy events into a routine part of scientific research and long distance transportation.

NASA recognized that no long-term program could continue to throw away the entire spacecraft after one use. But the problems of reusability were enormous. Developing such a craft required a completely different engineering approach from that used for the Apollo program. The earlier programs had been built on very high reliability systems, but with short operational lifetimes. The high reliable systems frequently were custom and sometimes hand built. They were produced in very small numbers with few requirements for spare parts. The short operational life of these systems was in part created by this reliability. They could be guaranteed to work within a specified time period but were not suitable for frequent long-term use. Any high use vehicle such as the shuttle would require systems with long operational lifetimes to reduce maintenance and to ensure a reliable schedule.

Previous vehicles had been made to carry no more than three passengers, with no cargo, existing in primitive conditions for less than a week. The interior of the Apollo spacecraft was about the size of small walk-in closet. It had no toilet facilities, no food preparation capability, and very little storage area. What little room was available was consumed with provisions to support the crew during the flight to and from the Moon. To perform its mission, the shuttle would be required to stay in orbit over two weeks as the crew of up to seven people carried out experiments. The shuttle would have to include not only crew provisions, but have storage for the experiments and any samples they produced. A primary purpose of the shuttle was to deliver satellites to Earth orbit. To provide this capability at a reasonable cost and to meet the Department of Defense requirements, the shuttle payload bay had to be large enough for 40,000 pound, 40-50 foot satellites.

The Apollo crew had to be in excellent physical health and meet strict constraints. These requirements would be impractical for a four shuttle fleet flying dozens of missions each year. The training requirements for Apollo crews spanned years of work in expensive simulators and in one-on-one instruction. This approach would be too costly for shuttle. Also, shuttle missions would require, in addition to pilots, scientific researchers with specialized knowledge in areas

such as biochemistry, astronomy, and semiconductor technology. These areas were not widely represented in the astronaut core at the outset of the shuttle program.

This newer spacecraft would have to be capable of landing on the ground instead of in the ocean, creating new difficulties. Precise landings would be required because NASA could no longer take advantage of the large expanses of water. Several designs were considered, including supplying the shuttle with air-breathing jet engines (in addition to its rocket engines) to allow it to “wave off” for multiple landing attempts. This approach was abandoned after pilots demonstrated that a glider approach provided sufficient margins of safety. The large size of the shuttle, which could not fly on its own, greatly limited the options for landing sites. NASA ultimately modified a Boeing 747 to return the shuttles from other landing sites should a contingency landing be required. However, this capability was not planned for the average mission because it interfered with the schedule for preparing the shuttle for its next flight. Also, the flight aboard the Boeing 747 introduced additional risk as the carrier aircraft could crash even on a routine ferry mission.

With more frequent flights, the operations could not rely on a massive work force to support landing operations. During the Apollo program, NASA maintained divisions of personnel dedicated to planning and executing landings of the spacecraft. In addition, the U.S. Navy deployed small fleets of aircraft carriers, destroyers, and support craft to pluck the astronauts and their capsules from the water. None of these would be required for the shuttle, but landing on a runway did not solve this issue completely. These were still amazingly complex vehicles with complicated and sometimes hazardous systems requiring significant handling.

The large sizes proposed for the new shuttle created problems in aerodynamic heating on reentry never faced before. The cone shaped Apollo spacecraft re-entered the atmosphere with the blunt end facing toward the ground. As the protective heat shield absorbed the friction from the atmosphere, it would ablate or slough off carrying the heat with it. This approach was not feasible with the shuttle for two reasons. First, this system would be too heavy for this large 250,000-pound spacecraft. Second, the ablative system was an on-time use system and would have to be replaced after each mission. NASA had to design a reusable system capable of protecting the equivalent of a DC-9 re-entering the atmosphere at 15,000 miles per hour.

To meet these challenges, NASA called on its most senior engineer, Maxime (Max) Faget. Universally recognized as the premier spacecraft design engineer in the world, Faget began his career with the National Advisory Committee for Aeronautics, NASA's predecessor. He had worked with aircraft and space vehicles his entire life and been a principal player in every human capable spacecraft NASA ever launched. He designed and held the patents on the Gemini and Apollo spacecraft.

Faget assembled a team of experienced engineers from across the NASA field centers. By the time the shuttle program began, each of these centers had developed specific areas of expertise that would be needed in the new program. The Kennedy Space Center would serve as the launch and now the landing area, and would prepare the vehicles for their next missions. The Johnson Space Center would manage the development of the orbiter, provide mission operations, and continue to act as the base for astronaut training. The Marshall Space Flight Center would design and develop the propulsion systems.

Recognizing that this system would be different from any previous space effort, Faget went to the airline industry to learn about reusability and "turnaround" of flying vehicles. He found airline operations to be quite different from NASA's current flight approach. While NASA exhaustively tested each system before a mission, airline officials explained that they tested only certain systems each flight with the remainder checked on a prescribed schedule. This approach significantly reduced the time required for flight processing, permitting airlines to fly a vehicle very quickly after its last flight. Faget recognized that the shuttle was a more complex vehicle than a commercial aircraft, but he incorporated the airlines' overall approach into the shuttle operations and planning. Early manifests show the same shuttle vehicle flying more than once a month.

Most of all, Faget followed one of his personal mandates, "Keep it as simple as possible with the fewest number of parts to break."³³⁴ As with any engineering design, there were many options for meeting the requirements levied on the shuttle systems. In previous space flight programs, the designers had had the luxury of developing competing designs to the prototype and sometimes flight ready stages before choosing which to incorporate in the final vehicle. The

³³⁴Interview, Johnson Space Center Oral History Project, 19 August 1998, NOH-OHP-30

interdependency of shuttle systems and funding precluded this approach. Building on his experience, Faget reduced system complexity as much as possible. For example, in selecting which of two designs to use for the small maneuvering rocket system, he opted for the design that did not require separate boost pumps to maintain fuel pressure. The design incorporating the pumps had performed well in tests, but it had more moving parts providing more opportunities for one to fail.

Unlike the previous programs, the shuttle program had to operate within a specified budget. This change in procedure for NASA has been cited as a major stumbling block in shuttle development. The argument is that without an unlimited budget, NASA (or any organization) could not develop a safe spacecraft absent unlimited funding. In reality the budget constraints, although affecting the final design, were simply another parameter to be considered by the management team. As experienced research and development professionals, the group was accustomed to working within budget parameters. This program was no different from other programs in this regard. For example, aircraft manufacturers establish a development budget for all new air frames to be introduced into either the commercial or the defense market. Compromises have been made on every aircraft ever built.

The budget constraint eliminated the flyback booster originally intended to lift the shuttle most of the way into space, replacing it with the expendable external tank and shuttle-mounted main engines that would be returned. At the time this decision was made, NASA acknowledged that this approach would increase the operational cost of the shuttle program. However, it lowered development costs and helped keep the program within the specified funding profile. The design change never was considered an increase in the overall system risk. In fact, some of those involved saw the new design as less risky because it incorporated fewer new elements in a design which already involved several “first time” elements.

Similarly, budget constraints were not the only factor in the decision to use solid rocket boosters instead of other options. This decision epitomizes the complex interactions of factors in engineering design. Each factor had to be weighed against other factors with no common unit of measurement to compare the relative weight of each. Was it more important to save \$10 million dollars during the design phase or \$100 million over the operational life of the vehicle?

