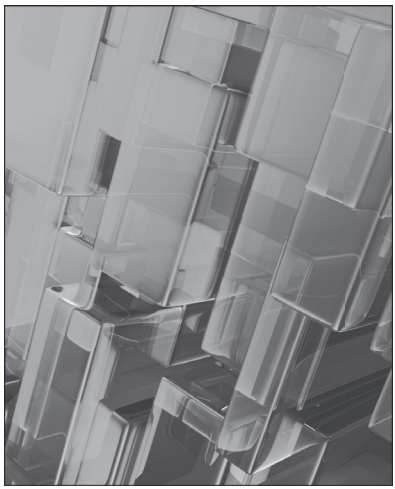
Project Management Case Studies, Fifth Edition
By Harold Kerzner

Part 11

PROJECT RISK MANAGEMENT

In today's world of project management, perhaps the single most important skill that a project manager can possess is risk management. Risk management includes identifying the risks, assessing the risks either quantitatively or qualitatively, choosing the appropriate method for handling the risks, and then monitoring and documenting the risks.

Effective risk management requires that the project manager be proactive and demonstrate a willingness to develop contingency plans, actively monitor the project, and be willing to respond quickly when a serious risk event occurs. Time and money are required for effective risk management to take place.



The Space Shuttle *Challenger* Disaster

On January 28, 1986, the space shuttle *Challenger* lifted off the launch pad at 11:38 a.m., beginning the flight of Mission 51-L. Approximately 75 seconds into the flight, the *Challenger* was engulfed in an explosive burn, and all communication and telemetry ceased. Seven brave crewmembers lost their lives. On board the *Challenger* were Francis R. (Dick) Scobee (commander), Michael John Smith (pilot), Ellison S. Onizuka (mission specialist 1), Judith Arlene Resnik (mission specialist 2), Ronald Erwin McNair (mission specialist 3), S. Christa McAuliffe (payload specialist 1), and Gregory Bruce Jarvis (payload specialist 2). A faulty seal, or O-ring, on one of the two solid rocket boosters (SRBs) caused the accident.

Following the accident, significant energy was expended trying to ascertain whether the accident had been predictable. Controversy arose from the desire to assign, or to avoid, blame. Some publications called it a management failure, specifically in risk management, while others called it a technical failure.

Whenever accidents had occurred in the past at the National Aeronautics and Space Administration (NASA), an internal investigation team had been formed.

But in this case, perhaps because of the visibility, the White House took the initiative in appointing an independent commission. There did exist significant justification for the commission. NASA was in a state of disarray, especially in the management ranks. The agency had been without a permanent administrator for almost four months. The turnover rate at the upper echelons of management was high, and there seemed to be a lack of direction from the top down.

This mission had been known as the Teacher in Space mission, and Christa McAuliffe, a Concord, New Hampshire, schoolteacher, had been selected from a list of over 10,000 applicants. The nation knew the names of all of the crewmembers on board *Challenger.* The mission had been highly publicized for months, stating that Christa McAuliffe would be teaching students from aboard the *Challenger* on day 4 of the mission.

The Presidential Commission consisted of the following members:

- William P. Rogers, chairman: Former secretary of state under President Nixon and attorney general under President Eisenhower.
- Neil A. Armstrong, vice chairman: Former astronaut and spacecraft commander for Apollo 11.
- David C. Acheson: Former senior vice president and general counsel, Communications Satellite Corporation (1967–1974), and a partner in the law firm of Drinker Biddle & Reath.
- Dr. Eugene E. Covert: Professor and head, Department of Aeronautics and Astronautics at Massachusetts Institute of Technology.
- Dr. Richard P. Feynman: Physicist and professor of theoretical physics at California Institute of Technology; Nobel Prize winner in Physics, 1965
- Robert B. Hotz: Editor-in-chief of *Aviation Week & Space Technology* magazine (1953–1980).
- Major General Donald J. Kutyna, USAF: Director of Space Systems and Command, Control, Communications.
- Dr. Sally K. Ride: Astronaut and mission specialist on STS-7, launched on June 18, 1983, making her the first American woman in space. She also flew on mission 41-G, launched October 5, 1984. She held a doctorate in physics from Stanford University (1978) and was still an active astronaut.
- Robert W. Rummel: Vice president of Trans World Airlines and president of Robert W. Rummel Associates, Inc., of Mesa, Arizona.
- Joseph F. Sutter: Executive vice president of the Boeing Commercial Airplane Company.
- Dr. Arthur B. C. Walker, Jr.: Astronomer and professor of applied physics; formerly associate dean of the Graduate Division at Stanford University, and consultant to Aerospace Corporation, Rand Corporation, and the National Science Foundation.
- Dr. Albert D. Wheelon: Executive vice president, Hughes Aircraft Company.
- Brigadier General Charles Yeager, USAF (retired): Former experimental test pilot. He was the first person to break the sound barrier and the first to fly at a speed of more than 1,600 miles an hour.
- Dr. Alton G. Keel, Jr., Executive Director: Detailed to the Commission from his position in the Executive Office of the President, Office

of Management and Budget, as associate director for National Security and International Affairs; formerly assistant secretary of the Air Force for Research, Development and Logistics, and Senate Staff.

The Commission interviewed more than 160 individuals, and more than 35 formal panel investigative sessions were held generating almost 12,000 pages of transcript. Almost 6,300 documents totaling more than 122,000 pages, along with hundreds of photographs, were examined and made a part of the Commission's permanent database and archives. These sessions and all the data gathered added to the 2,800 pages of hearing transcript generated by the Commission in both closed and open sessions. Unless otherwise stated, all of the quotations and memos in this case study are from direct testimony cited in the *Report by the Presidential Commission* (*RPC)* (http://history.nasa.gov/rogersrep/genindex.htm).

BACKGROUND TO THE SPACE TRANSPORTATION SYSTEM

During the early 1960s, NASA's strategic plans for post-*Apollo* manned space exploration rested on a three-legged stool. The first leg was a reusable space transportation system, the space shuttle, which could transport people and equipment to low-Earth orbits and then return to Earth in preparation for the next mission. The second leg was a manned space station that would be resupplied by the space shuttle and serve as a launch platform for space research and planetary exploration. The third leg would be planetary exploration to Mars. But by the late 1960s, the United States was involved in the Vietnam War, which was becoming costly. In addition, confidence in the government was eroding because of civil unrest and assassinations. With limited funding due to budgetary cuts and with the lunar landing missions coming to an end, prioritization of projects was necessary. With a Democratic Congress continuously attacking the cost of space exploration and minimal support from President Nixon, the space program was left standing on one leg only, the space shuttle.

President Nixon made it clear that funding all the programs NASA envisioned would be impossible and that funding for even one program on the order of the *Apollo* program was likewise not possible. President Nixon seemed to favor the space station concept, but this required the development of a reusable space shuttle. Thus NASA's Space Shuttle Program became the near-term priority.

One of the reasons for the high priority given to the Space Shuttle Program was a 1972 study completed by Dr. Oskar Morgenstern and Dr. Klaus Heiss of the Princeton-based Mathematica organization. The study showed that the space shuttle would be able to orbit payloads for as little as $100 per pound based on 60 launches per year with payloads of 65,000 pounds. This provided tremendous promise for military applications such as reconnaissance and weather satellites as well as for scientific research.

Unfortunately, the pricing data were somewhat tainted. Much of the cost data were provided by companies that hoped to become NASA contractors and that therefore provided unrealistically low cost estimates in hopes of winning future bids. The actual cost per pound would prove to be more than 20 times the original estimate. Furthermore, the main engines never achieved the 109 percent of thrust that NASA desired, thus limiting the payloads to 47,000 pounds instead of the predicted 65,000 pounds. In addition, the European Space Agency began developing the capability to place satellites into orbit and began competing with NASA for the commercial satellite business.

NASA SUCCUMBS TO POLITICS AND PRESSURE

To retain shuttle funding, NASA was forced to make a series of major concessions. First, facing a highly constrained budget, NASA sacrificed the research and development (R&D) necessary to produce a truly reusable shuttle and instead accepted a design that was only partially reusable, eliminating one of the features that had made the shuttle attractive in the first place. SRBs were used instead of safer liquid-fueled boosters because they required a much smaller R&D effort. Numerous other design changes were made to reduce the level of R&D required.

Second, to increase its political clout and to guarantee a steady customer base, NASA enlisted the support of the United States Air Force. The Air Force could provide the considerable political clout of the Department of Defense and it used many satellites, which required launching. However, Air Force support did not come without a price. The shuttle payload bay was required to meet Air Force size and shape requirements, which placed key constraints on the ultimate design. Even more important was the Air Force requirement that the shuttle be able to launch from Vandenberg Air Force Base in California. This constraint required a larger cross range than the Florida site, which, in turn, decreased the total allowable vehicle weight. The weight reduction required the elimination of the design's air breathing engines, resulting in a single-pass unpowered landing. This greatly limited the safety and landing versatility of the vehicle.[1]

As the year 1986 began, there was extreme pressure on NASA to "Fly out the Manifest." From its inception, the Space Shuttle Program had been plagued by exaggerated expectations, funding inconsistencies, and political pressure. The ultimate vehicle and mission design were shaped almost as much by politics as by physics. President Kennedy's declaration that the United States would land a man on the moon before the end of the decade (the 1960s) had provided NASA's *Apollo* program with high visibility, a clear direction, and powerful political

[1] Kurt Hoover and Wallace T. Fowler, "Studies in Ethics, Safety and Liability for Engineers." www .tsgc.utexas. edu/archive/general/ethics/shuttle.html page 2.

backing. The Space Shuttle Program was not as fortunate; it had neither a clear direction nor consistent political backing.

Cost containment became a critical issue for NASA. In order to minimize cost, NASA designed a space shuttle system that utilized both liquid and solid propellants. Liquid-propellant engines are more easily controllable than solid-propellant engines. Flow of liquid propellant from the storage tanks to the engine can be throttled and even shut down in case of an emergency. Unfortunately, an all-liquid-fuel design was prohibitive because a liquid-fuel system is significantly more expensive to maintain than a solid-fuel system.

Solid-fuel systems are less costly to maintain. However, once a solid-propellant system is ignited, it cannot be easily throttled or shut down. Solid-propellant rocket motors burn until all of the propellant is consumed. This could have a significant impact on safety, especially during launch, at which time the SRBs are ignited and have maximum propellant loads. Also, SRBs can be designed for reusability, whereas liquid engines are generally used only once.

The final design that NASA selected was a compromise of both solid- and liquid-fuel engines. The space shuttle would be a three-element system composed of the orbiter vehicle, an expendable external liquid-fuel tank carrying[2] The orbiter's engines were liquid fuel because of the necessity for throttle capability. The two SRBs would provide the added thrust necessary to launch the space shuttle into its orbiting altitude.

In 1972, NASA selected Rockwell as the prime contractor for building the orbiter. Many industry leaders believed that other competitors that had actively participated in the *Apollo* program had a competitive advantage. Rockwell, however, was awarded the contract. Rockwell's proposal did not include an escape system. NASA officials decided against the launch escape system since it would have added too much weight to the shuttle at launch and was very expensive. There was also some concern on how effective an escape system would be if an accident occurred during launch when all of the engines were ignited. Thus, the Space Shuttle Program became the first U.S. manned spacecraft without a launch escape system for the crew.

In 1973, NASA went out for competitive bidding for the SRBs. The competitors were Morton-Thiokol, Inc. (MTI) (henceforth called Thiokol), Aerojet General, Lockheed, and United Technologies. The contract was eventually awarded to Thiokol because of its low cost, $100 million lower than the nearest competitor. Some believed that other competitors that ranked higher in technical design and safety should have been given the contract. NASA believed that Thiokol-built solid rocket motors would provide the lowest cost per flight.

---

[2] The terms "solid rocket booster" (SRB) and "solid rocket motor" (SRM) will be used interchangeably.

SOLID ROCKET BOOSTERS

Thiokol's SRBs had a height of approximately 150 feet and a diameter of 12 feet. The empty weight of each booster was 192,000 pounds, and the full weight was 1,300,000 pounds. Once ignited, each booster provided 2.65 million pounds of thrust, which is more than 70 percent of the thrust needed to lift off the launch pad.

Thiokol's design for the boosters was criticized by some competitors and even by some NASA personnel. The boosters were to be manufactured in four segments and then shipped from Utah to the launch site, where the segments would be assembled into a single unit. The Thiokol design was largely based on the segmented design of the Titan III solid rocket motor produced by United Technologies in the 1950s for Air Force satellite programs. Satellite programs were unmanned efforts.

The four solid rocket sections made up the case of the booster, which essentially encased the rocket fuel and directed the flow of the exhaust gases. This is shown in Figure I. The cylindrical shell of the case is protected from the propellant by a layer of insulation. The mating sections of the field joint are called the tang and the clevis. One hundred seventy-seven pins spaced around the circumference of each joint hold the tang and the clevis together. The joint is sealed in three ways. First, zinc chromate putty is placed in the gap between the mating segments and their insulation. This putty protects the second and third seals, which are rubberlike rings, called O-rings. The first O-ring is called the primary O-ring and is lodged in the gap between the tang and the clevis. The last seal is called the secondary O-ring, which is identical to the primary O-ring except it is positioned farther downstream in the gap. Each O-ring is 0.280 inches in diameter. The placement of each O-ring can be seen in Figure II. Another component of the field joint is called the leak check port, which is shown in Figure III. The leak check port is designed to allow technicians to check the status of the two O-ring seals. Pressurized air is inserted through the leak check port into the gap between the two O-rings. If the O-rings maintain the pressure and do not let the pressurized air past the seal, the technicians know the seal is operating properly.[3] In the Titan III assembly process, the joints between the segmented sections contained one O-ring. Thiokol's design had two O-rings instead of one. The second O-ring was initially considered redundant but was included to improve safety.

The purpose of the O-rings was to seal the space in the joints such that the hot exhaust gases could not escape and damage the case of the boosters.

Both the Titan III and shuttle O-rings were made of Viton rubber, which is an elastomeric material. For comparison, rubber is also an elastomer. The elastomeric material used is a fluoroelastomer, which is an elastomer that contains fluorine. This material was chosen because of its resistance to high temperatures

[3] "The *Challenger* Accident: Mechanical Causes of the *Challenger* Accident," University of Texas, http://www.me.utexas.edu/~uer/challenger/chall2.html, pp. 1–2.