It is true that solid boosters had never been used on a spacecraft carrying people, but this team had a history of doing things never before done. When they started, no one had ever flown in space before. Gunther Wendt, who managed the launch complex operations at the Kennedy Space Center, since the earliest days of NASA beginning with the first American launches using chimpanzees as substitutes for astronauts, today laughs at the idea that the shuttle was an untried design. He explains that everything involving human space flight operations was a new idea at some time over the last 36 years. The approach has been to understand the design, acknowledge its risks, and plan for dealing with failures. When no more risks can be identified and the overall risk level is deemed acceptable, Wendt declares “it is time to launch and pray you haven’t missed anything.”³³⁵

The solid rocket alternative, liquid fueled boosters, were viewed as potentially less costly. Shuttle boosters were to be based on the reliable design used in the Titan III rocket. Large solid rocket boosters had an excellent flight record. The Titan boosters had never failed in flight. Other systems, including Department of Defense rockets had flown very successfully and the using solid boosters. The shuttle boosters would be larger than any built to date, so NASA and Morton Thiokol added a second O-ring seal to provide redundancy in the solid rocket booster joints. By building on the operational Titan booster, the systems could be adapted for shuttle without a full design effort.

In addition, the alternative liquid boosters would require more complicated systems than those used in solid rocket boosters. Liquid boosters have pumps to transport the fuel to the engines, pressurization systems to force the fuel to the pumps, and systems to maintain the proper temperature within the tanks. Solid rocket boosters have none of these. Finally, with the attempt by NASA to reuse as many components as possible, solid rocket boosters simply were more suitable choice.

The scenario was that after the boosters had separated from the shuttle’s external tank, they descended under parachute into the Atlantic Ocean. They would float in the water until snared by NASA ships designed for this purpose, and be towed into port at the Cape Canaveral Air Force Station (Figures 5-4, 5-5). The solid rocket booster design was ideally matched to this

³³⁵ Interview, Johnson Space Center Oral History Project, 23 January 1998, NOH-OHP-14.

approach. With very few mechanical systems, the boosters were only marginally affected by their immersion in salt water. The many mechanical parts in liquid boosters made them unsuitable for salt-water landing and recovery as planned for the shuttle program.

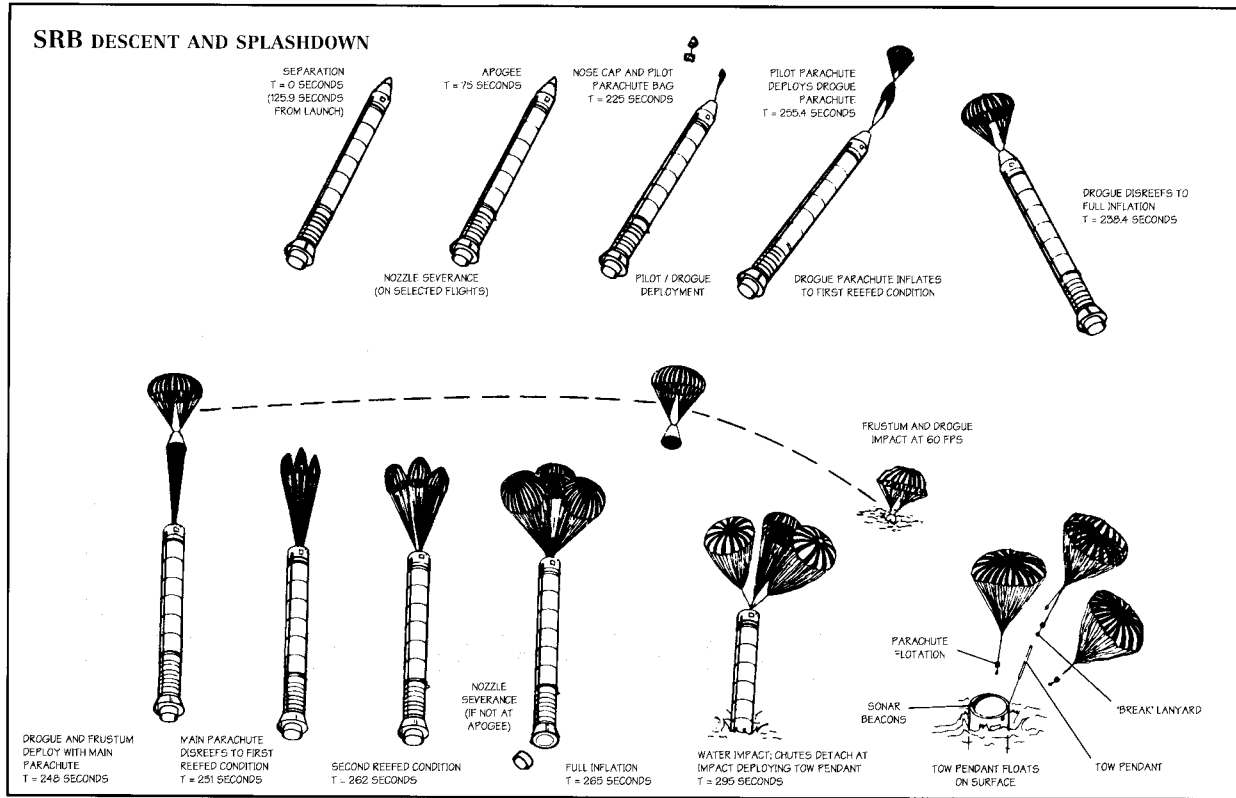


Figure 5-4 - solid rocket booster Descent and Splashdown³³⁶

³³⁶ Jenkins, p. 252



Figure 5-5 - Retrieval of solid rocket booster from STS-26-R³³⁷

The solid rocket boosters as well as the rest of the new space shuttle design encountered the typical design problems, but these issues were handled within the strict NASA design control process. This process, developed over twenty years of experience, was directed specifically at controlling all elements of knowledge within the program. The agency recognized from the outset the risk of what was already a risky business could be lowered by ensuring all personnel had access to issues, past or present, affecting the overall vehicle. In this environment, the issues received maximum exposure and people across the program were able to apply their expertise for developing resolutions to the problem. This process allowed no issue to be inadvertently dropped from consideration. Each issue was placed in a database which tracked it until it was resolved, and which alerted management to issues that had not been closed for extended periods of time.

External safety oversight committees monitored NASA's actions to ensure no shortcuts were taken. Following the Apollo fire, the President established the Aerospace Safety Advisory Panel whose task was to provide an independent audit of NASA activities. The panel's reports were forwarded directly to the President and NASA was required to respond promptly to any issues in a similar report to the White House. In addition to this targeted panel, NASA was

subject to frequent external analyses from the executive and legislative branches of government. The General Accounting Office investigated NASA budget estimates, operational projections, and contracting policies. The congressional committees authorizing and appropriating the NASA budget submitted numerous requests for data on shuttle development and the progress of the program. In addition, the NASA administrator and senior managers testified before the committees during the annual budget process.

Recognizing the scope of the shuttle development effort, NASA modified its safety system to place the safety personnel within each organization. First, the designated safety personnel became part of the operational team and were placed close to the work. Much of the knowledge transfer within any engineering organization occurs informally among colleagues. Early indications of a problem may surface during everyday activities. As an integrated member of the team, the safety representative would be called upon as a matter of course to participate in the problem's solution. Second, NASA managers thought that without a formal external watchdog, all employees would develop a heightened responsibility for safe flight. No one would assume that the quality control personnel would catch mistakes. If it worked, they received the credit. If it did not work, they would be asked to explain. Fritz von Bun, an engineer working for NASA, explaining this concept told the following story:

A German colleague developed several instruments to be flown aboard the spacecraft. He delivered them to NASA that subjected the instruments to numerous quality control checks. They all passed. When the NASA project manager expressed surprise at the result, my colleague was indignant, "Of course they work, did you think I would send you something that was broken?"³³⁸

When the shuttle began to fly and the O-rings exhibited unusual behavior, NASA aggressively looked into the problem. During development, NASA ordered additional testing and considered changing the design to clamp the tang and clevis together at each joint. Although concerned about the initial blow-by on the second shuttle mission, the agency recognized that this small amount of erosion did not present a significant risk to mission safety. This issue did not rate any discussion at the Flight Readiness Review for the third mission. As the erosion began to occur on later missions, the level of attention increased. The problem, already being

³³⁷ Jenks, p. 252.