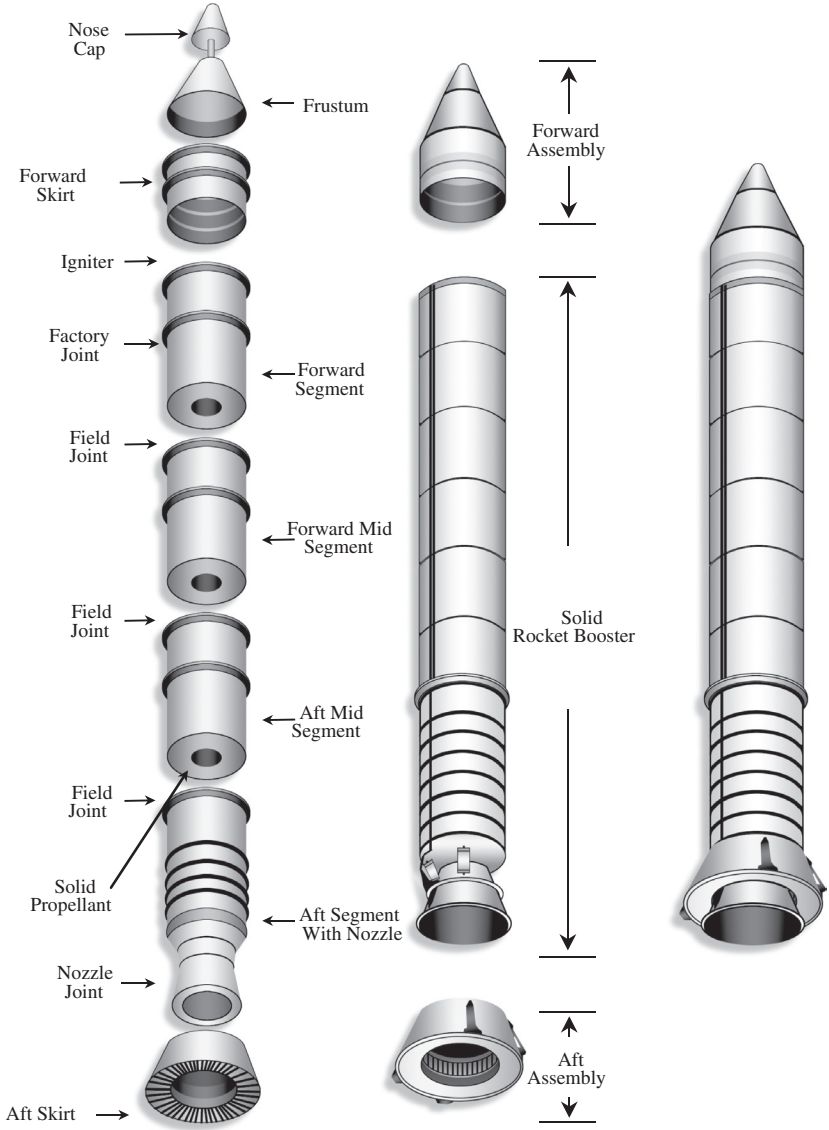


FIGURE I Solid rocket booster

and its compatibility with the surrounding materials. The Titan III O-rings were molded in one piece, whereas the shuttle's SRB O-rings would be manufactured in five sections and then glued together. Routinely, repairs would be necessary for inclusions and voids in the rubber received from the material suppliers.

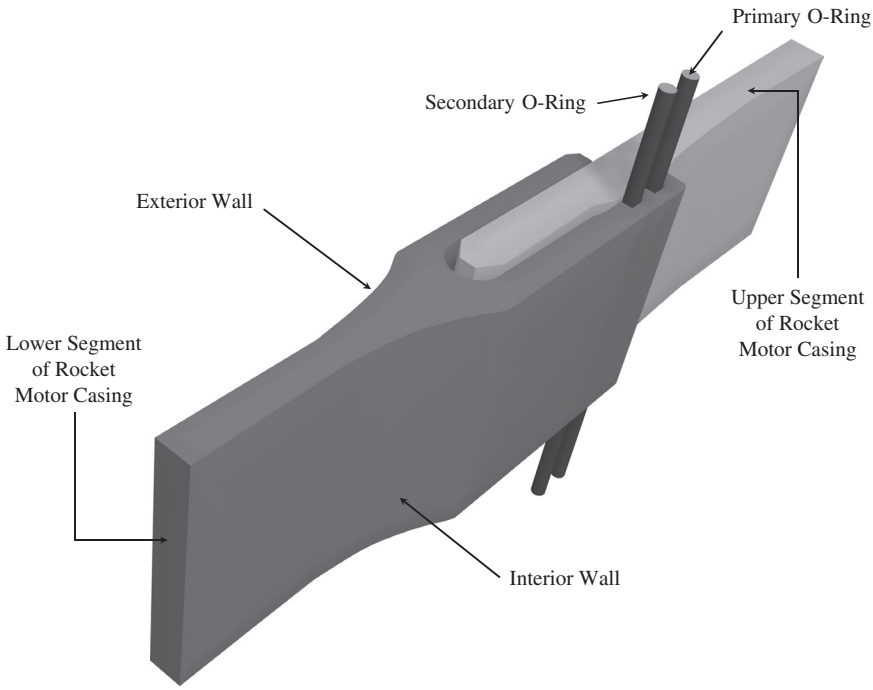


FIGURE II Location of the O-rings

BLOWHOLES

The primary purpose of the zinc chromate putty was to act as a thermal barrier that protected the O-rings from the hot exhaust. As mentioned, the O-ring seals were tested using the leak check port to pressurize the gap between the seals. During the test, the secondary seal was pushed down into the same, seated position as it occupied during ignition pressurization. However, because the leak check port was between the two O-ring seals, the primary O-ring was pushed up and seated against the putty. The position of the O-rings during flight and their position during the leak check test is shown in Figure III. During early flights, engineers worried that, because the putty above the primary seal could withstand high pressures, the presence of the putty would prevent the leak test from identifying problems with the primary seal. They contended that the putty would seal the gap during testing regardless of the condition of the primary seal. Since the proper operation of the primary seal was essential, engineers decided to increase the pressure used during the test to above the pressure that the putty could withstand. This would ensure that the primary O-ring was properly sealing the gap without the aid of

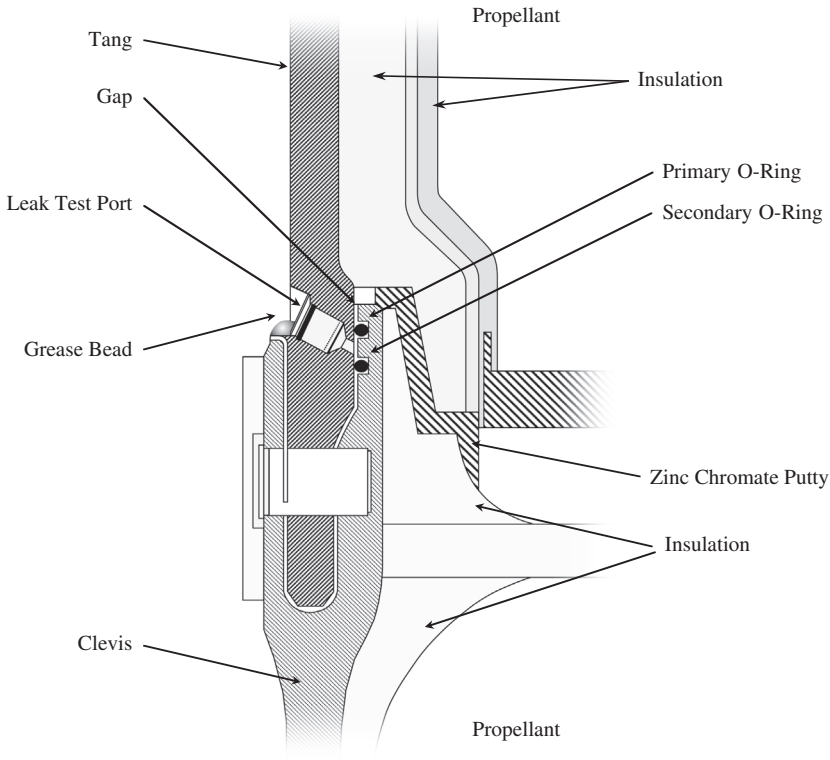


FIGURE III Cross section showing the leak test port

the putty. Unfortunately, during this new procedure, the high-test pressures blew holes through the putty before the primary O-ring could seal the gap.

Since the putty was on the interior of the assembled SRB, technicians could not mend the blowholes in the putty. As a result, this procedure left small, tunneled holes in the putty. These holes would allow focused exhaust gases to contact a small segment of the primary O-ring during launch. Engineers realized that this was a problem but decided to test the seals at the high pressure despite the formation of blowholes rather than risking a launch with a faulty primary seal.

The purpose of the putty was to prevent the hot exhaust gases from reaching the O-rings. For the first nine successful shuttle launches, NASA and Thiokol used asbestos-bearing putty manufactured by the Fuller-O'Brien Company of San Francisco. However, because of the notoriety of products containing asbestos and

the fear of potential lawsuits, Fuller-O'Brien stopped manufacturing the putty that had served the shuttle so well. This created a problem for NASA and Thiokol.

The new putty selected came from Randolph Products of Carlstadt, New Jersey. Unfortunately, with the new putty, blowholes and O-ring erosion were becoming more common to a point where the shuttle engineers became worried. Yet the new putty was still used on the boosters. Following the *Challenger* disaster, testing showed that, at low temperatures, the Randolph putty became much stiffer than the Fuller-O'Brien putty and lost much of its stickiness.[4]

O-RING EROSION

If the hot exhaust gases penetrated the putty and contacted the primary O-ring, the extreme temperatures would break down the O-ring material. Because engineers were aware of the possibility of O-ring erosion, the joints were checked after each flight for evidence of erosion. The amount of O-ring erosion found on flights before the new high-pressure leak check procedure was around 12 percent. After the new high-pressure leak test procedure, the percentage of O-ring erosion was found to increase by 88 percent. In some cases, high percentages of O-ring erosion allowed the exhaust gases to pass the primary O-ring and begin eroding the secondary O-ring. Some managers argued that some O-ring erosion was "acceptable" because the O-rings were found to seal the gap even if they were eroded by as much as one-third their original diameter.[5] The engineers believed that the design and operation of the joints were acceptable risks because a safety margin could be identified quantitatively. This numerical boundary would become an important precedent for future risk assessment.

JOINT ROTATION

During ignition, the internal pressure from the burning fuel applies approximately 1,000 pounds per square inch on the case wall, causing the walls to expand. Because the joints are generally stiffer than the case walls, each section tends to bulge out. The swelling of the solid rocket sections causes the tang and the clevis to become misaligned; this misalignment is called joint rotation. A diagram showing a field joint before and after joint rotation is seen in Figure IV. The problem with joint rotation is that it increases the gap size near the O-rings. This increase in size is extremely fast, which makes it difficult for the O-rings to follow the increasing gap and keep the seal.[6]

Prior to ignition, the gap between the tang and the clevis is approximately 0.004 inches. At ignition, the gap enlarges to between 0.042 and 0.060 inches *for a maximum of 0.60 seconds* and then returns to its original position.

---

[4] Ibid., p. 3.
[5] Ibid., p. 4.
[6] Ibid.

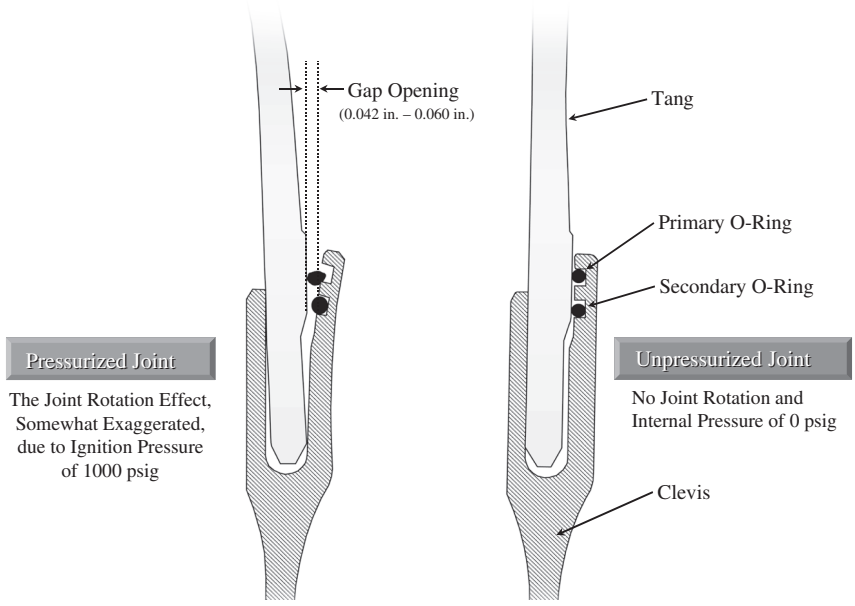


FIGURE IV Field joint rotation

O-RING RESILIENCE

The term "O-ring resilience" refers to the ability of the O-ring to return to its original shape after it has been deformed. This property is analogous to the ability of a rubber band to return to its original shape after it has been stretched. As with a rubber band, the resiliency of an O-ring is related directly to its temperature. As the temperature of the O-ring gets lower, the O-ring material becomes stiffer. Tests have shown that an O-ring at 75°F is five times more responsive in returning to its original shape than an O-ring at 30°F. This decrease in O-ring resiliency during a cold-weather launch would make the O-ring much less likely to follow the increasing gap size during joint rotation. As a result of poor O-ring resiliency, the O-ring would not seal properly.[7]

THE EXTERNAL TANK

The solid rockets are each joined forward and aft to the external liquid fuel tank. They are not connected to the orbiter vehicle. The solid-rocket motors are mounted

[7] Ibid., pp. 4–5.

first, and the external liquid-fuel tank is put between them and connected. Then the orbiter is mounted to the external tank at two places in the back and one place forward. Those connections carry all of the structural loads for the entire system at liftoff and through the ascent phase of flight. Also connected to the orbiter, under the orbiter's wing, are two large propellant lines 17 inches in diameter. The one on the port side carries liquid hydrogen from the hydrogen tank in the back part of the external tank. The line on the right side carries liquid oxygen from the oxygen tank at the forward end, inside the external tank.[8]

The external tank contains about 1.6 million pounds of propellant, or about 526,000 gallons. The orbiter's three engines burn the liquid hydrogen and liquid oxygen at a ratio of 6:1 and at a rate equivalent to emptying out a family swimming pool every 10 seconds. Once ignited, the exhaust gases leave the orbiter's three engines at approximately 6,000 miles per hour. After the fuel is consumed, the external tank separates from the orbiter, falls to Earth, and disintegrates in the atmosphere on reentry.

THE SPARE PARTS PROBLEM

In March 1985, NASA's administrator, James Beggs, announced that there would be one shuttle flight per month for all of fiscal year 1985. In actuality, there were only six flights. Repairs became a problem. Continuous repairs were needed on the heat tiles required for reentry, the braking system, and the main engines' hydraulic pumps. Parts were routinely borrowed from other shuttles. The cost of spare parts was excessively high, and NASA was looking for cost containment.

RISK IDENTIFICATION PROCEDURES

The necessity for risk management was apparent right from the start. Prior to the launch of the first shuttle in April of 1981, hazards were analyzed and subjected to a formalized hazard reduction process as described in the NASA Handbook, NHB5300.4. The process required that the credibility and probability of the hazards be determined. A Senior Safety Review Board was established for overseeing the risk assessment process. For the most part, the risk assessment process was qualitative. The conclusion reached was that no single hazard or combination of hazards should prevent the launch of the first shuttle *as long as the aggregate risk remained acceptable.*

NASA used a rather simplistic safety (risk) classification system. A quantitative method for risk assessment was not in place at NASA because gathering the data needed to generate statistical models would be expensive and labor-intensive. If the risk identification procedures were overly complex, NASA would have been buried in paperwork due to the number of components on the space shuttle. The risk classification system selected by NASA is shown in Table I.

---

[8] *Report by the Presidential Commission (RPC),* p. 50.

TABLE I RISK CLASSIFICATION SYSTEM

Level	Description
Criticality 1 (C1)	Loss of life and/or vehicle if the component fails.
Criticality 2 (C2)	Loss of mission if the component fails.
Criticality 3 (C3)	All others.
Criticality 1R (C1R)	Redundant components exist. The failure of both could cause loss of life and/or vehicle.
Criticality 2R (C2R)	Redundant components exist. The failure of both could cause loss of mission.

From 1982 on, the O-ring seal was labeled Criticality 1. By 1985, there were 700 components identified as Criticality 1.

TELECONFERENCING

The Space Shuttle Program involves a vast number of people at both NASA and the contractors. Because of the geographical separation between NASA and the contractors, it became impractical to have continuous meetings. Travel between Thiokol in Utah and the Cape in Florida took one day each way. Therefore, teleconferencing became the primary method of communication and a way of life. Interface meetings were still held, but the emphasis was on teleconferencing. All locations could be linked together in one teleconference and data could be faxed back and forth as needed.

PAPERWORK CONSTRAINTS

With the rather optimistic flight schedule provided to the news media, NASA was under scrutiny and pressure to deliver. For fiscal 1986, the mission manifest called for 16 flights. The pressure to meet schedule was about to take its toll. Safety problems had to be resolved quickly.