³³⁸ Interview, 12 April 1988.

tracked in the NASA anomaly system, acquired a large file in the documentation system, and was reported up the chain of command.

NASA managers launched investigations into the anomaly, created a test program to better understand it, and consulted with O-ring experts across the country. They recognized that the phenomenon they saw had not been expected and could not be explained easily. The internal NASA experts at the Marshall Space Flight Center and the Morton Thiokol contractors made several changes to the solid rocket booster assembly and test sequence in attempts to resolve the issue. Thermal putty application was modified to provide a better barrier against hot gases reaching the O-rings. The pressure used to test the joint integrity was increased to ensure there were no leaks. The external experts, while explaining that this was an O-ring application beyond conventional engineering techniques, provided limited advice.

In complete compliance with the NASA safety and mission assurance hazard control program, each step was carefully documented in the system. As the engineering team developed new methods for dealing with the seal erosion, procedures were modified to meet the new requirement and rationale for each change was documented. All changes were elevated to management as required by the procedures. All NASA and contractor employees had the opportunity to voice their opinion. Numerous management and engineering meetings were conducted across the country via teleconferences with any employee welcome to attend. The room where each meeting was held as well as the entire "net" was polled for input to the discussion.

On the operational side, NASA maintained its long-standing tradition that anyone can raise a flag and stop a launch. This approach was tempered by the maxim that you are "go unless you believe you are not." Concerns about risks always are present in any launch. To stop the countdown, an individual had to provide data that brought new light to the situation. All knew the existing risks but welcomed insight that might affect the launch decision. If a person thought their opinion was not receiving the necessary attention, he or she had many avenues to elevate the issue. In addition, anonymous methods were available for reporting concerns.

The preparation for STS-51L, the last flight of the *Challenger*, was treated in exactly the same manner as the previous twenty-four flights. With a few minor training and flight timeline

exceptions, the mission followed the standard preparation template. The orbiter had no outstanding problems that had not been documented as acceptable. The external tank was manufactured and accepted as another in a series of identical articles. The solid rocket boosters had been verified, with many of their components having been used on previous missions.

There were safety-of-flight concerns raised for a number of systems. These issues arose for each mission, and all were dealt with before the launch decision was made. This typical situation developed because of the complexity of the shuttle system. Given the large number of parts, management provided a forum for discussing problems that occurred near the time of launch as well as any residual issues from past flights. This approach gave all involved a clear picture of the vehicle which would be launched, including any non-standard configurations. All had the opportunity to question how this configuration might produce unanticipated results.

Given the unusual weather, NASA closely examined all of its constraints to ensure that the cold temperature would violate none. Much of the attention centered around the ice that had formed on the launch pad. It was feared that the ice could loosen during launch and damage the fragile shuttle thermal tiles. Also, the concern was raised that the ice would affect the performance of launch pad systems. No member of the senior management team identified the solid rocket boosters as an element of risk.

Although it is well known today that the night before the launch a debate raged over the solid rocket booster O-rings, even this issue was resolved in accordance with procedures. Initially, the topic was discussed informally among NASA and Morton Thiokol managers. They decided the issue should become a part of the formal launch decision process. Several meetings were convened where often-heated discussions allowed all participants to voice their opinions. In the end, Thiokol agreed to the launch. NASA documented their agreement using its Certification of Flight Readiness process. All parties signed the certificate that there was no reason not to launch. No individuals exercised their privilege to escalate the issue to higher authority. Although the Thiokol engineers did not agree with their managers, Boisjoly recognized the managers' prerogative to make the decision in his testimony to the Presidential Commission:

I must emphasize, I had my say, and I never [would] take [away] any management right to take the input of an engineer and then make a decision

based upon that input, and I truly believe that, and so there was no point in me doing anything any further than I had already attempted to do.³³⁹

5.3 So What Went Wrong?

In the classical paradigm, the possible causes of the *Challenger* failure are grouped into five hypotheses. Each of these, from the lack of adequate funding to the claim of political pressure, has some merit in any analysis of the accident. Also, each is correct to some extent. NASA did have to function within a funding profile for the first time in human space flight history. There is evidence of groupthink within the NASA culture. The safety program had been modified between the Apollo and shuttle programs. The management processes should have seen the problem with the O-rings sooner, certainly before a catastrophic failure. NASA perceived, maybe incorrectly, that there was political or other external pressure to launch the mission.

However, this grouping of multiple factors into not one, but five hypotheses, indicates that a single root cause is a fictional creature. Attempts to diminish or discredit any hypothesis represent a narrowing of the universe of ideas concerning the cause of the failure. While it is acknowledged that data must be sorted into categories to bring about any structured understanding, this paring of the data set eliminates key elements in the search. The very elements discarded may at first appear unimportant, and only recognized as the entire puzzle is assembled. Also, there is no need to begin to narrow the database when widening it may provide a more complete picture of the failure. This approach may be more cumbersome, but complex systems require sophisticated methods of analysis.

The contemporary paradigm acknowledges the complexity of a system such as the space shuttle Program and is structured to accommodate it. There is no preconceived judgment that one piece of data is relevant and another is not. The paradigm incorporates the overwhelming documentation of the shuttle system prepared by NASA and its contractors as well as the literature and popular press written about NASA, the shuttle, and related topics. Even when the data set is not complete, it may play a part in understanding the risk of system failure.

³³⁹ Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, p. 93.

In fact, the contemporary analyst returns to the basic principles of physics to understand the elements leading to the failure. Rather than rejecting any data, they are included until it is proven that they are of no value. The principle that all parameters will be considered influential until they are an order of magnitude smaller in value than the predominant parameter is applied to the data. In doing so, Newtonian physics provides a first sort of the data into the known and the unknown. The analyst is left with an understanding of what data is available for the known data set, and what is not known or available, the unknown. The analyst may seek the unknown data to add to the analysis, or may acknowledge its absence.

The contemporary analyst does not discard the classical root cause analysis, instead using it to create a more complete picture of the *Challenger* failure. In itself, the fact that many analysts have identified the hypotheses indicates that there probably is some validity to each. The complexity of the vehicle itself makes it unlikely that any single aspect of the design alone created the failure. The design decisions may now appear flawed, but their development represents a logical approach to creating a new spacecraft. Management changes made since the Apollo program, including those in the safety program, highlight areas which should be examined closely. The same is true for the political pressures NASA faced for the first time. Having lost its Cold War mandate, the agency found itself in unfamiliar territory. However, these hypotheses do not have to be viewed as competing to determine who “wins” the argument.

Beginning with the identification of possible failure scenarios, the contemporary organization first would consider their completeness from a classical frame of reference. Once satisfied that these analyses were complete, the organization would assess the probability of occurrence for each. The competing solutions would be regarded, individually and in combinations, as clues in this search for some effect, perhaps small, which interacted with other factors to generate the feedback that contributed to the accident. Such effects could be found, for example, in the structure of NASA’s problem reporting system. Renowned for its ability to accurately track any anomaly, this system may have had an unanticipated effect. The managers had so much faith in the system that they did not consider that the system itself could interfere with communications to the point where O-ring problems remained in routine decision processes. Finally, the contemporary organization would always remember the impossibility of a perfect list

of identified possible failure scenarios and watch for perhaps subtle changes in behavior of the systems or the organization.