As the number of flights scheduled began to increase, so did the requirements for additional paperwork. The majority of the paperwork had to be completed prior to NASA's Flight Readiness Review (FRR) meetings. Approximately one week prior to every flight, flight operations and cargo managers were required to endorse the commitment of flight readiness to the NASA associate administrator for space flight at the FRR meeting. The responsible project/element managers would conduct pre-FRR meetings with their contractors, center managers, and the NASA Level II manager. The content of the FRR meetings included the following:

- Determine overall status as well as establish the baseline in terms of significant changes since the last mission.
- Review significant problems resolved since the last review and significant anomalies from the previous flight.

- Review all open items and constraints remaining to be resolved before the mission.
- Present all new waivers since the last flight.

NASA personnel were working excessive overtime, including weekends, to fulfill the paperwork requirements and prepare for the required meetings. As the number of space flights increased, so did the paperwork and overtime.

The paperwork constraints were affecting the contractors as well. Additional paperwork requirements existed for problem solving and investigations. On October 1, 1985, an interoffice memo was sent from Scott Stein, space booster project engineer at Thiokol, to Bob Lund, vice president for engineering at Thiokol, and other selected managers concerning the O-Ring Investigation Task Force:

> We are currently being hog-tied by paperwork every time we try to accomplish anything. I understand that for production programs, the paperwork is necessary. However, for a priority, short schedule investigation, it makes accomplishment of our goals in a timely manner extremely difficult, if not impossible. We need the authority to bypass some of the paperwork jungle. As a representative example of problems and time that could easily be eliminated, consider assembly or disassembly of test hardware by manufacturing personnel. . . . I know the established paperwork procedures can be violated if someone with enough authority dictates it. We did that with the DR system when the FWC hardware "Tiger Team" was established. If changes are not made to allow us to accomplish work in a reasonable amount of time, then the O-ring investigation task force will never have the potency necessary to resolve problems in a timely manner.[9]

Both NASA and the contractors were now feeling the pressure caused by the paperwork constraints.

ISSUING WAIVERS

One quick way of reducing paperwork and meetings was to issue a waiver. Historically, a waiver was a formalized process that allowed an exception to a rule, a specification, a technical criterion, or a risk. Waivers were ways to reduce excessive paperwork requirements. Project managers and contract administrators had the authority to issue waivers, often with the intent of bypassing standard protocols in order to maintain a schedule. The use of waivers had been in place well before the manned space program even began. What is important here was *not* NASA's use of the waiver but the *justification* for the waiver, given the risks.

NASA had issued waivers on both Criticality 1 status designations and launch constraints. In 1982, the SRBs were designated C1 by the Marshall Space Flight Center because failure of the O-rings could have caused loss of crew and the shuttle. This meant that the secondary O-rings were not considered redundant. The SRB project manager at Marshall, Larry Malloy, issued a waiver just in time

[9] Reproduced in *RPC*, p. 253

for the next shuttle launch to take place as planned. Later, the O-rings designation went from C1 to C1R (i.e., a redundant process), thus partially avoiding the need for a waiver. The waiver was a necessity to keep the shuttle flying according to the original manifest.

Having a risk identification of C1 was not regarded as a sufficient reason to cancel a launch. It simply meant that component failure could be disastrous. It implied that this might be a potential problem that needed attention. If the risks were acceptable, NASA could still launch. A more serious condition was the issuing of launch constraints. Launch constraints were official NASA designations for situations in which mission safety was a serious enough problem to justify a decision not to launch. But once again, a launch constraint did not imply that the launch should be delayed. It meant that this was an important problem and needed to be addressed.

Following the 1985 mission that showed O-ring erosion and exhaust gas blow-by, a launch constraint was imposed. Yet on each of the next five shuttle missions, NASA's Malloy issued a launch constraint waiver allowing the flights to take place on schedule without any changes to the O-rings.

Were the waivers a violation of serious safety rules just to keep the shuttle flying? The answer is *no.* NASA had protocols such as policies, procedures, and rules for adherence to safety. Waivers were also protocols but for the purpose of deviating from other existing protocols. Larry Malloy, his colleagues at NASA, and the contractors had no intentions of doing evil. Waivers were simply a way of saying that they believed that the risk is an *acceptable risk.*

The lifting of launch constraints and the issuance of waivers became the norm—standard operating procedure. Waivers became a way of life. If waivers were issued and the mission was completed successfully, then the same waivers would exist for the next flight and did not have to be brought up for discussion at the FRR meeting. The justification for the waivers seemed to be the similarity among flight launch conditions, temperature, and so on. Launching under similar conditions seemed to be important for the engineers at NASA and Thiokol because it meant that the forces acting on the O-rings were within their region of experience and could be correlated to existing data. The launch temperature effect on the O-rings was considered predictable and therefore constituted an acceptable risk to both NASA and Thiokol, thus perhaps eliminating costly program delays that would have resulted from having to redesign the O-rings. The completion of each shuttle mission added another data point to the region of experience, thus guaranteeing the same waivers on the next launch. Flying with acceptable risk became the norm in NASA's culture.

LAUNCH LIFTOFF SEQUENCE PROFILE: POSSIBLE ABORTS

During the countdown to liftoff, the launch team closely monitors weather conditions, not only at the launch site but also at touchdown sites, should the mission need to be prematurely aborted.

Dr. Feynman: "Would you explain why we are so sensitive to the weather?"

Mr. Moore (NASA's deputy administrator for space flight): "Yes, there are several reasons. I mentioned the return to the landing site. We need to have visibility if we get into a situation where we need to return to the landing site after launch, and the pilots and the commanders need to be able to see the runway and so forth. So, you need a ceiling limitation on it [i.e., weather].

"We also need to maintain specifications on wind velocity so we don't exceed crosswinds. Landing on a runway and getting too high of a crosswind may cause us to deviate off of the runway and so forth, so we have a crosswind limit. During ascent, assuming a normal flight, a chief concern is damage to tiles due to rain. We have had experiences in seeing what the effects of a brief shower can do in terms of the tiles. The tiles are thermal insulation blocks, very thick. A lot of them are very thick on the bottom of the orbiter. But if you have a raindrop and you are going at a very high velocity, it tends to erode the tiles, pock the tiles, and that causes us a grave concern regarding the thermal protection.

"In addition to that, you are worried about the turnaround time of the orbiters as well, because with the kind of tile damage that one could get in rain, you have an awful lot of work to do to go back and replace tiles back on the system. So, there are a number of concerns that weather enters into, and it is a major factor in our assessment of whether or not we are ready to launch."[10]

Approximately six to seven seconds prior to liftoff, the shuttle's main engines (liquid fuel) ignite. These engines consume one-half million gallons of liquid fuel. It takes nine hours prior to launch to fill the liquid-fuel tanks. At ignition, the engines are throttled up to 104 percent of rated power. Redundancy checks on the engines' systems are then made. The launch site ground complex and the orbiter's onboard computer complex check a large number of details and parameters about the main engines to make sure that everything is proper and that the main engines are performing as planned.

If a malfunction is detected, the system automatically goes into a shutdown sequence, and the mission is scrubbed. The primary concern at this point is to make the vehicle "safe." The crew remains on board and performs a number of functions to get the vehicle into a safe mode. These functions include making sure that all propellant and electrical systems are properly safed. Ground crews at the launch pad begin servicing the launch pad. Once the launch pad is in a safe condition, the hazard and safety teams begin draining the remaining liquid fuel out of the external tank.

If no malfunction is detected during this six-second period of liquid fuel burn, then a signal is sent to ignite the two SRBs, and liftoff occurs. For the next

[10] Ibid., p. 18.

two minutes, with all engines ignited, the shuttle goes through a Max Q, or high dynamic pressure phase, that exerts maximum pressure loads on the orbiter vehicle. Based on the launch profile, the main engines may be throttled down slightly during the Max Q phase to lower the loads.

After 128 seconds into the launch sequence, all of the solid fuel is expended and the SRB staging occurs. The SRB parachutes are deployed. The SRBs then fall back to Earth 162 miles from the launch site and are recovered for examination, cleaning, and reuse on future missions. The main liquid-fuel engines are then throttled up to maximum power. After 523 seconds into the liftoff, the external liquid-fuel tanks are essentially expended of fuel. The main engines are shut down. Ten to 18 seconds later, the external tank is separated from the orbiter and disintegrates on reentry into the atmosphere.

From a safety perspective, the most hazardous period is the first 128 seconds when the SRBs are ignited. Here's what Arnold Aldrich, manager of NASA's STS Program, Johnson Space Center, had to say:

Mr. Aldrich: "Once the shuttle system starts off the launch pad, there is no capability in the system to separate these [solid-propellant] rockets until they reach burnout. They will burn for two minutes and eight or nine seconds, and the system must stay together. There is not a capability built into the vehicle that would allow these to separate. There is a capability available to the flight crew to separate at this interface the orbiter from the tank, but that is thought to be unacceptable during the first stage when the booster rockets are on and thrusting. So, essentially the first two minutes and a little more of flight, the stack is intended and designed to stay together, and it must stay together to fly successfully."

Mr. Hotz: "Mr. Aldrich, why is it unacceptable to separate the orbiter at that stage?"

Mr. Aldrich: "It is unacceptable because of the separation dynamics and the rupture of the propellant lines. You cannot perform the kind of a clean separation required for safety in the proximity of these vehicles at the velocities and the thrust levels they are undergoing, [and] the atmosphere they are flying through. In that regime, it is the design characteristic of the total system."[11]

If an abort is deemed necessary during the first 128 seconds, the actual abort will not begin until *after* SRB staging has occurred, which is after 128 seconds into the launch sequence. Based on the reason and timing of an abort, options include those listed inTable II.

---

[11] Ibid., p. 51

TABLE II ABORT OPTIONS FOR SHUTTLE

Type of Abort	Landing Site
Once-around abort	Edwards Air Force Base
Transatlantic abort	DaKar
Transatlantic abort	Casablanca
Return to landing site	Kennedy Space Center

Arnold Aldrich was questioned on different abort profiles.

Chairman Rogers: "During the two-minute period, is it possible to abort through the orbiter?"

Mr. Aldrich: "You can abort for certain conditions. You can start an abort, but the vehicle won't do anything yet, and the intended aborts are built around failures in the main engine system, the liquid propellant systems and their controls. If you have a failure of a main engine, it is well detected by the crew and by the ground support, and you can call for a return-to-launch-site abort. That would be logged in the computer. The computer would be set up to execute it, but everything waits until the solids take you to altitude. At that time, the solids will separate in the sequence I described, and then the vehicle flies downrange some 400 miles, maybe 10 to 15 additional minutes, while all of the tank propellant is expelled through these engines.

"As a precursor to setting up the conditions for this return-to-launch-site abort to be successful towards the end of that burn downrange, using the propellants and the thrust of the main engines, the vehicle turns and actually points heads up back towards Florida. When the tank is essentially depleted, automatic signals are sent to close off the [liquid] propellant lines and to separate the orbiter, and the orbiter then does a similar approach to the one we are familiar with orbit back to the Kennedy Space Center for approach and landing."

Dr. Walker: "So, the propellant is expelled but not burned?"

Mr. Aldrich: "No, it is burned. You burn the system on two engines all the way down-range until it is gone, and then you turn around and come back because you don't have enough to burn to orbit. That is the return-to-launch-site abort, and it applies during the first 240 seconds of—no, 240 is not right. It is longer than that—the first four minutes, either before or after separation you can set that abort up, but it will occur after the solids separate, and if you have a main engine anomaly after the solids separate, at that time you can start the RTLS, and it will go through that same sequence and come back."

Dr. Ride: "And you can also only do an RTLS if you have lost just one main engine. So if you lose all three main engines, RTLS isn't a viable abort mode."

Mr. Aldrich: "Once you get through the four minutes, there's a period where you now don't have the energy conditions right to come back, and you have a forward abort, and Jesse mentioned the sites in Spain and on the coast of Africa. We have what is called a trans-Atlantic abort, and where you can use a very similar sequence to the one I just described. You still separate the solids, you still burn all the propellant out of the tanks, but you fly across and land across the ocean."

Mr. Hotz: "Mr. Aldrich, could you recapitulate just a bit here? Is what you are telling us that for two minutes of flight, until the solids separate, there is no practical abort mode?"

Mr. Aldrich: "Yes, sir."

Mr. Hotz: "Thank you."

Mr. Aldrich: "A trans-Atlantic abort can cover a range of just a few seconds up to about a minute in the middle where the across-the-ocean sites are effective, and then you reach this abort once-around capability where you go all the way around and land in California or back to Kennedy by going around the earth. And finally, you have abort-to-orbit where you have enough propulsion to make orbit but not enough to achieve the exact orbital parameters that you desire. That is the way that the abort profiles are executed.

"There are many, many nuances of crew procedure and different conditions and combinations of sequences of failures that make it much more complicated than I have described it."[12]

THE O-RING PROBLEM

There were two kinds of joints on the shuttle—field joints that were assembled at the launch site connecting together the SRB's cylindrical cases, and nozzle joints that connected the aft end of the case to the nozzle. During the pressure of ignition, the field joints could become bent such that the secondary O-ring could lose contact within an estimated 0.17 to 0.33 seconds after ignition. If the primary O-ring failed to seal properly before the gap within the joints opened up and the secondary seal failed, the results could be disastrous.

When the solid-propellant boosters are recovered after separation, they are disassembled and checked for damage. The O-rings could show evidence of coming into contact with heat. Hot gases from the ignition sequence could blow by the primary O-ring briefly before sealing. This blow-by phenomenon could last for only a few milliseconds before sealing and result in no heat damage to the O-ring. If the actual sealing process takes longer than expected, then charring and erosion of the O-rings can occur. This would be evidenced by gray or black soot and erosion to the O-rings. The terms used are "impingement erosion" and "bypass" erosion, with the latter identified also as "sooted blow-by."

---

[12] Ibid., pp. 51–52.

Roger Boisjoly of Thiokol describes blow-by erosion and joint rotation as follows:

> O-ring material gets removed from the cross section of the O-ring much, much faster than when you have bypass erosion or blow-by, as people have been terming it. We usually use the characteristic blow-by to define gas past it, and we use the other term [bypass erosion] to indicate that we are eroding at the same time. And so you can have blow-by without erosion, [and] you [can] have blow-by with erosion. . . .[13]
>
> At the beginning of the transient cycle [initial ignition rotation, up to 0.17 seconds] . . . [the primary O-ring] is still being attacked by hot gas, and it is eroding at the same time it is trying to seal, and it is a race between, will it erode more than the time allowed to have it seal.[14]

On January 24, 1985, STS 51-C [Flight No. 15] was launched at 51°F, which was the lowest temperature of any launch up to that time. Analyses of the joints showed evidence of damage. Black soot appeared between the primary and secondary O-rings. The engineers concluded that the cold weather had caused the O-rings to harden and move more slowly. This allowed the hot gases to blow by and erode the O-rings. This scorching effect indicated that low-temperature launches could be disastrous.

On July 31, 1985, Roger Boisjoly of Thiokol sent an interoffice memo to R. K. Lund, vice president for engineering at Thiokol:

> This letter is written to insure that management is fully aware of the seriousness of the current O-ring erosion problem in the SRM joints from an engineering standpoint.
>
> The mistakenly accepted position on the joint problem was to fly without fear of failure and to run a series of design evaluations which would ultimately lead to a solution or at least a significant reduction of the erosion problem. This position is now drastically changed as a result of the SRM 16A nozzle joint erosion which eroded a secondary O-ring with the primary O-ring never sealing.
>
> If the same scenario should occur in a field joint (and it could), then it is a jump ball as to the success or failure of the joint because the secondary O-ring cannot respond to the clevis opening rate and may not be capable of pressurization. The result would be a catastrophe of the highest order—loss of human life.
>
> An unofficial team [a memo defining the team and its purpose was never published] with [a] leader was formed on 19 July 1985 and was tasked with solving the problem for both the short and long term. This unofficial team is essentially nonexistent at this time. In my opinion, the team must be officially given the responsibility and the authority to execute the work that needs to be done on a non-interference basis (full time assignment until completed).

---

[13] Ibid., pp. 784–785.
[14] Ibid., p. 136.

> It is my honest and very real fear that if we do not take immediate action to dedicate a team to solve the problem with the field joint having the number one priority, then we stand in jeopardy of losing a flight along with all the launch pad facilities.[15]

On August 9, 1985, a letter was sent from Brian Russell, manager of the SRM Ignition System, to James Thomas at the Marshall Space Flight Center. The memo addressed the following:

> Per your request, this letter contains the answers to the two questions you asked at the July Problem Review Board telecon.
>
> *Question:* If the field joint secondary seal lifts off the metal mating surfaces during motor pressurization, how soon will it return to a position where contact is re-established?
>
> *Answer:* Bench test data indicate that the O-ring resiliency (its capability to follow the metal) is a function of temperature and rate of case expansion. MTI [Thiokol] measured the force of the O-ring against Instron plattens, which simulated the nominal squeeze on the O-ring and approximated the case expansion distance and rate.
>
> At 100°F, the O-ring maintained contact. At 75°F, the O-ring lost contact for 2.4 seconds. At 50°F, the O-ring did not re-establish contact in 10 minutes at which time the test was terminated.
>
> The conclusion is that secondary sealing capability in the SRM field joint cannot be guaranteed.
>
> *Question:* If the primary O-ring does not seal, will the secondary seal seat in sufficient time to prevent joint leakage?
>
> *Answer:* MTI has no reason to suspect that the primary seal would ever fail after pressure equilibrium is reached; i.e., after the ignition transient. If the primary O-ring were to fail from 0 to 170 milliseconds, there is a very high probability that the secondary O-ring would hold pressure since the case has not expanded appreciably at this point. If the primary seal were to fail from 170 to 330 milliseconds, the probability of the secondary seal holding is reduced. From 330 to 600 milliseconds the chance of the secondary seal holding is small. This is a direct result of the O-ring's slow response compared to the metal case segments as the joint rotates.[16]

At NASA, the concern for a solution to the O-ring problem became not only a technical crisis but also a budgetary crisis. In a July 23, 1985, memorandum from Richard Cook, program analyst, to Michael Mann, chief of the STS Resource Analysis Branch, the impact of the problem was noted:

> Earlier this week you asked me to investigate reported problems with the charring of seals between SRB motor segments during flight operations. Discussions

---

[15] Ibid., pp. 691–692.
[16] Ibid., pp. 1568–1569.

with program engineers show this to be a potentially major problem affecting both flight safety and program costs.

Presently three seals between SRB segments use double O-rings sealed with putty. In recent Shuttle flights, charring of these rings has occurred. The O-rings are designed so that if one fails, the other will hold against the pressure of firing. However, at least in the joint between the nozzle and the aft segment, not only has the first O-ring been destroyed, but the second has been partially eaten away.

Engineers have not yet determined the cause of the problem. Candidates include the use of a new type of putty (the putty formerly in use was removed from the market by EPA [Environmental Protection Agency] because it contained asbestos), failure of the second ring to slip into the groove which must engage it for it to work properly, or new, and as yet unidentified, assembly procedures at Thiokol. MSC is trying to identify the cause of the problem, including on-site investigation at Thiokol, and OSF hopes to have some results from their analysis within thirty days. There is little question, however, that flight safety has been and is still being compromised by potential failure of the seals, and it is acknowledged that failure during launch would certainly be catastrophic. There is also indication that staff personnel knew of this problem sometime in advance of management's becoming apprised of what was going on.

The potential impact of the problem depends on the as yet undiscovered cause. If the cause is minor, there should be little or no impact on budget or flight rate. A worst case scenario, however, would lead to the suspension of shuttle flights, redesign of the SRB, and scrapping of existing stockpiled hardware. The impact on the FY 1987-8 budget could be immense.

It should be pointed out that Code M anagement [NASA's associate administrator for space flight] is viewing the situation with the utmost seriousness. From a budgetary standpoint, I would think that any NASA budget submitted this year for FY 1987 and beyond should certainly be based on a reliable judgment as to the cause of the SRB seal problem and a corresponding decision as to budgetary action needed to provide for its solution.[17]

On October 30, 1985, NASA launched Flight STS 61-A [Flight No. 22] at 75°F. This flight also showed signs of sooted blow-by, but the color was significantly blacker. Although there was some heat effect, there was no measurable erosion observed on the secondary O-ring. Since blow-by and erosion had now occurred at a higher launch temperature, the original premise that launches under cold temperatures were a problem was now being questioned. Table III shows the temperature at launch of all the shuttle flights up to this time and the O-ring damage, if any.

Management at both NASA and Thiokol wanted *concrete* evidence that launch temperature was directly correlated to blow-by and erosion. Other than

[17] Ibid., pp. 391–392.

TABLE III EROSION AND BLOW-BY HISTORY (TEMPERATURE IN ASCENDING ORDER FROM COLDEST TO WARMEST)

Flight	Date	Temperature (°F)	Erosion Incidents	Blow-by Incidents	Comments
51-C	01/24/85	53	3	2	Most erosion any flight; blow-by secondary O-rings heated up
41-B	02/03/84	57	1		Deep, extensive erosion
61-C	01/12/86	58	1		O-rings erosion
41-C	04/06/84	63	1		O-rings heated but no damage
1	04/12/81	66			Coolest launch without problems
6	04/04/83	67			
51-A	11/08/84	67			
51-D	04/12/85	67			
5	11/11/82	68			
3	03/22/82	69			
2	11/12/81	70	1		Extent of erosion unknown
9	11/28/83	70			
41-D	08/30/84	70	1		
51-G	06/17/85	70			
7	06/18/83	72			
8	08/30/83	73			
51-B	04/29/85	75			
61-A	10/20/85	75		2	No erosion but soot between O-rings
51-1	08/27/85	76			
61	11/26/85	76			
41-G	10/05/84	78			
51-J	10/03/85	79			
4	06/27/82	80	No data; casing lost at sea		
51-F	07/29/85	81			

simply a gut feel, engineers were now stymied on how to show the direct correlation. NASA was not ready to cancel a launch simply due to an engineer's gut feel.

William Lucas, director of the Marshall Space Center, made it clear that NASA's manifest for launches would be adhered to. Managers at NASA were pressured to resolve problems internally rather than to escalate them up the chain of command. Managers became afraid to inform anyone higher up that they had a problem, even though they knew that one existed.

Richard Feynman, Nobel laureate and member of the Rogers Commission, concluded that a NASA official altered the safety criteria so that flights could be certified on time under pressure imposed by the leadership of William Lucas. Feynman commented:

> . . . They, therefore, fly in a relatively unsafe condition with a chance of failure of the order of one percent. Official management claims to believe that the probability of failure is a thousand times less.

Without concrete evidence of the temperature effect on the O-rings, the secondary O-ring was regarded as a redundant safety constraint, and the criticality factor was changed from C1 to C1R. Potentially serious problems were treated as anomalies peculiar to a given flight. Under the guise of anomalies, NASA began issuing waivers to maintain the flight schedules. Pressure was placed on contractors to issue closure reports. On December 24, 1985, L. O. Wear, NASA's SRM Program Office manager, sent a letter to Joe Kilminster, Thiokol's vice president for the Space Booster Program:

> During a recent review of the SRM Problem Review Board open problem list I found that we have 20 open problems, 11 opened during the past 6 months, 13 open over 6 months, 1 three years old, 2 two years old, and 1 closed during the past six months. As you can see our closure record is very poor. You are requested to initiate the required effort to assure more timely closures and the MTI personnel shall coordinate directly with the S&E personnel the contents of the closure reports.[18]

PRESSURE, PAPERWORK, AND WAIVERS

To maintain the flight schedule, critical issues such as launch constraints had to be resolved or waived. This would require extensive documentation. During the Rogers Commission investigation, it seemed that there had been a total lack of coordination between NASA's Marshall Space Center and Thiokol prior to the *Challenger* disaster. Joe Kilminster, Thiokol's vice president for the Space Booster Program, testified:

Mr. Kilminster: "Mr. Chairman, if I could, I would like to respond to that. In response to the concern that was expressed—and I had discussions with the team leader, the task force team leader, Mr. Don Kettner, and Mr. Russell and Mr. Ebeling. We held a meeting in my office and that was done in the October time period where we called the people who were in a support role to the task team, as well as the task force members themselves.

---

[18] Ibid., p. 1554.

"In that discussion, some of the task force members were looking to circumvent some of our established systems. In some cases, that was acceptable; in other cases, it was not. For example, some of the work that they had recommended to be done was involved with full-scale hardware, putting some of these joints together with various putty layup configurations; for instance, taking them apart and finding out what we could from that inspection process."

Dr. Sutter: "Was that one of these things that was outside of the normal work, or was that accepted as a good idea or a bad idea?"

Mr. Kilminster: "A good idea, but outside the normal work, if you will."

Dr. Sutter: "Why not do it?"

Mr. Kilminster: "Well, we were doing it. But the question was, can we circumvent the system, the paper system that requires, for instance, the handling constraints on those flight hardware items? And I said no, we can't do that. We have to maintain our handling system, for instance, so that we don't stand the possibility of injuring or damaging a piece of flight hardware.

"I asked at that time if adding some more people, for instance, a safety engineer—that was one of the things we discussed in there. The consensus was no, we really didn't need a safety engineer. We had the manufacturing engineer in attendance who was in support of that role, and I persuaded him that, typical of the way we normally worked, that he should be calling on the resources from his own organization, that is, in Manufacturing, in order to get this work done and get it done in a timely fashion.

"And I also suggested that if they ran across a problem in doing that, they should bubble that up in their management chain to get help in getting the resources to get that done. Now, after that session, it was my impression that there was improvement based on some of the concerns that had been expressed, and we did get quite a bit of work done. For your evaluation, I would like to talk a little bit about the sequence of events for this task force."

Chairman Rogers: "Can I interrupt? Did you know at that time it was a launch constraint, a formal launch constraint?"

Mr. Kilminster: "Not an overall launch constraint as such. Similar to the words that have been said before, each Flight Readiness Review had to address any anomalies or concerns that were identified at previous launches and in that sense, each of those anomalies or concerns were established in my mind as launch constraints unless they were properly reviewed and agreed upon by all parties."

Chairman Rogers: "You didn't know there was a difference between the launch constraint and just considering it an anomaly? You thought they were the same thing?"

Mr. Kilminster: "No, sir. I did not think they were the same thing."

Chairman Rogers: "My question is: Did you know that this launch constraint was placed on the flights in July 1985?"

Mr. Kilminster: "Until we resolved the O-ring problem on that nozzle joint, yes. We had to resolve that in a fashion for the subsequent flight before we would be okay to fly again."

Chairman Rogers: "So you did know there was a constraint on that?"

Mr. Kilminster: "On a one flight per one flight basis; yes, sir."

Chairman Rogers: "What else would a constraint mean?"

Mr. Kilminster: "Well, I get the feeling that there's a perception here that a launch constraint means all launches, whereas we were addressing each launch through the Flight Readiness Review process as we went."

Chairman Rogers: "No, I don't think—the testimony that we've had is that a launch constraint is put on because it is a very serious problem and the constraint means don't fly unless it's fixed or taken care of, but somebody has the authority to waive it for a particular flight. And in this case, Mr. Mulloy was authorized to waive it, which he did, for a number of flights before 51-L. Just prior to 51-L, the papers showed the launch constraint was closed out, which I guess means no longer existed. And that was done on January 23, 1986. Now, did you know that sequence of events?"

Mr. Kilminster: "Again, my understanding of *closing out,* as the term has been used here, was to close it out on the problem actions list, but not as an overall standard requirement. We had to address these at subsequent Flight Readiness Reviews to ensure that we were all satisfied with the proceeding to launch."

Chairman Rogers: "Did you understand the waiver process, that once a constraint was placed on this kind of a problem, that a flight could not occur unless there was a formal waiver?"

Mr. Kilminster: "Not in the sense of a formal waiver, no, sir."

Chairman Rogers: "Did any of you? Didn't you get the documents saying that?"

Mr. McDonald: "I don't recall seeing any documents for a formal waiver."[19]

MISSION 51-L

On January 25, 1986, questionable weather caused a delay of Mission 51-L to January 27. On January 26, the launch was reconfirmed for 9:37 a.m. on the 27th. However, on the morning of January 27, a malfunction with the hatch, combined with high crosswinds, caused another delay. All preliminary procedures had been completed and the crew had just boarded when the first problem appeared. A microsensor on the hatch indicated that the hatch was not shut securely. It turned out that the hatch was shut securely but the sensor had malfunctioned. Valuable time was lost in determining the problem.

After the hatch was finally closed, the external handle could not be removed. The threads on the connecting bolt were stripped and, instead of cleanly disengaging

[19] Ibid., pp. 1577–1578.

when turned, simply spun around. Attempts to use a portable drill to remove the handle failed. Technicians on the scene asked Mission Control for permission to saw off the bolt. Fearing some form of structural stress to the hatch, engineers made numerous time-consuming calculations before giving the go-ahead to cut off the bolt. The entire process consumed almost two hours before the countdown resumed.

However, the misfortunes continued. During the attempts to verify the integrity of the hatch and remove the handle, the wind had been steadily rising. Chief Astronaut John Young flew a series of approaches in the shuttle training aircraft and confirmed the worst fears of mission control. The crosswinds at the Cape were in excess of the level allowed for the abort contingency. The opportunity had been missed. The mission was then reset to launch the next day, January 28, at 9:38 a.m. Everyone was quite discouraged since extremely cold weather was forecast for Tuesday that could further postpone the launch.[20]

Weather conditions indicated that the temperature at launch could be as low as 26°F. This would be much colder and well below the temperature range that the O-rings were designed to operate in. The components of the solid rocket motors were qualified only to 40°F at the lower limit. Undoubtedly, when the sun came up and launch time approached, both the air temperature and vehicle would warm up, but there was still concern. Would the ambient temperature be high enough to meet the launch requirements? NASA's Launch Commit Criteria stated that no launch should occur at temperatures below 31°F. There were also worries over any permanent effects on the shuttle due to the cold overnight temperatures. NASA became concerned and asked Thiokol for their recommendation on whether or not to launch. NASA admitted under testimony that if Thiokol had recommended not launching, then the launch would not have taken place.

At 5:45 p.m. eastern standard time, a teleconference was held among the Kennedy Space Center, Marshall Space Flight Center, and Thiokol. Bob Lund, vice president for engineering, summarized the concerns of the Thiokol engineers that in Thiokol's opinion, the launch should be delayed until noontime or even later such that a launch temperature of at least 53°F could be achieved. Thiokol's engineers were concerned that no data were available for launches at this temperature of 26°F. This was the first time in 14 years that Thiokol had recommended not to launch.

The design validation tests originally done by Thiokol covered only a narrow temperature range. The temperature data did not include any temperatures below 53°F. The O-rings from Flight 51-C, which had been launched under cold conditions the previous year, showed very significant erosion. These were the only data available on the effects of cold, but all of the Thiokol engineers

[20] Hoover and Wallace, "Studies in Ethics, Safety and Liability for Engineers," pp. 3–4.

agreed that the cold weather would decrease the elasticity of the synthetic rubber O-rings, which in turn might cause them to seal slowly and allow hot gases to surge through the joint.[21]

Another teleconference was set up for 8:45 p.m. to invite more parties to be involved in the decision. Meanwhile, Thiokol was asked to fax all relevant and supporting charts to all parties involved in the 8:45 p.m. teleconference.

The following information was included in the pages that were faxed:

Blow-by History

SRM-15 Worst Blow-by
- Two case joints (80°), (110°) *Arc*
- Much worse visually than SRM-22

SRM-22 Blow-by
- Two case joints (30–40°)

SRM-13A, 15, 16A, 18, 23A, 24A
- Nozzle blow-by

Field Joint Primary Concerns—SRM-25
- A temperature lower than the current database results in changing primary O-ring sealing timing function
- SRM-15A—80° arc black grease between O-rings SRM-15B—110° arc black grease between O-rings
- Lower O-ring squeeze due to lower temp
- Higher O-ring shore hardness
- Thicker grease viscosity
- Higher O-ring pressure activation time
- If actuation time increases, threshold of secondary seal pressurization capability is approached.
- If threshold is reached then secondary seal may not be capable of being pressurized.