The organizing concepts of the contemporary paradigm provide a structure for a coordinated rather than competing set of hypotheses. Using this approach, the data concerning the *Challenger* accident takes on a different meaning than when considered in isolation. Each contributing element is considered individually while at the same time viewed as an element to be placed into a larger overall framework. Even the act of constructing the framework provides additional data. If a given piece of information, such as the process for determining acceptable weather conditions when the written procedures provide no guidance, has no place in the existing framework the data are not discarded. Instead, the framework is studied to determine how it should be altered to accommodate this new information. Rather than this situation being considered an issue, the new data may require that the framework be altered.

The technical aspects and policy considerations are viewed as contributing to the failure together, not separately. The barriers typically placed in the classical paradigm to isolate one field of study from another are discarded. Not only are technical and policy issues, as fields of study combined in a single analysis, particular specialties within each field should be also viewed as interrelated elements. Using *Challenger* as an example, one can start with engineering as the field of study in the technical area. Engineering may be divided into disciplines such as structures, electronics, and thermodynamics. As part of the shuttle accident, thermodynamics plays a large part in the study of the system failure. The policy analysts look to the management, political, and ethical aspects of the accident. Any of these factors may be considered in conjunction with a second, third or more in combination. Rather than sift through the data looking for a cause, the analyst starts with the initial known facts and builds the structure for understanding the causes that led to the accident. Although the resulting structure may not be pictured visibly in a three-dimensional matrix, a multidimensional view may provide the most accurate representation of the accident. Why not look at the factors as pieces of a puzzle, rather than separate smaller puzzles?

Given the consequences of the respective failures may be well documented, the contemporary organization would consider in depth the probability that each failure would occur.

No organization has the resources to consider each consequence to an equal depth, and consequently must eliminate some from further consideration. Using a prior example, the consequences from losing an orbiter wing are catastrophic. However, if all wing components and associated operations remain unchanged, the likelihood that the wing will fail is very low. Efforts would be concentrated on other factors that have a higher likelihood of contributing to a system failure. Such factors may be divided into two categories. First are those factors that are known to have a high consequence and also known to be more likely to occur. The high energy shuttle main engines are representative of this category. Second are those factors which are not viewed necessarily as of high consequence and high likelihood, but which are likely to contribute to a failure. Prior to an accident, no classical analyst would view the NASA decision board structure as a contributor. A contemporary analyst would consider this structure, although not necessarily know the degree to which it contributed to the likelihood of a failure.

In this new view, all of the hypotheses contain elements that contribute to the failure. The alternative, employed with the contemporary paradigm, is to use the data to develop clues for creating a picture of the failure. In this particular case, it can be illustrated how NASA and its contractors could have behaved differently. Starting from the beginning of the program, NASA could have chosen an alternative configuration that did not include solid rocket boosters. The agency could have given more weight in the decision process to liquid fueled boosters which could be shut down in flight if a problem developed. A different contractor for the boosters might have used another design for the joints that did not introduce the seal problems found in the Morton Thiokol rocket. The NASA safety program used in the Apollo program could have been kept in place for the shuttle program. Practically every decision made in shuttle design and development might have had some impact.

Even so, this changed behavior may not have prevented the accident, but it would have reduced the probability the accident would occur. There is little doubt that a different management reporting structure would have altered the decision process to launch the *Challenger*. The controversy over the O-rings never was elevated to top-level NASA management, even during pre-launch discussions on the effects of the frigid temperatures. If the topic had been raised, the decision might have gone the other way. In testimony before the Presidential Commission, Arnold Aldrich, NSTS Program Director, testified that he had never

been informed of the solid rocket booster seal teleconferences and the arguments surrounding the safety of flight. He indicated that they would have had a strong influence on his decision making process.³⁴⁰ As Figure 5-6 shows top management testified at the Presidential Commission hearings that they simply were not aware of the O-ring problems.

<i>NASA Official</i>	<i>Position</i>	<i>Description of Awareness of O-Ring Problems</i>
John Young	Chief, Astronaut Office	"The secret seal, which no one that we know knew about." ⁹³
Milton Silveira	Chief Engineer	". . . If I had known . . . I'm sure in the '82 time period when we first came to that conclusion [that the seal was not redundant], I would have insisted that we get busy right now on a design change and also look for any temporary fix we could do to improve the operation of the seal." ⁹⁴
James Beggs	(Former) NASA Administrator	"I had no specific concerns with the joint, the O-rings or the putty. . . ." ⁹⁵
Arnold Aldrich	Manager, National Space Transportation System	None were aware of Thiokol's concern about negative effect of cold temperature on O-ring performance, nor were they informed of the same concern raised after STS 51-C. ⁹⁶
Jesse Moore	(Former) Associate Administrator for Space Flight	
Richard Smith	Director, Kennedy Space Center	
James A. Thomas	Deputy Director, Kennedy Launch and Landing Operations	

Figure 5-6 - The people who did not know³⁴¹

In the first departure from the classical paradigm, a NASA organization employing the contemporary paradigm would have used a broader systems approach to take these elements and develop a more comprehensive lens. This approach looks across the complex systems as well as delving into each system. The methodology employed by NASA performs this function to a limited extent. NASA performs multiple analyses intend to identify any interactions among systems. Technically, systems are examined to uncover unexpected impacts on one system

³⁴⁰ Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, p. 91.

created by the performance of another system. This well documented phenomenon, labeled “sneak circuits” in electrical engineering, becomes part of the record in the NASA hazard analysis process. The effects help the involved personnel develop corrections for critical systems, flight rules, and operational processes.

Looking for hidden or unexpected linkages among systems, the analyst deals with the basic facts without prejudging whether they are the primary element in a failure. This approach differs fundamentally from the current NASA approach described above. In the NASA methodology, each factor is weighed for its visible potential contribution to the failure. Each factor is assigned a relative influence to be included into the overall calculation regarding the risk to the vehicle. Unproved allegations are considered just that, unproved, and have no place in the analysis. In the contemporary analysis, elements that appear to bear on the failure, but which cannot be quantified immediately or whose impacts is certain but cannot easily be measured, are included. The difficulty in dealing with a factor is not a reason for discarding it. For example, the Three Mile Island failure had an impact on the public perception of the safety of nuclear power. However, the effect of this perception on legislation regulating this industry is difficult to gauge. The regulations may have come about without the accident, but it is hard to determine the relative contribution of public opinion. These systems are complex, and unfortunately so are the methods that are used to understand them.

Using this approach, the *Challenger* failure described above takes on an entirely different appearance. Did the cold weather contribute to the accident? Of course. NASA was operating far outside its experience base. No spacecraft had ever been launched within the U.S. at these temperatures. The systems had been designed to operate in a temperate launch environment. Cold weather did not necessarily preclude a launch, but it was not part of the system requirements. Russia, on-the-other-hand, routinely launches at the Baikonur Cosmodrome, Kazakhstan, in sub-zero temperatures. Their systems, however, were designed to operate in this environment. NASA had little experience in how the cold weather affected performance. The lack of restrictions on launching in this colder environment may have been due in part to the fact that NASA considered freezing temperatures in Florida a small probability event and as such did not address it in its documented processes and procedures.

³⁴¹ Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, p. 135.

Had NASA made engineering decisions that motivated by funding or schedule or policy affected the final design of the shuttle? The question here is who doesn't make these decisions when designing a system. Trade-offs are a necessary part of any design. Petroski describes the situation eloquently:³⁴²

The choices of design are ultimately the choices of life. While the engineer can pursue on paper two or even many different designs that fulfill the requirements of a projected structure, in the last analysis only one design can be chosen to be built, just as, finally, only one route can be taken on a single trip from Chicago to New York no matter how many are considered in the planning. Deciding which paper design will be cast in concrete presents the designer or the selection committee with a problem not unlike that faced by Robert Frost:

*Two roads diverged in a yellow wood,
And sorry I could not travel both
And be one traveler, long I stood
And looked down one as far as I could
To where it bent in the undergrowth;*

Were the operational procedures followed with too many rigors to the point where people forgot that they were just documents? Absolutely, and this is where the contemporary approach illustrates its value. The NASA managers followed the procedures to a fault; managers executed every step with each being checked for completion and for accuracy. Herein lies the problem. No one stepped back to ask if the procedures were sound in this new environment.