Conclusions

Temperature of O-ring is not only parameter controlling blow-by:
- SRM-15 with blow-by had an O-ring temp at 53°F.
- SRM-22 with blow-by had an O-ring temp at 75°F.
- Four development motors with no blow-by were tested at O-ring temp of 47° to 52°F.
- Development motors had putty packing which resulted in better performance.
- At about 50°F blow-by could be experienced in case joints.
- Temp for SRM-25 on 1-28-86 launch will be: 29°F 9 a.m.
  38°F 2 p.m.
- Have no data that would indicate SRM-25 is different than SRM-15 other than temp.

[21] Ibid., p. 4.

Recommendations

- O-ring temp must be ≥ 53°F at launch.
- Development motors at 47° to 52°F with putty packing had no blow-by.
- SRM-15 (the best simulation) worked at 53°F.
- Project ambient conditions (temp & wind) to determine launch time.

From NASA's perspective, the launch window was from 9:30 a.m. to 12:30 p.m. on January 28. This was based on weather conditions and visibility, not only at the launch site but also at the landing sites, should an abort be necessary. An additional consideration was the fact that the temperature might not reach 53°F prior to the launch window closing. Actually, the temperature at the Kennedy Space Center was not expected to reach 50°F until two days later. NASA was hoping that Thiokol would change its mind and recommend launch.

THE SECOND TELECONFERENCE

At the second teleconference, Bob Lund once again asserted Thiokol's recommendation not to launch below 53°F. NASA's Mulloy then burst out over the teleconference network: "My God, Morton Thiokol! When do you want me to launch—next April?"

NASA challenged Thiokol's interpretation of the data and argued that Thiokol was inappropriately attempting to establish a new Launch Commit Criterion just prior to launch. NASA asked Thiokol to reevaluate its conclusions. Crediting NASA's comments with some validity, Thiokol then requested a five- minute *off-line* caucus. In the room at Thiokol were 14 engineers, namely:

1. Jerald Mason, senior vice president, Wasatch Operations
2. Calvin Wiggins, vice president and general manager, Space Division
3. Joe C. Kilminster, vice president, Space Booster Programs
4. Robert K. Lund, vice president, Engineering
5. Larry H. Sayer, director, Engineering and Design
6. William Macbeth, manager, Case Projects, Space Booster Project
7. Donald M. Ketner, supervisor, Gas Dynamics Section and head Seal Task Force
8. Roger Boisjoly, member, Seal Task Force
9. Arnold R. Thompson, supervisor, Rocket Motor Cases
10. Jack R. Kapp, manager, Applied Mechanics Department
11. Jerry Burn, associate engineer, Applied Mechanics
12. Joel Maw, associate scientist, Heat Transfer Section
13. Brian Russell, manager, Special Projects, SRM Project
14. Robert Ebeling, manager, Ignition System and Final Assembly, SRB Project

There were no safety personnel in the room because nobody thought to invite them. The caucus lasted some 30 minutes. Thiokol (specifically Joe Kilminster)

then returned to the teleconference stating that they were unable to sustain a valid argument that temperature affects O-ring blow-by and erosion. *Thiokol then reversed its position and was now recommending launch.*

NASA stated that the launch of the *Challenger* would not take place without Thiokol's approval. But when Thiokol reversed its position following the caucus and agreed to launch, NASA interpreted this as an acceptable risk. The launch would now take place.

Mr. McDonald (Thiokol): "The assessment of the data was that the data was not totally conclusive, that the temperature could affect everything relative to the seal. But there was data that indicated that there were things going in the wrong direction, and this was far from our experience base.

"The conclusion being that Thiokol was directed to reassess all the data because the recommendation was not considered acceptable at that time of [waiting for] the 53 degrees [to occur]. NASA asked us for a reassessment and some more data to show that the temperature in itself can cause this to be a more serious concern than we had said it would be. At that time Thiokol in Utah said that they would like to go off-line and caucus for about five minutes and reassess what data they had there or any other additional data.

"And that caucus lasted for, I think, a half hour before they were ready to go back on. When they came back on they said they had reassessed all the data and had come to the conclusions that the temperature influence, based on the data they had available to them, was inconclusive and therefore they recommended a launch."[22]

During the Rogers Commission testimony, NASA's Mulloy stated his thought process in requesting Thiokol to rethink their position:

General Kutyna: "You said the temperature had little effect?"
Mr. Mulloy: "I didn't say that. I said I can't get a correlation between O-ring erosion, blow-by and O-ring, and temperature."
General Kutyna: "51-C was a pretty cool launch. That was January of last year."
Mr. Mulloy: "It was cold before then but it was not that much colder than other launches."
General Kutyna: "So it didn't approximate this particular one?"
Mr. Mulloy: "Unfortunately, that is one you look at and say, aha, is it related to a temperature gradient and the cold. The temperature of the O-ring on 51-C, I believe, was 53 degrees. We have fired motors at 48 degrees."[23]

---

[22] *RPC,* p. 300.
[23] Ibid., p. 290

Mulloy asserted he had not pressured Thiokol into changing their position. Yet the testimony of Thiokol's engineers stated they believed they were being pressured.

Roger Boisjoly, one of Thiokol's experts on O-rings, was present during the caucus and vehemently opposed the launch. During testimony, Boisjoly described his impressions of what occurred during the caucus:

Mr. Boisjoly: "The caucus was started by Mr. Mason stating that a management decision was necessary. Those of us who were opposed to the launch continued to speak out, and I am specifically speaking of Mr. Thompson and myself because in my recollection, he and I were the only ones who vigorously continued to oppose the launch. And we were attempting to go back and rereview and try to make clear what we were trying to get across, and we couldn't understand why it was going to be reversed.

"So, we spoke out and tried to explain again the effects of low temperature. Arnie actually got up from his position which was down the table and walked up the table and put a quad pad down in front of the table, in front of the management folks, and tried to sketch out once again what his concern was with the joint, and when he realized he wasn't getting through, he just stopped.

"I tried one more time with the photos. I grabbed the photos and I went up and discussed the photos once again and tried to make the point that it was my opinion from actual observations that temperature was indeed a discriminator, and we should not ignore the physical evidence that we had observed.

"And again, I brought up the point that SRM-15 had a 110 degree arc of black grease, while SRM-22 had a relatively different amount, which was less and wasn't quite as black. I also stopped when it was apparent that I could not get anybody to listen."

Dr. Walker: "At this point did anyone else [i.e., engineers] speak up in favor of the launch?"

Mr. Boisjoly: "No, sir. No one said anything, in my recollection. Nobody said a word. It was then being discussed amongst the management folks. After Arnie and I had our last say, Mr. Mason said we have to make a management decision. He turned to Bob Lund and asked him to take off his engineering hat and put on his management hat. From this point on, management formulated the points to base their decision on. There was never one comment in favor, as I have said, of launching by any engineer or other nonmanagement person in the room before or after the caucus. I was not even asked to participate in giving any input to the final decision charts.

"I went back on the net with the final charts or final chart, which was the rationale for launching, and that was presented by Mr. Kilminster. It was handwritten on a notepad, and he read from that notepad. I did not agree

with some of the statements that were being made to support the decision. I was never asked nor polled, and it was clearly a management decision from that point.

"I must emphasize, I had my say, and I never take any management right to take the input of an engineer and then make a decision based upon that input, and I truly believe that. I have worked at a lot of companies, and that has been done from time to time, and I truly believe that, and so there was no point in me doing anything any further [other] than [what] I had already attempted to do.

"I did not see the final version of the chart until the next day. I just heard it read. I left the room feeling badly defeated, but I felt I really did all I could to stop the launch. I felt personally that management was under a lot of pressure to launch, and they made a very tough decision, but I didn't agree with it.

"One of my colleagues who was in the meeting 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 in total reverse to what the position usually is in a preflight conversation or a Flight Readiness Review. It is usually exactly opposite that."

Dr. Walker: "Do you know the source of the pressure on management that you alluded to?"

Mr. Boisjoly: "Well, the comments made over the net are what I felt. I can't speak for them, but I felt it. I felt the tone of the meeting exactly as I summed up, that we were being put in a position to prove that we should not launch rather than being put in the position and prove that we had enough data to launch."[24]

General Kutyna: "What was the motivation driving those who were trying to overturn your opposition?"

Mr. Boisjoly: "They felt that we had not demonstrated, or I had not demonstrated, because I was the prime mover in SRM-15. Because of my personal observations and involvement in the Flight Readiness Reviews, they felt that I had not conclusively demonstrated that there was a tie-in between temperature and blow-by.

"My main concern was if the timing function changed and that seal took longer to get there, then you might not have any seal left because it might be eroded before it seats. And then, if that timing function is such that it pushes you from the 170 millisecond region into the 330 second region, you might not have a secondary seal to pick up if the primary is gone. That was my major concern.

"I can't quantify it. I just don't know how to quantify that. But I felt that the observations made were telling us that there was a message there telling us that temperature was a discriminator, and I couldn't get that point across. I basically had no direct input into the final recommendation to launch, and I

[24] Ibid., pp. 793–794.

was not polled. "I think Astronaut Crippin hit the tone of the meeting exactly right on the head when he said that the opposite was true of the way the meetings were normally conducted. We normally have to absolutely prove beyond a shadow of a doubt that we have the ability to fly, and it seemed like we were trying to prove, have proved that we had data to prove that we couldn't fly at this time, instead of the reverse. That was the tone of the meeting, in my opinion."[25]

Jerald Mason, senior vice president at Thiokol's Wasatch Division, directed the caucus at Thiokol. Mason continuously asserted that a management decision was needed and instructed Bob Lund, vice president for engineering, to take off his engineering hat and put on his management hat. During testimony, Mason commented on his interpretation of the data:

Dr. Ride [a member of the Commission]: "You know, what we've seen in the charts so far is that the data was inconclusive and so you said go ahead."

Mr. Mason: ". . . I hope I didn't convey that. But the reason for the discussion was the fact that we didn't have enough data to quantify the effect of the cold, and that was the heart of our discussion. . . . We have had blow-by on earlier flights. We had not had any reason to believe that we couldn't experience it again at any temperature. . . ."[26]

At the end of the second teleconference, NASA's Hardy at Marshall Space Flight Center requested that Thiokol put their recommendation to launch in writing and fax it to both Marshall Space Flight Center and Kennedy Space Center. The list that follows is from a memo that was signed by Joe Kilminster, vice president for Thiokol's Space Booster Program, and faxed at 11:45 p.m. the night before the launch.

- Calculations show that SRM-25 O-rings will be 20° colder than SRM-15 O-rings.
- Temperature data not conclusive on predicting primary O-ring blow-by.

Engineering assessment is that:

- Colder O-rings will have increased effective durometer ("harder").
- "Harder" O-rings will take longer to "seat."
  - More gas may pass primary O-ring before the primary seal seats (relative to SRM-15).

---

[25] Ibid., p. 676.
[26] Ibid., p. 764.

- Demonstrated sealing threshold is three times greater than 0.038″ erosion experienced on SRM-15.
- If the primary seal does not seat, the secondary seal will seat.
  - Pressure will get to secondary seal before the metal parts rotate.
  - O-ring pressure leak check places secondary seal in outboard position, which minimizes sealing time.
- MTI recommends STS-51L launch proceed on 28 January 1986.
  - SRM-25 will not be significantly different from SRM-15.[27]

THE ICE PROBLEM

At 1:30 a.m. on the day of the launch, NASA's Gene Thomas, launch director, ordered a complete inspection of the launch site due to cold weather and severe ice conditions. The prelaunch inspection of the *Challenger* and the launch pad by the ice team was unusual, to say the least. The ice team's responsibility was to remove any frost or ice on the vehicle or launch structure. What they found during their inspection looked like something out of a science fiction movie. The freeze-protection plan implemented by Kennedy personnel had gone very wrong. Hundreds of icicles, some up to 16 inches long, clung to the launch structure. The handrails and walkways near the shuttle entrance were covered in ice, making them extremely dangerous if the crew had to make an emergency evacuation. One solid sheet of ice stretched from the 195-foot level to the 235-foot level on the gantry. However, NASA continued to cling to its calculations that there would be no damage due to flying ice shaken loose during the launch.[28] A decision was then made to delay the launch from 9:38 a.m. to 11:30 a.m. so that the ice on the launch pad could melt. The delay was still within the launch window of 9:30 a.m.–12:30 p.m.

At 8:30 a.m., a second ice inspection was made. Ice was still significantly present at the launch site. Robert Glaysher, vice president for orbital operations at Rockwell, stated that the launch was unsafe. Rockwell's concern was that falling ice could damage the heat tiles on the orbiter. This could have a serious impact during reentry.

At 10:30 a.m., a third ice inspection was made. Though some of the ice was beginning to melt, there was still significant ice on the launch pad. The temperature of the left SRB was measured at 33°F and the right booster was measured at 19°F. Even though the right booster was 34 degrees colder than Thiokol's original recommendation for a launch temperature (i.e., 53°F), no one seemed alarmed. Rockwell also agreed to launch, even though its earlier statement had been that the launch was unsafe.

---

[27] Ibid., p. 764.
[28] Hoover and Wallace, "Studies in Ethics, Safety and Liability for Engineers," p. 5.

Arnold Aldrich, manager of the STS Program at the Johnson Space Center, testified on the concern over the ice problem:

Mr. Aldrich: "Kennedy facility people at that meeting, everyone in that meeting, voted strongly to proceed and said they had no concern, except for Rockwell. The comment to me from Rockwell, which was not written specifically to the exact words, and either recorded or logged, was that they had some concern about the possibility of ice damage to the orbiter. Although it was a minor concern, they felt that we had no experience base launching in this exact configuration before, and therefore they thought we had some additional risk of orbiter damage from ice than we had on previous meetings, or from previous missions."

Chairman Rogers: "Did they sign off on it or not?"

Mr. Aldrich: "We don*'t have* a sign-off at that point. It was not—it was not maybe 20 minutes, but it was close to that. It was within the last hour of launch."

Chairman Rogers: "But they still objected?"

Mr. Aldrich: "They issued what I would call a concern, a less than 100 percent concurrence in the launch. They did not say we do not want to launch, and the rest of the team overruled them. They issued a more conservative concern. They did not say don't launch."

General Kutyna: "I can't recall a launch that I have had where there was 100 percent certainty that everything was perfect, and everyone around the table would agree to that. It is the job of the launch director to listen to everyone, and it's our job around the table to listen and say there is this element of risk, and you characterize this as 90 percent, or 95, and then you get a consensus that that risk is an acceptable risk, and then you launch.

"So I think this gentleman is characterizing the degree of risk, and he's honest, and he had to say something."

Dr. Ride: "But one point is that their concern is a specific concern, and they weren't concerned about the overall temperature or damage to the solid rockets or damage to the external tank. They were worried about pieces of ice coming off and denting the tile."[29]

Following the accident, the Rogers Commission identified three major concerns about the ice-on-the-pad issue:

1. An analysis of all of the testimony and interviews established that Rockwell's recommendation on launch was ambiguous. The Commission found it difficult, as did Mr. Aldrich, to conclude that there was a

[29] Ibid., pp. 237–238.

no-launch recommendation. Moreover, all parties were asked specifically to contact Aldrich or Moore about launch objections due to weather. Rockwell made no phone calls or further objections to Aldrich or other NASA officials after the 9:00 a.m. Mission Management Team meeting and subsequent to the resumption of the countdown.