The identification of precursor elements is fundamental to the contemporary equation and may have gone a long way toward preventing the *Challenger* failure. The most obvious example here is the erosion in the O-rings during the 24 flights that preceded the accident. The engineers were well aware of the correlation between O-ring resiliency and temperature. Likewise, the burn-through of the primary O-rings and effects on the secondary seal was well documented. NASA, their contractors, and their external experts concentrated on correcting the erosion problem. The parties employed all their engineering expertise to uncover the cause of the unanticipated problems and to pursue a solution. Each effort was directed at maintaining flight safety and assuring that the O-rings would perform as intended. The checks and balances system ensured that each individual flight system was ready for a mission. But it did not consider

³⁴² Petroski, pp. 73-74.

whether it had an effect on other aspects of the mission that were unintended. For example, NASA was so concerned about O-ring seal leakage that procedures were changed to increase the pressure in the seal leak test. This test was intended to demonstrate the integrity of the seal, but it also had an unintended effect of creating holes in the putty providing thermal insulation of the seal. No one put two and two together.

Through the formal waiver process, NASA documented all deviations from these procedures. Although the paper trail for *Challenger* is impeccable, mechanisms were not in place to force an across-the-board look similar to that given to each system. However, the process did not consider that the weather, the systems design, the past flight experience, and the limits of systems knowledge should be considered together. The narrow focus, although performing an excellent task of identifying the individual issues, does little to question the basis on which the procedures were built.

How would NASA have behaved differently using the contemporary paradigm? First, it would have recognized that the situation presented innumerable factors that had never been included in any analysis. The data base for low temperature missions was limited. The procedures were not designed to detect problems in these weather conditions. NASA used its limited data to make mission critical decisions without stepping back to consider whether the agency's actions encompassed the full universe of possibilities.

One of the findings of the Presidential Commission is that the data were there regarding the cold temperature's effects on the O-rings for anyone to examine. The Presidential Commission and later analysts have illustrated that the identical data elements could have been arranged differently to highlight the temperature sensitivity of the joint seals. Although the agency followed standard engineering design practices, this concern was not considered a critical element. All designs require that certain factors be discarded as the requirements focus on performance, cost and schedule. The tunnel vision that results is quite valid for constructing a complex system. However, it is dangerous when considering the operation of the system as these discarded elements present themselves in situations that are not anticipated.

Even the testing procedures were not designed to explore this area because NASA did not see it as an issue. The O-rings were tested at varying temperatures and the results demonstrated

that the seals behaved differently as the seals were warmed or cooled. However, no requirements identified this performance as critical to the safety of the mission.

Using a contemporary approach, NASA would not have required the “hard” data demanded on the night before the launch. Anyone looking at the launch pad with the icicles hanging from every surface would know this was a situation never before encountered. The situation did not call for data to explain why the shuttle should not be launched or even why it should be launched. Rather, the decision-makers should have reviewed the data in light of the overall situation. It was the unknown factors that should have been considered. Lack of quantitative or qualitative data was always a concern. In this situation, NASA had the opportunity to obtain the data required and to delay the launch until the data had been analyzed.

Managers would recognize that the shuttle systems might exhibit behavior or work together in ways not seen before. Most important, the decision-makers would know what they did not know. They would be cognizant of the limitations of the classical approach. Given the unusual situation the management team faced on the night preceding the launch and in the final hours of the countdown, the contemporary analyst would recognize that the data were not available to reach the deterministic conclusions required by the classical paradigm and embodied in the decision making process.

No amount of work would bring this certainty. The decision had to be made using a combination of hard data, engineering knowledge, and opinion without the requirement for a “black or white” choice. The hard data that could be obtained already were available for perusal. Unfortunately, this data was not displayed in a manner that clearly illuminated the correlation between temperature and O-ring resiliency.³⁴³ The decision-makers faced a situation where they needed to respond with incomplete data. The team would need to apply engineering judgment to these data and rely on the informed opinion of those asked without demanding that they produce incontrovertible data to back them. This approach has similarities to that employed by design engineers when they apply materials to a problem in new untried ways. In these cases, they do not know that the system will work as intended with these new materials. For example, there

³⁴³ Tufte, p. 16.

was a first stone bridge to replace wooden bridges, and a first metal bridge, and a first suspension bridge, etc.

This contemporary approach may appear useful, but how can it be implemented within an organization? Engineers, in particular, are educated to consider the data, reduce it to the lowest level of understanding, and search for the linkage between the cause and effect of any failure. This approach has to be modified for an organization to use the contemporary paradigm. The answer is training. First, consider how NASA is structured today. NASA trains its employees to look for deviations from a known situation and to follow a prescribed procedure for correcting it. The procedures are well documented, with an elaborate configuration control process for ensuring that only the most current procedures are followed. The Presidential Commission had no difficulty following the “paper trail” showing the design, development, problem identification, and resolution rationale for the decision to launch the *Challenger*.

Deviations from the procedure must be justified, and it is assumed that if the procedure is followed then the system will be safe. The contemporary paradigm challenges the classical approach by accepting that NASA executed the flight preparations and operations planning exactly as written. The difference is that a contemporary organization would have been trained to look beyond the written documentation and to question the wisdom of employing it for this flight or other flights where the conditions were unusual. This approach may be extended to look at the structure of the flight approval process and to question certain aspects of it. For example, it was customary to continue to launch missions with known problems for which solutions were in work. The final *Challenger* O-ring waivers were granted on this basis.³⁴⁴ This process assumes that the problem is sufficiently well understood to continue to fly and illustrates confidence that the solution being pursued will correct it. NASA had the data that indicated clearly that several times in the past the agency had thought it understood the solid rocket booster joint performance, only to find that it did not. The contemporary analyst would use these data in a different way.

Operators would continue to identify and prepare for high-risk failures such as the failure of a shuttle main engine. The physics of flight remain unchanged with the contemporary

³⁴⁴ Report of the Presidential Commission on the Space Shuttle *Challenger* Accident, pp. 147-148.

paradigm. Similarly, the value of quantitative data is undiminished. These data allow an organization to sort among what is known and what is unknown. For example, the engineering data that provided details on the O-ring design, its problems, and flight performance are of great value when weighing the decision on whether to launch. However, these data may be used in non-linear decision processes as well as linear deterministic ones.

Instead of trying to identify and train for every failure scenario, however, the operators would train in the skills necessary to see beyond the known data. They would train to understand the situation and recognize what they do not know. Like an iceberg, they may not know how much ice lies beneath the surface of the water but they recognize that just because they cannot see it does not mean that it does not exist; they factor this uncertainty into their analysis. An example of such a change was the decision to alter the pressure at which the O-ring seal test was performed. This test was designed to verify the seal would remain sealed at high pressures as the solid rocket boosters were ignited. By this standard, the test was successful, showing the seals held. From a different perspective, this test introduced a new environment to the seal, one for which it had not been designed. The test actually created or expanded holes in the thermal putty designed to isolate the O-rings from the hot gases within the solid rocket booster.

In the contemporary organization, the operators are no longer looking only in but across the systems. They continue to look for problems that may be resolved using standard engineering methods. In addition, the operators expand the areas to be researched because they recognize that few changes are isolated to resolving the original problem. Rather than looking only for known malfunctions, they are alert for deviations from a system's normal function that they might not understand. Following the change in the solid rocket booster testing process, the incidence of seal erosion increased. In response, NASA accelerated its implementation of a new solid rocket booster seal design. The agency did not stop to look at whether any of its changes introduced unanticipated effects.

In a contemporary organization, failures that might first appear independent would be viewed as possibly linked, with "possibly" being an acceptable reason for examining them. This broader, more holistic approach would treat the unexplained *Challenger* erosion problem differently. System operators would look at the changes introduced to correct a less serious,

although unanticipated problem, and recognize that they had introduced a more serious situation. These changes would be reversed, and the phenomenon examined from that point. After all, when using these new procedures the erosion increased, but the management had deemed this higher erosion level to be acceptable. At the time of the initial erosion, the pre-*Challenger* level had been considered unacceptable.

The contemporary paradigm has another distinction in this search for the cause of a system failure. There is no expectation that the cause will ever be found, or that by finding it we can prevent future failures. The *Challenger* accident was the result of a complex interaction of events. We can fix what we know but that is no guarantee there will be no further failures. There is no guarantee that a new design will produce a better result. The new design could behave exactly as the old, or could introduce new factors not seen in the old design. These factors could be severe, making the older seal design safer to fly. In addition, the new design would have none of the flight experience gained by the operational team in past missions. Without such data, the new seal design would introduce some risk into the program. Following the redesign of the solid rocket booster following the accident, NASA was confident that seal blow-by or erosion would be eliminated. This was not the case as seal erosion has been observed on missions after flights resumed. Maybe NASA did not understand all the involved factors even following this extensive development effort.

The exact sequence of events leading up to the failure never will be repeated, so preparing for them is a waste of time. Never again will all of the known factors occur in the same instant, and it cannot be determined which of these contributed to the failure. Nor is it possible to determine whether the accident would have occurred had only one factor been absent or diminished. These are the known factors only; the unknown factors play an equally important part. Continued dissection of the *Challenger* failure wastes resources that could be applied to preventing future, but not identical failures. The lesson to learn from this system failure is to change the way we manage risks in complex systems.

5.4 Where You Stand Depends On Where You Sit

The consequences flowing from the *Challenger* failure are countless. Our country lost seven people and a \$2 billion spacecraft. America completely changed its policy for launching humans and satellites into space. NASA lost much of its “can do” mantle of invulnerability. American satellite manufacturers were left with no launch vehicle, forcing them to redesign for launches elsewhere.

Despite this situation, classical analysts continue to focus on individual elements of what really are multiple consequences. A simple tabulation of the literature illustrates the wide variety of opinion as to the consequence. The resulting lack of consensus gives few clues to how a contemporary organization should proceed. All of the consequences for the *Challenger* accident that are recognized contribute in some way to the best possible understanding of the failure. Some contributions, such as the revamping of the space policy, are apparent. Less apparent are the ways in which the changed space policy has affected the nation’s exploration and use of space. Today, the expendable launch industry that was declared obsolete by the then new space shuttle is flourishing. In addition to improvements in rockets already flying, the major aerospace companies are investing huge sums in the next generation of satellites. Start-up companies, employing former senior NASA officials, are attracting capital and building competing low cost launchers. This new environment may be traced directly to the *Challenger* accident.

Perrow gives a hint as to how the contemporary paradigm would function in dealing with this issue. He recognizes that consequences may be placed into a series of categories. The individual who views the failure from his or her frame of reference establishes these categories. His approach attempts to rank the consequences by their effect on public safety. In doing so, he explicitly states that this consequence ranks above all others in deserving consideration regarding system failure. After all, what could rank above public safety?

Perrow’s approach searches for more than one consequence in order to identify the most severe one, but only as it relates to the risk to human life directly as a consequence of the failure. Perrow looks at the “victims” and makes all decisions based on their number. From this viewpoint, the *Challenger* accident was not a very serious system failure. With seven deaths, it was hardly more than a traffic accident. The shuttle does not have the capacity to place a large

number of people at risk. There are no long-term effects from the failure on the health of the public. In his analysis, Perrow disregards the potential long-term effects such a failure could have on public health. In an extreme example, the failure of the shuttle could compromise the U.S. national security by hampering the country's ability to monitor foreign threats. Such threats fall squarely within the Perrow approach, but are not considered. At a minimum, this paradigm should attempt to determine less than obvious consequences that could affect the premises outlined by Perrow.

Recognizing that Perrow's approach simply is one among many, the contemporary model presents a more sophisticated approach that recognizes the multiple non-lethal effects of the *Challenger* failure. The contemporary model does not judge whether one frame of reference is more important than another, instead placing each system failure into the chosen frame. The contemporary analyst considers all frames of reference including the less obvious consequences that are more difficult to measure.

The consequences of the accident which are seen as a given by the classical analyst may not in fact be attributable to the failure. For example, the nation, having forced all satellite manufacturers onto the shuttle, now lost a significant market share to the European consortium, ArianeSpace. Classical analysts assert the shuttle had not met expectations and the U.S. rocket manufacturers had been forced out of the market. The facts do not support this conclusion when viewed through the lens of the contemporary paradigm. The Ariane rocket competed quite successfully with the shuttle even when the latter was the primary launch vehicle for the U.S. Why couldn't the American aerospace companies do likewise? The standard answer is that the governments involved subsidized the European consortium. Taking this point of view, wasn't this transfer of flights to Ariane inevitable given the subsidies the consortium enjoyed? Perhaps the shuttle accident had only marginal bearing on the shift of the expendable launch market to overseas providers.

The cost of flying the shuttle also has a bearing on this question. Human-rated vehicles are much more expensive to certify and to launch than robotic vehicles. The shuttle system was designed to be multipurpose; incurring costs that would not apply to a single purpose expendable launch vehicle developed solely to deliver satellites to orbit. Could the shuttle ever have

competed on the basis of price with an unmanned vehicle? Had the *Challenger* not exploded, the shuttle system would still be useful for research purposes and for its unique capabilities such as satellite retrieval, but not as a delivery vehicle. The shuttle can do many things that robotic rockets cannot; this does not make it the preferred launch vehicle for satellites.

In a second example, NASA used the structural spare parts maintained for the fleet in building the replacement shuttle, the *Endeavour*. What will happen should some of these parts be needed for repairing a non-catastrophic failure? A shuttle could be damaged in a processing accident or during a flight resulting in irreparable damage to a wing or to the fuselage. Without the spare parts, an otherwise functional shuttle is eliminated from the fleet. The reduced fleet could not meet the schedules required to launch, assemble, and operate the International Space Station. Although this eventuality is removed in time by over a decade since the accident, it is still a major consequence of the *Challenger* accident, and is not considered in the classical paradigm.

This expanded set of consequences does not comprise the entire set with which the contemporary analyst would have to deal. In addition to the attempts to place the consequences into categories founded on the observer's area of interest, the study focuses in large part on what can be determined using the classical paradigm. Many of the consequences, however, are hidden from direct view. Time, unanticipated market forces, or a lack of vision may cause this lack of clarity or planning on the part of those affected by the *Challenger* accident. The contemporary interpretation of the accident is more holistic, seeking effects which may be difficult to capture quantitatively and which may never be proven.

For example, the effect of the accident on the thousands of children who viewed it on television will take years to determine. Like members of older generations who will never forget the assassinations of President Kennedy, Martin Luther King, and Robert Kennedy, the *Challenger* accident is a powerful memory for anyone alive at the time. Today, people remark that the assassinations affected their behavior and helped them look beyond the immediate day-to-day world toward the future. The shuttle accident also has shaped a generation of Americans. How many children were discouraged by the tragedy and chose a profession other than science? Equally, how many recognized the challenge of space and chose to pursue a technical education?