2. The Commission was also concerned about the NASA response to the Rockwell position at the 9:00 a.m. meeting. While it was understood that decisions have to be made in launching a Shuttle, the Commission was not convinced Levels I and II of NASA's management appropriately considered Rockwell's concern about the ice. However ambiguous Rockwell's position was, it was clear that they did tell NASA that the ice was an unknown condition. Given the extent of the ice on the pad, the admitted unknown effect of the Solid Rocket Motor and Space Shuttle Main Engines ignition on the ice, as well as the fact that debris striking the orbiter was a potential flight safety hazard, the Commission found the decision to launch questionable under those circumstances. In this situation, NASA appeared to be requiring a contractor to prove that it was not safe to launch, rather than proving it was safe. Nevertheless, the Commission had determined that the ice was not a cause of the 51-L accident and does not conclude that NASA's decision to launch specifically overrode a no-launch recommendation by an element contractor.
3. The Commission concluded that the freeze protection plan for launch pad 39B was inadequate. The Commission believed that the severe cold and presence of so much ice on the fixed service structure made it inadvisable to launch on the morning of January 28, and that margins of safety were whittled down too far.

It became obvious that NASA's management knew of the ice problem, but did they know of Thiokol's original recommendation not to launch and then its reversal? Larry Malloy, the SRB project manager for NASA, and Stanley Reinartz, NASA's manager of the Shuttle Office, both admitted that they told Arnold Aldrich, manager of the STS program, Johnson Space Center, about their concern for the ice problem, but there was no discussion about the teleconferences with Thiokol over the O-rings. It appeared that Malloy and Reinartz considered the ice as a potential problem whereas the O-rings constituted an acceptable risk. Therefore, only potential problems went up the chain of command, not the components of the "aggregate acceptable launch risk." It became common practice in FRR documentation to use the term "acceptable risk." This became the norm at NASA and resulted in insulating senior management from certain potential problems. The culture that had developed at NASA created the flawed decision-making process rather than an intent by individuals to withhold information and jeopardize safety.

THE ACCIDENT

Just after liftoff at 0.678 seconds into the flight, photographic data showed a strong puff of gray smoke spurting from the vicinity of the aft field joint on the right SRB. The two pad 39B cameras that would have recorded the precise location of the puff were inoperative. Computer graphic analysis of film from other cameras indicated the initial smoke came from the 270- to 310-degree sector of the circumference of the aft field joint of the right SRB. This area of the solid booster faced the external tank. The vaporized material streaming from the joint indicated there was incomplete sealing action within the joint.

Eight more distinctive puffs of increasingly blacker smoke were recorded between 0.836 and 2.500 seconds. The smoke appeared to puff upward from the joint. While each smoke puff was being left behind by the upward flight of the shuttle, the next fresh puff could be seen near the level of the joint. The multiple smoke puffs in this sequence occurred about four times per second, approximating the frequency of the structural load dynamics and resultant joint flexing. Computer graphics applied to NASA photos from a variety of cameras in this sequence again placed the smoke puffs' origin in the same 270- to 310-degree sector of the circumference as the original smoke spurt.

As the shuttle *Challenger* increased its upward velocity, it flew past the emerging and expanding smoke puffs. The last smoke was seen above the field joint at 2.733 seconds.

The black color and dense composition of the smoke puffs suggested that the grease, joint insulation, and rubber O-rings in the joint seal were being burned and eroded by the hot propellant gases.

At approximately 37 seconds, *Challenger* encountered the first of several high-altitude wind-shear conditions that lasted about 64 seconds. The wind shear created forces of relatively large fluctuations on the vehicle itself. These were immediately sensed and countered by the guidance, navigation, and control systems.

The steering system (thrust vector control) of the SRB responded to all commands and wind-shear effects. The wind shear caused the steering system to be more active than on any previous flight.

Both the *Challenger*'s main engines and the solid rockets operated at reduced thrust approaching and passing through the area of maximum dynamic pressure of 720 pounds per square foot. Main engines had been throttled up to 104 percent thrust, and the SRBs were increasing their thrust when the first flickering flame appeared on the right SRB in the area of the aft field joint. This first very small flame was detected on image-enhanced film at 58.788 seconds into the flight. It appeared to originate at about 305 degrees around the booster circumference at or near the aft field joint.

One film frame later from the same camera, the flame was visible without image enhancement. It grew into a continuous, well-defined plume at 59.262

seconds. At approximately the same time (60 seconds), telemetry showed a pressure differential between the chamber pressures in the right and left boosters. The right booster chamber pressure was lower, confirming the growing leak in the area of the field joint.

As the flame plume increased in size, it was deflected rearward by the aerodynamic slipstream and circumferentially by the protruding structure of the upper ring attaching the booster to the external tank. These deflections directed the flame plume onto the surface of the external tank. This sequence of flame spreading is confirmed by analysis of the recovered wreckage. The growing flame also impinged on the strut attaching the SRB to the external tank.

The first visual indication that swirling flame from the right SRB breached the external tank was at 64.660 seconds, when there was an abrupt change in the shape and color of the plume. This indicated that it was mixing with leaking hydrogen from the external tank. Telemetered changes in the hydrogen tank pressurization confirmed the leak. Within 45 milliseconds of the breach of the external tank, a bright, sustained glow developed on the black tiled underside of the *Challenger* between it and the external tank.

Beginning around 72 seconds, a series of events occurred extremely rapidly that terminated the flight. Telemetered data indicated a wide variety of flight system actions that supported the visual evidence of the photos as the shuttle struggled futilely against the forces that were destroying it.

At about 72.20 seconds, the lower strut linking the SRB and the external tank was severed or pulled away from the weakened hydrogen tank, permitting the right SRB to rotate around the upper attachment strut. This rotation was indicated by divergent yaw and pitch rates between the left and right SRBs.

At 73.124 seconds, a circumferential white vapor pattern was observed blooming from the side of the external tank bottom dome. This was the beginning of the structural failure of the hydrogen tank that culminated in the entire aft dome dropping away. This released massive amounts of liquid hydrogen from the tank and created a sudden forward thrust of about 2.8 million pounds, pushing the hydrogen tank upward into the intertank structure. About the same time, the rotating right SRB impacted the intertank structure and the lower part of the liquid oxygen tank. These structures failed at 73.137 seconds, as evidenced by the white vapors appearing in the intertank region.

Within milliseconds there was massive, almost explosive, burning of the hydrogen streaming from the failed tank bottom and the liquid oxygen breach in the area of the intertank.

At this point in its trajectory, while traveling at a Mach number of 1.92 at an altitude of 46,000 feet, the *Challenger* was totally enveloped in the explosive burn. The *Challenger*'s reaction control system ruptured, and a hypergolic burn of its propellants occurred, producing the oxygen-hydrogen flames. The reddish brown colors of the hypergolic fuel burn were visible on the edge of the main

fireball. The orbiter, under severe aerodynamic loads, broke into several large sections, which emerged from the fireball. Separate sections that can be identified on film include the main engine/tail section with the engines still burning, one wing of the orbiter, and the forward fuselage trailing a mass of umbilical lines pulled loose from the payload bay.

The consensus of the Commission and participating investigative agencies was that the loss of the space shuttle *Challenger* was caused by a failure in the joint between the two lower segments of the right solid rocket motor. The specific failure was the destruction of the seals that were intended to prevent hot gases from leaking through the joint during the propellant burn of the rocket motor. The evidence assembled by the Commission indicates that no other element of the space shuttle system contributed to this failure.

In arriving at this conclusion, the Commission reviewed in detail all available data, reports, and records; directed and supervised numerous tests, analyses, and experiments by NASA, civilian contractors, and various government agencies; and then developed specific failure scenarios and the range of most probably causative factors.

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 joint to dynamic loading.

NASA AND THE MEDIA

Following the tragedy, many believed that NASA's decision to launch had been an attempt to minimize further ridicule by the media. Successful shuttle flights were no longer news because they were almost ordinary. However, launch aborts and delayed landings were more newsworthy because they were less common. The *Columbia* launch, which had immediately preceded the *Challenger* mission, had been delayed seven times. The *Challenger* launch had gone through four delays already. News anchor personnel were criticizing NASA. Some believed that NASA felt it had to do something quickly to dispel its poor public image.

The *Challenger* mission had had more media coverage and political ramifications than other recent missions. This would be the launch of the Teacher in Space Project. The original launch date of the *Challenger* had been scheduled just before President Reagan's State of the Union message, which was to be delivered the evening of January 28. Some believed that the president had intended to publicly praise NASA for the Teacher in Space Project and possibly even talk to Ms. McAuliffe live during his address. This would certainly have enhanced NASA's image. Following the tragedy, there were questions as to whether the White House had pressured NASA into launching the shuttle because of President Reagan's (and NASA's) love of favorable publicity. The Commission, however, found no evidence of White House intervention in the decision to launch.

FINDINGS OF THE COMMISSION

Determining the cause of an engineering disaster can take years of investigation. The *Challenger* disaster arose from many factors, including launch conditions, mechanical failure, faulty communication, and poor decision making. In the end, the last-minute decision to launch combined all possible factors into a lethal action.

The Commission concluded that the accident was rooted in history. The space shuttle's SRB problem began with the faulty design of its joint and increased as both NASA and contractor management first failed to recognize that they had a problem, then failed to fix it, and finally treated it as an acceptable flight risk.

Morton Thiokol, Inc., the contractor, did not accept the implication of tests early in the program that the design had a serious and unanticipated flaw. NASA did not accept the judgment of its engineers that the design was unacceptable, and as the joint problems grew in number and severity, NASA minimized them in management briefings and reports. Thiokol's stated position was that "the condition is not desirable but is acceptable."

Neither Thiokol nor NASA expected the rubber O-rings sealing the joints to be touched by hot gases of motor ignition, much less to be partially burned. However, as tests and then flights confirmed damage to the sealing rings, the reaction by both NASA and Thiokol was to increase the amount of damage considered "acceptable." At no time did management either recommend a redesign of the joint or call for the shuttle's grounding until the problem was solved.

The genesis of the *Challenger* accident—the failure of the joint of the right solid rocket motor—lay in decisions made in the design of the joint and in the failure by both Thiokol and NASA's Solid Rocket Booster project office to understand and respond to facts obtained during testing.

The Commission concluded that neither Thiokol nor NASA had responded adequately to internal warnings about the faulty seal design. Furthermore, Thiokol and NASA did not make a timely attempt to develop and verify a new seal after the initial design was shown to be deficient. Neither organization developed a solution to the unexpected occurrences of O-ring erosion and blow-by, even though this problem was experienced frequently during the shuttle flight history. Instead, Thiokol and NASA management came to accept erosion and blow-by as unavoidable and an acceptable flight risk. Specifically, the Commission found six things:

1. The joint test and certification program was inadequate. There was no requirement to configure the qualifications test motor as it would be in flight, and the motors were static tested in a horizontal position, not in the vertical flight position.
2. Prior to the accident, neither NASA nor Thiokol fully understood the mechanism by which the joint sealing action took place.

3. NASA and Thiokol accepted escalating risk apparently because they "got away with it last time." As Commissioner Feynman observed, the decision making was:

> A kind of Russian roulette. . . . [The shuttle] flies [with O-ring erosion] and nothing happens. Then it is suggested, therefore, that the risk is no longer so high for the next flights. We can lower our standards a little bit because we got away with it last time. . . . You got away with it, but it shouldn't be done over and over again like that.

4. NASA's system for tracking anomalies for Flight Readiness Reviews failed in that, despite a history of persistent O-ring erosion and blow-by, flight was still permitted. It failed again in the strange sequence of six consecutive launch constraint waivers prior to 51-L, permitting it to fly without any record of a waiver, or even of an explicit constraint. Tracking and continuing only anomalies that are outside the database of prior flight allowed major problems to be removed from, and lost by, the reporting system.
5. The O-ring erosion history presented to Level I at NASA Headquarters in August 1985 was sufficiently detailed to require corrective action prior to the next flight.
6. A careful analysis of the flight history of O-ring performance would have revealed the correlation of O-ring damage and low temperature. Neither NASA nor Thiokol carried out such an analysis; consequently, they were unprepared to properly evaluate the risks of launching the 51-L mission in conditions more extreme than they had encountered before.

The Commission also identified a concern for the "silent" safety program. The Commission was surprised to realize after many hours of testimony that NASA's safety staff was never mentioned. No witness related the approval or disapproval of the reliability engineers, and none expressed the satisfaction or dissatisfaction of the quality assurance staff. No one thought to invite a safety representative or a reliability and quality assurance engineer to the January 27, 1986, teleconference between Marshall and Thiokol. Similarly, there was no safety representative on the Mission Management Team that made key decisions during the countdown on January 28, 1986.

The unrelenting pressure to meet the demands of an accelerating flight schedule might have been handled adequately by NASA if it had insisted on the exactingly thorough procedures that had been its hallmark during the *Apollo* program. An extensive and redundant safety program comprising interdependent safety, reliability, and quality assurance functions had existed during the lunar program to discover any potential safety problems. Between that period and 1986, however, the safety program had become ineffective. This loss of effectiveness seriously degraded the checks and balances essential for maintaining flight safety. On April 3, 1986, Arnold Aldrich, the Space Shuttle Program manager, appeared before the

Commission at a public hearing in Washington, D.C. He described five different communication or organization failures that affected the launch decision on January 28, 1986. Four of those failures related directly to faults within the safety program. These faults included a lack of problem reporting requirements, inadequate trend analysis, misrepresentation of criticality, and lack of involvement in critical discussions. A robust safety organization that was properly staffed and supported might well have avoided these faults, and thus eliminated the communication failures.

NASA had a safety program to ensure that the communication failures to which Mr. Aldrich referred did not occur. In the case of Mission 51-L, however, that program fell short.

The Commission concluded that there were severe pressures placed on the launch decision-making system to maintain a flight schedule. These pressures caused rational men to make irrational decisions.

With the 1982 completion of the orbital flight test series, NASA began a planned acceleration of the space shuttle launch schedule. One early plan contemplated an eventual rate of a mission a week, but realism forced several downward revisions. In 1985, NASA published a projection calling for an annual rate of 24 flights by 1990. Long before the *Challenger* accident, however, it was becoming obvious that even the modified goal of two flights a month was overambitious.

In establishing the schedule, NASA had not provided adequate resources. As a result, the capabilities of the launch decision-making system were strained by the modest nine-mission rate of 1985, and evidence suggested that NASA would not have been able to accomplish the 15 flights scheduled for 1986. These were the major conclusions of a Commission examination of the pressures and problems attendant upon the accelerated launch schedule:

1. The capabilities of the launch decision-making system were stretched to the limit to support the flight rate in winter 1985/1986. Projections into the spring and summer of 1986 showed a clear trend; the system, as it existed, would have been unable to deliver crew training software for scheduled flights by the designated dates. The result would have been an unacceptable compression of the time available for the crews to accomplish their required training.
2. Parts were in critically short supply. The shuttle program made a conscious decision to postpone spare parts procurements in favor of budget items of perceived higher priority. Lack of spare parts would likely have limited flight operations in 1986.
3. Stated manifesting policies were not enforced. Numerous late manifest changes (after the cargo integration review) had been made to both major payloads and minor payloads throughout the shuttle program:
   - Late changes to major payloads or program requirements required extensive resources (money, manpower, facilities) to implement.

- If many late changes to "minor" payloads occurred, resources were quickly absorbed.
- Payload specialists frequently were added to a flight well after announced deadlines.
- Late changes to a mission adversely affected the training and development of procedures for subsequent missions.

4. The scheduled flight rate did not accurately reflect the capabilities and resources.
   - The flight rate was not reduced to accommodate periods of adjustment in the capacity of the workforce. There was no margin for error in the system to accommodate unforeseen hardware problems.
   - Resources were directed primarily toward supporting the flights; thus, not enough were available to improve and expand facilities needed to support a higher flight rate.
5. Training simulators may have been the limiting factor on the flight rate: The two simulators available at that time could not train crews for more than 12 to 15 flights per year.
6. When flights came in rapid succession, the requirements then current did not ensure that critical anomalies occurring during one flight would be identified and addressed appropriately before the next flight.

CHAIN-OF-COMMAND COMMUNICATION FAILURE

The Commission also identified a communication failure within the reporting structure at both NASA and Thiokol. Part of the problem with the chain-of-command structure was the idea of the proper reporting channel. Engineers report only to their immediate managers, while those managers report only to their direct supervisors. Engineers and managers believed in the chain-of-command structure; they felt reluctant to go above their superiors with their concerns. Boisjoly at Thiokol and Powers at Marshall felt that they had done all that they could as far as voicing their concerns. Anything more could have cost them their jobs. When questioned at the Rogers Commission hearing about why he did not voice his concerns to others, Powers replied, "That would not be my reporting channel." The chain-of-command structure dictated the only path that information could travel at both NASA and Thiokol. If information was modified or silenced at the bottom of the chain, there was not an alternate path for it to take to reach high-level officials at NASA. The Rogers Commission concluded that there was a breakdown in communication between Thiokol engineers and top NASA officials and faulted the management structure for not allowing important information about the SRBs to flow to the people who needed to know it. The Commission reported that the "fundamental problem was poor technical decision-making over a period of several years by top NASA and contractor personnel."

Bad news does not travel well in organizations like NASA and Thiokol. When the early signs of problems with the SRBs appeared, Thiokol managers did not believe that the problems were serious. Thiokol did not want to accept the fact that there could be a problem with its boosters. When Marshall received news of the problems, it considered it Thiokol's problem and did not pass the bad news upward to NASA headquarters. At Thiokol, Boisjoly described his managers as shutting out the bad news. He claims that he argued about the importance of the O-ring seal problems until he was convinced that "no one wanted to hear what he had to say." When Lund finally decided to recommend delay of the launch to Marshall, managers at Marshall rejected the bad news and refused to accept the recommendation not to launch. As with any information going up the chain of command at these two organizations, bad news was often modified so that it had less impact, perhaps skewing its importance.[30]

On January 31, 1986, President Ronald Reagan stated:

> The future is not free: the story of all human progress is one of a struggle against all odds. We learned again that this America, which Abraham Lincoln called the last, best hope of man on Earth, was built on heroism and noble sacrifice. It was built by men and women like our seven star voyagers, who answered a call beyond duty, who gave more than was expected or required and who gave it with little thought of worldly reward.[31]

EPILOGUE

Following the tragic accident, virtually every senior manager involved in the space shuttle *Challenger* decision-making processes, at both NASA and Thiokol, accepted early retirement. Whether this was the result of media pressure, peer pressure, fatigue, or stress. we can only postulate. The only true failures are the ones from which nothing is learned. Lessons on how to improve the risk management process were learned, unfortunately at the expense of human life.

On January 27, 1967, Astronauts Gus Grissom, Edward White, and Roger Chaffee were killed on board a test on *Apollo-Saturn 204.* James Webb, NASA's administrator at that time, was allowed by President Johnson to conduct an internal investigation of the cause. The investigation was primarily a technical investigation. NASA was fairly open with the media during the investigation. As a result of the openness, the credibility of the agency was maintained.

---

[30] "The *Challenger* Accident: Administrative Causes of the *Challenger* Accident," http://www.me.utexas.edu/~uer/challenger/chall3.html, pp. 8–9.

[31] "Transcript of the President's Eulogy for the Seven Challenger Astronauts." *New York Times*, February 1, 1986. Available at www.nytimes.com/1986/02/01/us/transcript-of-the-president-s-eulogy-for-the-seven-challenger-astronauts.html.

With the *Challenger* accident, confusion arose as to whether it had been a technical failure or a management failure. There was no question in anyone's mind that the decision-making process was flawed. NASA and Thiokol acted independently in their response to criticism. Critical information was withheld, at least temporarily, and this undermined people's confidence in NASA. The media, as might have been expected, began vengeful attacks on NASA and Thiokol.

Following the *Apollo-Saturn 204* fire, few changes were made in management positions at NASA. Those changes that did occur were the result of a necessity for improvement and where change was definitely warranted. Following the *Challenger* accident, almost every top management position at NASA underwent a change of personnel.

How an organization fares after an accident is often measured by how well it interfaces with the media. Situations such as the Tylenol tragedy (subject of another case study in this volume) and the *Apollo-Saturn 204* fire bore this out.

Following the accident and after critical data were released, papers were published showing that the O-ring data correlation was indeed possible. In one such paper, Frederick Lighthall showed that not only was a correlation possible, but the real problem may be a professional weakness shared by many people, but especially engineers, who are required to analyze technical data.[32] Lighthall's argument was that engineering curriculums might not provide engineers with strong enough statistical education, especially in covariance analysis. The Rogers Commission also identified this conclusion when they found that there were no engineers at NASA trained in statistical sciences.

Almost all scientific achievements require the taking of risks. The hard part is deciding which risk is worth taking and which is not. Every person who has ever flown in space, whether military or civilian, was a volunteer. They were all risk takers who understood that safety in space can never be guaranteed with 100 percent accuracy.

QUESTIONS

Following are a series of questions categorized according to the principles of risk management. There may not be any single right or wrong answer to these questions.

Risk Management Plan

1. Does it appear, from the data provided in the case, that a risk management plan was in existence?

---

[32] Frederick F. Lighthall, "Launching the Space Shuttle *Challenger*: Disciplinary Deficiencies in the Analysis of Engineering Data," *IEEE Transactions on Engineering Management* 38, no. 1 (February 1991): 63–74.

2. If such a plan did exist, then why wasn't it followed—or was it followed?
3. Is there a difference between a risk management plan, a quality assurance plan, and a safety plan, or are they the same?
4. Would there have been a better way to handle risk management planning at NASA assuming 16 flights per year, 25 flights per year, or as originally planned, 60 flights per year? Why is the number of flights per year critical in designing a formalized risk management plan?

Risk Identification

1. What is the difference between a risk and an anomaly? Who determines the difference?
2. Does there appear to have been a structured process in place for risk identification at either NASA or Thiokol?
3. How should problems with risk identification be resolved if there exist differences of opinion between the customer and the contractors?
4. Should senior management or sponsors be informed about all risks identified or just the overall "aggregate" risk?
5. How should one identify or classify the risks associated with using solid rocket boosters on manned spacecraft rather than the conventional liquid-fuel boosters?
6. How should one identify or classify trade-off risks, such as trading off safety for political acceptability?
7. How should one identify or classify the risks associated with pressure resulting from making promises that may be hard to keep?
8. Suppose that a risk identification plan had been established at the beginning of the space program when the shuttle was still considered an experimental design. If the shuttle is now considered an operational vehicle rather than an experimental design, could that affect the way that risks were identified to the point where the risk identification plan would need to be changed?

Risk Quantification

1. Given the complexity of the Space Shuttle Program, is it feasible and/or practical to develop a methodology for quantifying risks, or should each situation be addressed individually? Can we have both a quantitative and qualitative risk evaluation system in place at the same time?
2. How does one quantify the dangers associated with the ice problem?
3. How should risk quantification problems be resolved if there exist differences of opinion between the customer and the contractors?
4. If a critical risk is discovered, what is the proper way for the project manager to present to senior management the impact of the risk? How do you as a project manager make sure that senior management understand the ramifications?

5. How were the identified risks quantified at NASA? Is the quantification system truly quantitative or is it a qualitative system?
6. Were probabilities assigned to any of the risks? Why or why not?

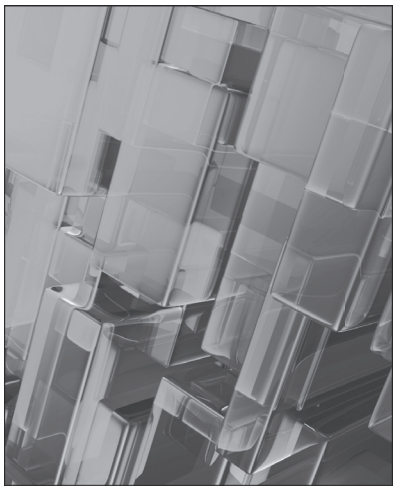
Risk Response (Risk Handling)

1. How does an organization decide what is or is not an acceptable risk?
2. Who should have final say in deciding upon the appropriate response mechanism for a risk?
3. What methods of risk response were used at NASA?
4. Did it appear that the risk response method selected was dependent on the risk or on other factors?
5. How should an organization decide whether or not to accept a risk and launch if the risks cannot be quantified?
6. What should be the determining factors in deciding which risks are brought upstairs to the executive levels for review before selecting the appropriate risk response mechanism?
7. Why weren't the astronauts involved in the launch decision (i.e., the acceptance of the risk)? Should they have been involved?
8. What risk response mechanism did NASA administrators use when they issued waivers for the Launch Commit Criteria?
9. Are waivers a type of risk response mechanism?
10. Did the need to maintain a flight schedule compromise the risk response mechanism that would otherwise have been taken?
11. What risk response mechanism were managers at Thiokol and NASA using when they ignored the recommendations of their engineers?
12. Did the engineers at Thiokol and NASA do all they could to convince their own management that the wrong risk response mechanism was about to be taken?
13. When NASA pressed its contractors to recommend a launch, did NASA's risk response mechanism violate their responsibility to ensure crew safety?
14. When NASA discounted the effects of the weather, did NASA's risk response mechanism violate their responsibility to ensure crew safety?

Risk Control

1. How much documentation should be necessary for the tracking of a risk management plan? Can this documentation become excessive and create decision-making problems?
2. Risk management includes the documentation of lessons learned. In the case study, was there an audit trail of lessons learned, or was that audit trail simply protection memos?

3. How might Thiokol engineers have convinced both their own management and NASA to postpone the launch?
4. Should someone have stopped the *Challenger* launch, and, if so, how could this have been accomplished without risking one's job and career?
5. How might an engineer deal with pressure from above to follow a course of action that the engineer knows to be wrong?
6. How could the chains of communication and responsibility for the Space Shuttle Program have been made to function better?
7. Because of the ice problem, Rockwell could not guarantee the shuttle's safety but did nothing to veto the launch. Is there a better way for situations as this to be handled in the future?
8. What level of risk should have been acceptable for launch?
9. How should we handle situations where people in authority believe that the potential rewards justify what they believe to be relatively minor risks?
10. If you were on a jury attempting to place liability, whom would you say was responsible for the *Challenger* disaster?



Packer Telecom

BACKGROUND

The rapid growth of the telecom industry made it apparent to Packer's executives that risk management must be performed on all development projects. If Packer was late in the introduction of a new product, then market share would be lost. Furthermore, Packer could lose valuable opportunities to partner with other companies if Packer was regarded as being behind the learning curve with regard to new product development.

Another problem facing Packer was the amount of money being committed to R&D. Typical companies spend 8 to 10 percent of earnings on R&D, whereas in the telecom industry, the number may be as high as 15 to 18 percent. Packer was spending 20 percent on R&D, and only a small percentage of the projects that started out in the conceptual phase ever reached the commercialization phase, where Packer could expect to recover its R&D costs. Management attributed the problem to a lack of effective risk management.

THE MEETING

PM: "I have spent a great deal of time trying to benchmark best practices in risk management. I was amazed to find that most companies are in the same boat as us, with very little knowledge in risk management. From the limited results I have found from other companies, I have been able to develop a risk management template for us to use."

Sponsor: "I've read over your report and looked at your templates. You have words and expressions in the templates that we don't use here at Packer. This concerns me greatly. Do we have to change the way we manage projects to use these templates? Are we expected to make major changes to our existing project management methodology?"

PM: "I was hoping we could use these templates in their existing format. If the other companies are using these templates, then we should also. These templates also have the same probability distributions that other companies are using. I consider these facts equivalent to a validation of the templates."

Sponsor: "Shouldn't the templates be tailored to our methodology for managing projects and our life-cycle phases? These templates may have undergone validation, but not at Packer. The probability distributions are also based on someone else's history, not our history. I cannot see anything in your report that talks about the justification of the probabilities.

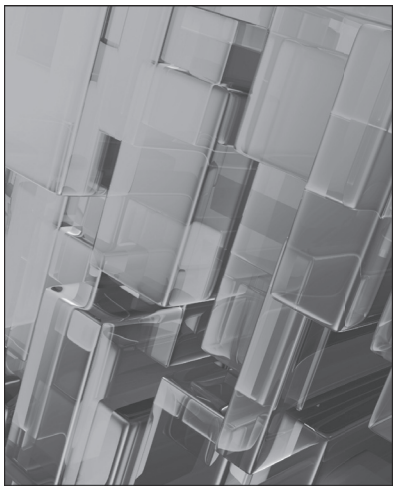
"The final problem I have is that the templates are based on history. It is my understanding that risk management should be forward looking, with an attempt at predicting the possible future outcomes. I cannot see any of this in your templates."

PM: "I understand your concerns, but I don't believe they are a problem. I would prefer to use the next project as a 'breakthrough project' using these templates. This will give us a good basis to validate the templates."

Sponsor: "I will need to think about your request. I am not sure that we can use these templates without some type of risk management training for our employees."

QUESTIONS

1. Can templates be transferred from one company to another, or should tailoring be mandatory?
2. Can probability distributions be transferred from one company to another? If not, then how do we develop a probability distribution?
3. How do you validate a risk management template?
4. Should a risk management template be forward looking?
5. Can employees begin using a risk management template without some form of specialized training?



Luxor Technologies

Between 1992 and 1996, Luxor Technologies had seen their business almost quadruple in the wireless communications area. Luxor's success was attributed largely to the strength of its technical community, which was regarded as second to none. The technical community was paid very well and given the freedom to innovate. Even though Luxor's revenue came from manufacturing, Luxor was regarded by Wall Street as being a technology-driven company.

The majority of Luxor's products were based on low-cost, high-quality applications of the state-of-the-art technology rather than advanced state-of-the-art technological breakthroughs. Applications engineering and process improvement were major strengths at Luxor. Luxor possessed patents in technology breakthrough, applications engineering, and even process improvement. Luxor refused to license its technology to other firms, even if the applicant was not a major competitor.

Patent protection and design secrecy were of paramount importance to Luxor. In this regard, Luxor became vertically integrated, manufacturing and assembling all components of its products internally. Only off-the-shelf components were purchased. Luxor believed that if it were to use outside vendors for sensitive component procurement, they would have to release critical and proprietary data to the vendors. Since these vendors most likely also serviced Luxor's competitors, Luxor maintained the approach of vertical integration to maintain secrecy.

Being the market leader technically afforded Luxor certain luxuries. Luxor saw no need for expertise in technical risk management. In cases where the

technical community was only able to achieve 75 to 80 percent of the desired specification limit, the product was released as it stood, accompanied by an announcement that there would be an upgrade the following year to achieve the remaining 20 to 25 percent of the specification limit, together with other features. Enhancements and upgrades were made on a yearly basis.

By the fall of 1996, however, Luxor's fortunes were diminishing. The competition was catching up quickly, thanks to major technological breakthroughs. Marketing estimated that, by 1998, Luxor would be a follower rather than a market leader. Luxor realized that something must be done, and quickly.

In January 1999, Luxor hired an expert in risk analysis and risk management to help it assess the potential damage to the firm and to assist in development of a mitigation plan. The consultant reviewed project histories and lessons learned on all projects undertaken from 1992 through 1998. The consultant concluded that the major risk to Luxor would be the technical risk and prepared Tables I and II. Table I shows the likelihood of a technical risk event occurring. The consultant identified the six most common technical risk events that could occur at Luxor over the next several years, based on the extrapolation of past and present data into the future. Table II shows the impact that a technical risk event could have on each project. Because of the high probability of state-of-the-art advancements needed in the future (i.e., 95 percent from Table I), the consultant identified the impact probabilities in Table II for both with and without state-of-the-art advancement needed.

Tables I and II confirmed management's fear that Luxor was in trouble. A strategic decision had to be made concerning the technical risks identified in Table I, specifically the first two risks. The competition had caught up to Luxor in applications engineering and was now surpassing Luxor in patents involving state-of-the-art advancements. From 1992 to 1998, time was considered a luxury for the technical community at Luxor. Now time was a serious constraint.