The businesses that transmitted communications through the commercial satellites, which were not launched because of the change in launch policy, suffered losses in sales. The lack of launch capability had a ripple effect rarely considered. Without the satellites, the communications providers could not lease the communications capabilities to customers. The effects were twofold. First, the providers lost revenue by having to provide contracted communications using other means. This approach created more traffic in an already congested system. Second, the users of the now unavailable circuits could not conduct business as they had anticipated. Business might be lost or at least curtailed to ensure orders could be filled and companies continue to operate.

The makers of expendable rockets saw their sales increase, but may never recover completely from the extended period where the shuttle was America's primary launch vehicle. This condition is an example of situation where it may be impossible to determine whether it is a consequence of the *Challenger* accident or other factors. The domestic rocket manufacturers were not prepared for the accident, and were forced to accelerate vehicle production. The European Space Agency's Ariane launch vehicle captured significant market share in this period. Nevertheless, the U.S. providers today maintain a strong presence in the worldwide market. The decade since the accident has seen tremendous growth in demand for rockets as the wireless communication market has exploded. So, was the situation after the *Challenger* accident worse than expected, but tempered by the increased market that still allows the U.S. room to participate?

Where the classical analyst would search out each of these typical consequences, the contemporary analyst understands that such an effort ultimately is a futile one. No type of quantification can establish whether a particular consequence would have occurred with or without the accident. Similarly, the degree to which it contributed is highly dependent on the observer. A Department of Defense analyst responsible for deploying national surveillance satellites might find the shuttle failure significant in the short run, but beneficial in the longer term. The country survived the period with a shortage of orbiting assets, developing a more robust capability spread across several launch systems. A military commander responsible for ensuring that the nation was prepared for nuclear attack would see the accident as an unconscionable lapse in security.

Once identified, the consequences cannot be added together like numbers to produce a total consequence score. The contemporary paradigm recognizes that, although the individual consequences may appear to have effects that can be ranked, there is no common scoring mechanism. The measurement of the consequences in many ways depends on which yardstick is being used. For example, how would the loss of scientific research resulting from the *Challenger* accident be ranked against the loss of market share for satellite launches? Even within one field, was the loss of biological research of greater significance than the loss of astronomical or semiconductor research? Similarly, are the policy implications of the *Challenger* failure more important than the fiscal cost? The shuttle and its systems were costly to construct and to maintain. The two and a half year grounding of the fleet following the accident produced costs with little return as NASA had to maintain the three remaining vehicles and preserve its work force in anticipation of the return to flight.

How should we measure the loss of the crew and the vehicle? Although the accident was a tragic loss of human life, the failure must be viewed in perspective. The loss is relatively minor when compared to major tragedies such as an airliner accident. In no way diminishing the meaning of the loss of life, the contemporary paradigm considers the overall effects of the accident. The changes in human space exploration resulting from the *Challenger* explosion far outweigh any direct effects from the loss of a single crew and one fourth of the shuttle fleet.

In addition to each of these factors, there remain consequences that go undetected. No amount of research will uncover these factors. As with Gleick's butterfly analogy from chaos theory, their impact is too remote to discern. However, this inability to directly measure the way in which the butterfly affects the outcome does not prevent the observer from viewing the overall impact of its fluttering. In the contemporary paradigm, the effects may be discerned indirectly through the performance of other factors. In the *Challenger* failure, the consequences of the accident may be visible through increased or decreased interest in the human space program. Although this change can never be proven to be the result of the accident, the contemporary organization notes the change and considers it when analyzing the consequences of a failure.

The contemporary approach to determining the consequences of a system failure is fundamentally different from the classical paradigm in another way. This new paradigm rejects

the postulate that the consequences are fixed and inevitable following a failure. First, it recognizes that the consequences can be influenced by actions taken before the failure. The shuttle program managers knew the risks of launching such a high-energy system. With many of them veterans of the Apollo program, the probability that there would be an accident was fixed in their mind. Even armed with this knowledge, the managers were not prepared for the consequences that followed. The operational procedures were in place and executed with alacrity immediately after the accident. However, this narrow focus did not consider non-operational consequences that could result.

The contemporary organization recognizes the consequences can be influenced by actions taken before the failure. By preparing for the known consequences of the *Challenger* failure, the organization can provide instructions on how to respond to the press, the administration, and the general public. When the *Challenger* failure occurred, the NASA public affairs organization was unprepared. This is not surprising, as the agency had not included the probability of a system failure in its strategic or tactical planning. With no advance preparation, the agency floundered in full view of the American people. The contemporary approach provides a completely different set of rules for examining the failure.

In another difference between the two paradigms, the contemporary analyst does not try to improve the classical approach to understanding the failure. Instead, the classical framework is discarded as not useful for determining the role of response in a system failure. This difference may be illustrated by an analogy. Using the Bible as a reference to discuss religion with an atheist is meaningless. The atheist does not accept the source. Likewise, the contemporary analyst does not accept the source of the classical mechanics, Newtonian physics, as the definitive word. Instead, the *Challenger* accident's consequences may be viewed not as inevitable but as malleable, with actions taken having some effect on the ultimate outcome.

5.5 The Inevitable Consequence Myth

In the fall of 1995, a professional politico, with no background in the space program, had replaced NASA's Administrator, James Beggs. Beggs had spent his career in the aerospace industry, rising to the top of the McDonnell Douglas management chain. While he was NASA

Administrator, the Reagan administration chose to prosecute him for fraudulent practices in connection with Department of Defense contracts at his former company. Beggs resigned his NASA post to fight the charges, which were later declared unfounded. NASA was left essentially leaderless. Where in the Apollo fire, NASA Administrator James Webb was ready to take charge and move forward, the interim NASA Administrator, William Graham, had no such vision when the shuttle was lost. In his defense, Graham knew that he was serving a caretaker role until the President could appoint a new Administrator. He had no history with the aerospace industry and lacked the experience necessary to react to such a large system failure.

In addition, Graham was hampered by the fact that there was no NASA or administration policy on what to do in the event of a catastrophic mishap and the agency floundered. NASA did not release a press statement for 24 hours following the loss of the *Challenger* and its crew. Although the agency was busy performing the operational procedures for the accident, none of these activities were conveyed to the public. No one took charge to provide a focal point for coordinating the accident investigation and for relaying its status to the American people. The situation was seen as confused and NASA appeared flustered to the point of inaction. It was left up to the President to establish a commission to investigate the accident.

There was no policy in place on whether to ground the remainder of the fleet, and on what steps would be necessary to allow the shuttle to fly again. While acknowledging the risk of shuttle flights, the agency had ignored the need to prepare for the inevitable failure. There were no criteria for recertifying the fleet and no procedures for recovering from the failure. From a technical viewpoint, the solid rocket boosters already manufactured using the existing seals were within safety requirements as long as they were launched in warmer weather. Although these boosters later were scrapped, the agency could have continued to fly shuttles while the Presidential Commission conducted its investigation.

As the details of the failure were revealed, NASA reacted to press and investigator's reports rather than take active steps to be out in front of the external forces. For example, the first reporting of the O-ring issue appeared in the New York Times with NASA left to explain how there was no cover-up. The agency's methodical steps to study the failure gained the appearance of stall tactics. Others saw NASA as incapable of conducting the investigation at all.

After the Presidential Commission was established, NASA was placed in the position of responding to findings developed by the commission. Despite developing all of the materials used by the commission, NASA never supplied information in advance of Commission press releases, leaving the agency to defend itself.

The contemporary analysts would examine the steps taken by NASA prior to the *Challenger* failure and in the months following it. Using the contemporary paradigm, they would question NASA's preparedness in two ways. First, how had the stage been set prior to the failure? What plans had been developed to deal with such a catastrophe? Had the agency prepared the public and NASA's government regulators for such an eventuality? During NASA's early years, the agency had made no secret of the risks involved. In the shuttle era, the descriptions of space flight moved from words such as "untried" and "risky" to "routine" and "operational." This change haunted the agency after the *Challenger* accident, as the public believed the new rhetoric.

Second, in the aftermath of the failure, how did NASA and its contractor management team react to affect the short and long-term consequences of the failure? The commander of the last *Challenger* flight prior to STS-51L, Henry Hartsfield, recounts "What I see out there reminds me of a sick chicken in a chicken yard, with everyone pecking at it."³⁴⁵

5.6 How Could NASA Have Prepared Differently?

Prior to the accident, NASA knew if it continued to launch shuttles, someday there would be a failure. The shuttle is a very high-energy system with many potential failure modes, many of which could destroy the vehicle. By ignoring this possibility in its planning, the agency was not prepared for the accident. There were no plans for catastrophic losses, and there was no preparation for how to announce any problems to the public. NASA recognized the risks on one level, the technical level, but did not foresee the fallout from a loss of the vehicle and its crew.

In a second example, the shuttle could be damaged during processing. For instance, it could be dropped due to a crane failure as it was being assembled. The vehicle could be damaged beyond salvaging. The contemporary organization would prepare for this accident and

be ready to respond. Although there was no loss of life, NASA would have to prepare for such a failure. The agency would need a plan for explaining how such an incident could occur, and how NASA would conduct an investigation into it. In a more severe case, the Boeing 747 carrier aircraft could crash while it was transporting the shuttle between facilities in Florida and California. Such an accident would mean not only the loss of the shuttle vehicle, but also the loss of the means to move the shuttle from one location to another.

Following the contemporary paradigm, the analyst would examine how NASA could have better set expectations internally and externally that a system failure was a possibility. Such preparation, although initially appearing that NASA was incapable of safe flights, ultimately would illustrate that the agency recognized the inherent risks. NASA could have emphasized the dangerous nature of human space flight. No activity that involves so much energy can be considered safe. In addition, the shuttle is a very complex vehicle with little margin for error. Despite NASA's claims that the vehicle was capable of flying routine missions, the physics of the situation contradicted this view.

NASA could have explained publicly that the shuttle is a research and development vehicle that does not have the reliability of a commercial aircraft. Built as an experimental aircraft, the basic design of the shuttle was never changed. Also, the vehicle was untried from the beginning as it was the first U.S. spacecraft that carried astronauts on its maiden voyage. The shuttle was a test vehicle whose risks were well understood inside the agency. However, NASA chose to maintain the relevant data at a lower profile. The agency could have published the probabilities that a Shuttle might fail, and educate policy makers about what this possibility implied for the program. With a small fleet of four vehicles, NASA had little room for error.

If the contemporary paradigm had been employed, managers would have been instructed not to minimize discussions of the risks, but to demonstrate that NASA fully understood and had accepted them. The risks of human space flight are significant and there is little that can be done to lower them beyond a given point. The energy of launch is unchangeable. The systems involved are necessarily complex. NASA would be advised to explain these risks to the

³⁴⁵ Collins, p. 236.

American public without attempting to treat the risks as “business as usual.” At the same time, NASA could have prepared in advance for how to respond to the accident when it occurred.

Following the contemporary paradigm, NASA would have had in place mechanisms for following this maxim. Senior managers would have scripts for reacting to any failure. Items such as press briefings would be coordinated so that the agency spoke with one voice. Contingency plans would outline in detail what steps were to be taken to brief the public and government officials. NASA would be out in front in discussing the failure, providing the latest data on the investigation and on the overall situation.

Standing policy on how to react to the failure would be executed. NASA would take the lead in discussing the failure, and in explaining how it would recover from it. The agency would emphasize the risks of space flight and would display how it had attempted to minimize these risks. Also, NASA would explain that a failure was inevitable and that it would work unceasingly to improve the systems on the shuttle vehicle. As the failure was identified, NASA would move aggressively toward making public the initial problem.

Examinations of NASA’s responses following the *Challenger* failure show that the overall consequences were not limited to activities surrounding the failure. Many of these responses were aimed at showing the nation was attempting to deal with the tragedy. Suddenly, decisions that had been thought through were considered shallow. The nation had not decided to make the space shuttle the “National Space Transportation System” without weighing the benefits and the drawbacks of such a course. A loss of a spacecraft became a national problem as opposed to an engineering issue to be addressed. For example, the decision was made to shift all commercial satellites to expendable rockets. This change in policy ignored the fact that launching satellites is a fundamental function of the shuttle and one of the principle reasons it was built in the first place. Expendable rockets are not more reliable than the shuttle, and they present additional challenges. The transfer of all future payloads to such rockets implied that expendable vehicles were more reliable; this is not the case.

Following the accident, NASA was ordered to make significant changes in its management structure with little basis for them except, “This is the way we did it in Apollo.” The problems with the Apollo program were ignored as it was held up as the standard for all

future programs. It is interesting that the Apollo program included only 8 trips to the Moon, with one of those not landing because of systems problems. The shuttle had flown three times as many flights when the accident occurred. Although none of these flights had left Earth orbit, the high-energy portion of the flight had been completed. With such a successful program, it is surprising that NASA adopted the Apollo model. The Apollo program had its own difficulties and should not be considered a standard for new programs. Reverting to “how we did it in the old days” does not reduce the risk of a failure in a complex system.

By using the contemporary paradigm, steps such as these would have been judged against the probability that they would help reduce the chances of an accident occurring. It would not be assumed that the way NASA was executing its responsibilities was somehow flawed. Instead, operations personnel would recognize that failures will occur in such a complex system and would prepare to handle them. Yes, there was a mistake, and yes, there was a failure. This situation does not necessarily indicate that that NASA erred in launching the *Challenger*.

Rather than reacting to the unfolding events, changes in policy would be weighed against their impact to the NASA mission and to the country. The failure of a shuttle would not be viewed as an event to permanently alter the vehicles’ use. The tragedy would be seen as an accident, one that would require NASA to make corrections to reduce the risk of a future failure. However, the loss of the shuttle and its crew were not inconceivable events and NASA, along with the rest of the country, should have examined the policies which governed space flight with this in mind. Was the reliance on the shuttle a mistake? Should the government have promoted the expendable launch vehicle market as a redundant source? While there are no direct answers to these questions, the contemporary paradigm provides answers to the fundamental questions of system failure: what caused it? And what were the consequences?

It may be used to look across a spectrum of potential causes for a system failure, training the personnel to look for the unexpected as well as the expected. This holistic view appears from the outside to be chaotic. Actually, it develops the flexibility required to recognize problems as they are developing. For example, NASA should have seen that the O-ring issue was something that was not understood. The agency concentrated its efforts on “running to ground” the factors associated with the erosion. NASA and its contractors would have been wiser to consider that

the joints were not behaving as expected. With a situation not anticipated, the agency should have stepped back and reviewed the risks associated with the erosion.

Even with perfect preparation for the particular failure seen in *Challenger* failure, NASA would find the work of limited value. The agency must prepare for the next failure, not a repetition of the last failure. In doing so, NASA is faced with a situation where data may not always be exact, and where the linkages among data may be absent. The *Challenger* failure had many causes and its effects are considerable. Recognizing these factors, the contemporary analyst seeks the lesson of finding the next risk in a complex system.

This paradigm also introduces the concept that consequences from the failure may be mitigated before or after the failure occurs. If Beggs had been NASA Administrator at the time of the failure, would anyone question that the outcome would be different? NASA let the Presidential Commission assume control of the failure investigation. This tactic differed radically from the way the agency dealt with past failures and NASA did not benefit from this new approach. NASA could have prepared for a catastrophic accident. It did not. NASA also could have reacted in a way that minimized the grounding of the shuttle fleet. It did not.