The strategic decision facing management was whether Luxor should struggle to remain a technical leader in wireless communications technology or simply

TABLE I LIKELIHOOD OF A TECHNICAL RISK

Event	Likelihood Rating
State-of-the-art advance needed	0.95
Scientific research required(without advancements)	0.80
Concept formulation	0.40
Prototype development	0.20
Prototype testing	0.15
Critical performance demonstrated	0.10

TABLE II IMPACT OF A TECHNICAL RISK EVENT

Event	Impact Rating	
	With State-of-the-Art Changes	**Without State-of-the-Art Changes**
Product performance not at 100% of specification	0.95	0.80
Product performance not at 75–80% of specification	0.75	0.30
Abandonment of project	0.70	0.10
Need for further enhancements	0.60	0.25
Reduced profit margins	0.45	0.10
Potential systems performance degradation	0.20	0.05

console itself with a future as a follower. Marketing was given the task of determining the potential impact of a change in strategy from a market leader to a market follower. The next list was prepared and presented to management by marketing:

1. The company's future growth rate will be limited.
2. Luxor will still remain strong in applications engineering but will need to outsource state-of-the-art development work.
3. Luxor will be required to provide outside vendors with proprietary information.
4. Luxor may no longer be vertically integrated (i.e., have backward integration).
5. Final product costs may be heavily influenced by the costs of subcontractors.
6. Luxor may not be able to remain a low-cost supplier.
7. Layoffs will be inevitable but perhaps not in the near term.
8. The marketing and selling of products may need to change. Can Luxor still market products as a low-cost, high-quality, state-of-the-art manufacturer?
9. Price-cutting by Luxor's competitors could have a serious impact on Luxor's future ability to survive.

The list presented by marketing demonstrated that there was a serious threat to Luxor's growth and even survival. Engineering then prepared a list of alternative courses of action that would enable Luxor to maintain its technical leadership position:

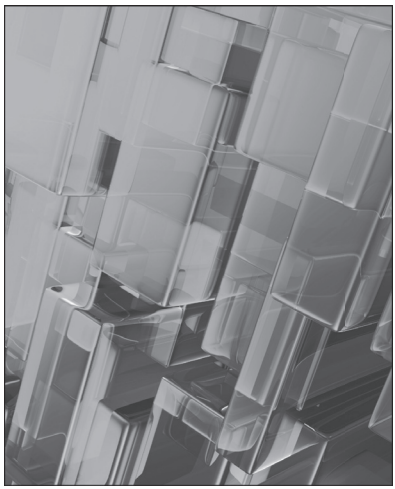
1. Luxor could hire away from the competition more staff personnel with pure and applied R&D skills. This would be a costly effort.

2. Luxor could slowly retrain part of its existing labor force using existing, experienced R&D personnel to conduct the training.
3. Luxor could fund seminars and university courses on general R&D methods as well as R&D methods for telecommunications projects. These programs were available locally.
4. Luxor could use tuition reimbursement funds to pay for distance learning courses (conducted over the Internet). These were full-semester programs.
5. Luxor could outsource technical development.
6. Luxor could purchase or license technology from other firms, including competitors. This assumed that competitors would agree to this at a reasonable price.
7. Luxor could develop joint ventures/mergers with other companies that, in turn, would probably require Luxor to disclose much of its proprietary knowledge.

With marketing's and engineering's lists before them, Luxor's management had to decide which path would be best for the long term.

QUESTIONS

1. Can the impact of one specific risk event, such as a technical risk event, create additional risks, which may or may not be technical risks? Can risk events be interrelated?
2. Does the list provided by marketing demonstrate the likelihood of a risk event or the impact of a risk event?
3. How does one assign probabilities to the marketing list?
4. The seven items in the list provided by engineering are all ways of mitigating certain risk events. If the company follows these suggestions, is it adopting a risk response mode of avoidance, assumption, reduction, or deflection?
5. Would you side with marketing or engineering? What should Luxor do at this point?



Altex Corporation

BACKGROUND

Following World War II, the United States entered into a Cold War with Russia. To win this Cold War, the United States had to develop sophisticated weapon systems with such destructive power that any aggressor knew that the retaliatory capability of the United States could and would inflict vast destruction.

Hundreds of millions of dollars were committed to ideas concerning technology that had not been developed as yet. Aerospace and defense contractors were growing without bounds, thanks to cost-plus-percentage-of-cost contract awards. Speed and technological capability were judged to be significantly more important than cost. To make matters worse, contracts were often awarded to the second or third most qualified bidder for the sole purpose of maintaining competition and maximizing the total number of defense contractors.

CONTRACT AWARD

During this period, Altex Corporation was elated when it learned that it had just been awarded the R&D phase of the Advanced Tactical Missile Program (ATMP). The terms of the contract specified that Altex had to submit to the Army, within 60 days after contract award, a formal project plan for the two-year ATMP effort. Contracts at that time did not require that a risk management plan be developed. A meeting was held with the project manager of R&D to assess the risks in the ATMP effort.

PM: "I'm in the process of developing the project plan. Should I also develop a risk management plan as part of the project plan?"

Sponsor: "Absolutely not! Most new weapon systems requirements are established by military personnel who have no sense of reality about what it takes to develop a weapon system based on technology that doesn't even exist yet. We'll be lucky if we can deliver 60–70 percent of the specification imposed on us."

PM: "But that's not what we stated in our proposal. I wasn't brought on board until after we won the award, so I wasn't privileged to know the thought process that went into the proposal. The proposal even went so far as to imply that we might be able to exceed the specification limits, and now you're saying that we should be happy with 60–70 percent."

Sponsor: "We say what we have to say to win the bid. Everyone does it. It is common practice. Whoever wins the R&D portion of the contract will also be first in line for the manufacturing effort and that's where the megabucks come from! If we can achieve 60–70 percent of specifications, it should placate the Army enough to give us a follow-on contract. If we told the Army the true cost of developing the technology to meet the specification limits, we would never get the contract. The program might even be canceled. The military people want this weapon system. They're not stupid! They know what is happening and they do not want to go to their superiors for more money until later on, downstream, after approval by Department of Defense and project kickoff. The government wants the lowest cost and we want long-term, follow-on production contracts, which can generate huge profits."

PM: "Aren't we simply telling lies in our proposal?"

Sponsor: "My engineers and scientists are highly optimistic and believe they can do the impossible. This is how technological breakthroughs are made. I prefer to call it 'overoptimism of technical capability' rather than 'telling lies.' If my engineers and scientists have to develop a risk management plan, they may become pessimistic, and that's not good for us!"

PM: "The problem with letting your engineers and scientists be optimistic is that they become reactive rather than proactive thinkers. Without proactive thinkers, we end up with virtually no risk management or contingency plans. When problems surface that require significantly more in the way of resources than we budgeted for, we will be forced to accept crisis management as a way of life. Our costs will increase and that's not going to make the Army happy."

Sponsor: "But the Army won't penalize us for failing to meet cost or for allowing the schedule to slip. If we fail to meet at least 60–70 percent of the specification limits, however, then we may well be in trouble. The Army knows there will be a follow-on contract request if we cannot meet specification limits. I consider 60–70 percent of the specifications to be the minimum acceptable limits for the Army. The Army wants the program kicked off right now.

"Another important point is that long-term contracts and follow-on production contracts allow us to build up a good working relationship with the Army. This is critical. Once we get the initial contract, as we did, the Army will always work with us for follow-on efforts. Whoever gets the R&D effort will almost always get the lucrative production contract. Military officers are under pressure to work with us because their careers may be in jeopardy if they have to tell their superiors that millions of dollars were awarded to the wrong defense contractor. From a career standpoint, the military officers are better off allowing us to downgrade the requirements than admitting that a mistake was made."

PM: "I'm just a little nervous managing a project that is so optimistic that major advances in the state of the art must occur to meet specifications. This is why I want to prepare a risk management plan."

Sponsor: "You don't need a risk management plan when you know you can spend as much as you want and also let the schedule slip. If you prepare a risk management plan, you will end up exposing a multitude of risks, especially technical risks. The Army might not know about many of these risks, so why expose them and open up Pandora's box? Personally, I believe that the Army does already know many of these risks, but does not want them publicized to their superiors.

"If you want to develop a risk management plan, then do it by yourself, and I really mean by yourself. Past experience has shown that our employees will be talking informally to Army personnel at least two to three times a week. I don't want anyone telling the customer that we have a risk management plan. The customer will obviously want to see it, and that's not good for us.

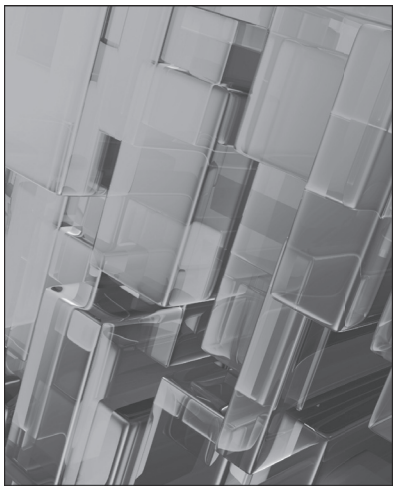
"If you are so incensed that you feel obligated to tell the customer what you're doing, then wait about a year and a half. By that time, the Army will have made a considerable investment in both us and the project, and they'll be locked into us for follow-on work. Because of the strategic timing and additional costs, they will never want to qualify a second supplier so late in the game. Just keep the risk management plan to yourself for now.

"If it looks like the Army might cancel the program, then we'll show them the risk management plan, and perhaps that will keep the program alive."

QUESTIONS

1. Why was a risk management plan considered unnecessary?
2. Should risk management planning be performed in the proposal stage or after contract award, assuming that it must be done?
3. Does the customer have the right to expect the contractor to perform risk analysis and develop a risk management plan if it is not called out as part of the contractual statement of work?

4. Would Altex have been more interested in developing a risk management plan if the project were funded entirely from within?
5. How effective will the risk management plan be if developed by the project manager without input from others?
6. Should the customer be allowed to participate in or assist the contractor in developing a risk management plan?
7. How might the Army have responded if it were presented with a risk management plan early during the R&D activities?
8. How effective is a risk management plan if cost overruns and schedule slippages are always allowed?
9. How can severe optimism or severe pessimism influence the development of a risk management plan?
10. How does one develop a risk management plan predicated upon needed advances in the state of the art?
11. Can the sudden disclosure of a risk management plan be used as a stopgap measure to prevent termination of a potentially failing project?
12. Can risk management planning be justified on almost all programs and projects?



Acme Corporation

BACKGROUND

Acme Corporation embarked on an optimistic project to develop a new product for the marketplace. Acme's scientific community made a technical breakthrough, and now the project appears to be in the development stage, more than being pure or applied research.

The product is considered to be high tech. If the product can be launched within the next four months, Acme expects to dominate the market for at least a year or so until the competition catches up. Marketing has stated that the product must sell for not more than $150 to $160 per unit to be the cost-focused market leader.

Acme uses a project management methodology for all multifunctional projects. The methodology has six life-cycle phases:

1. Preliminary planning
2. Detailed planning
3. Execution/design selection
4. Prototyping
5. Testing/buyoff
6. Production

At the end of each life-cycle phase, a gate/phase review meeting is held with the project sponsor and other appropriate stakeholders. Gate review meetings are

formal meetings. The company has demonstrated success following this methodology for managing projects.

At the end of the second life-cycle stage of this project, detailed planning, a meeting is held with just the project manager and the project sponsor. The purpose of the meeting is to review the detailed plan and identify any future problem areas that will require involvement by the project sponsor.

THE MEETING

Sponsor: "I simply do not understand this document you sent me titled 'Risk Management Plan.' All I see is a work breakdown structure with work packages at level 5 of the WBS accompanied by almost 100 risk events. Why am I looking at more than 100 risk events? Furthermore, they're not categorized in any manner. Doesn't our project management methodology provide any guidance on how to do this?"

PM: "All of these risk events can and will impact the design of the final product. We must be sure we select the right design at the lowest risk. Unfortunately, our project management methodology does not include any provisions or guidance on how to develop a risk management plan. Perhaps it should."

Sponsor: "I see no reason for an in-depth analysis of 100 or so risk events. That's too many. Where are the probabilities and expected outcomes or damages?"

PM: "My team will not be assigning probabilities or damages until we get closer to prototype development. Some of these risk events may go away altogether."

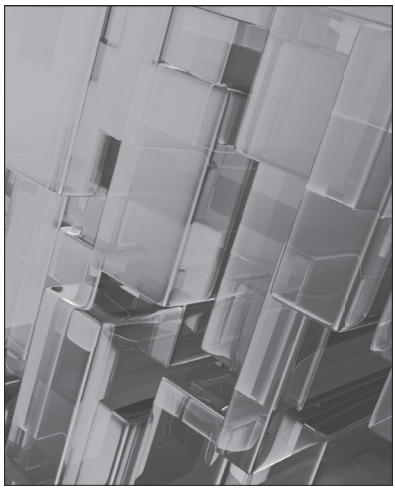
Sponsor: "Why spend all of this time and money on risk identification if the risks can go away next month? You've spent too much money doing this. If you spend the same amount of money on all of the risk management steps, then we'll be way over budget."

PM: "We haven't looked at the other risk management steps yet, but I believe all of the remaining steps will require less than 10 percent of the budget we used for risk identification. We'll stay on budget."

QUESTIONS

1. Was the document given to the sponsor a risk management plan?
2. Did the project manager actually perform effective risk management?
3. Was the appropriate amount of time and money spent identifying the risk events?
4. Should one step be allowed to "dominate" the entire risk management process?
5. Are there any significant benefits to the amount of work already done for risk identification?
6. Should the 100 or so risk events identified have been categorized? If so, how?
7. Can probabilities of occurrence and expected outcomes (i.e., damage) be accurately assigned to 100 risk events?

8. Should a project management methodology provide guidance for the development of a risk management plan?
9. Given the life-cycle phases in the case study, in which phase would it be appropriate to identify the risk management plan?
10. What are your feelings on the project manager's comments that he must wait until the prototyping phase to assign probabilities and outcomes?



The Risk Management Department

BACKGROUND

In 1946, shortly after the end of World War II, Cooper Manufacturing Company was created. The company manufactured small appliances for the home. By 2010, Cooper Manufacturing had more than 30 manufacturing plants, all located in the United States. The business now included both small and large household appliances. Almost all of its growth came from acquisitions that were paid for out of cash flow and borrowing from the financial markets.

Cooper's strategic plan called for global expansion beginning in 2003. With this in mind and with large financial reserves, Cooper planned on acquiring five to six companies a year. This would be in addition to whatever domestic acquisitions were also available. Almost all of the acquisitions were manufacturing companies that produced products related to the household marketplace. However, some of the acquisitions included air conditioning and furnace companies as well as home security systems.

RISK MANAGEMENT DEPARTMENT

During the 1980s, when Cooper Manufacturing began its rapid acquisition approach, it established a Risk Management Department. The Risk Management Department reported to the chief financial officer (CFO) and was considered to be part of the financial discipline of the company. The overall objective of the

Risk Management Department was to coordinate the protection of the company's assets. The primary means by which this was done was through the implementation of loss prevention programs. The department worked very closely with other internal departments such as Environmental Health and Safety. Outside consultants were brought in as necessary to support these activities.

One method employed by the company to ensure the entire company's cooperation and involvement in the risk management process was to hold each manufacturing division responsible for any specific losses up to a designated self-insured retention level. If there was a significant loss, the division must absorb the loss and its impact on the division's bottom-line profit margin. This directly involved the division in both loss prevention and claims management. When a claim did occur, the Risk Management Department maintained regular contact with the division's personnel to establish protocol on the claim and cash reserves and ultimate disposition.

As part of risk management, the company purchased insurance above the designated retention levels. The insurance premiums were allocated to each division. The premiums were calculated based on sales volume and claims loss history, with the most significant percentage being allocated against claims loss history.

Risk management was considered an integral part of the due diligence process for acquisitions and divestitures. It began at the onset of the process rather than at the end and resulted in a written report and presentation to the senior levels of management.

A NEW RISK MATERIALIZES

The original intent of the Risk Management Department was to protect the company's assets, especially from claims and lawsuits. The department focused heavily on financial and business risks with often little regard for human assets. All of this was about to change.

The majority of Cooper's manufacturing processes were labor-intensive assembly line processes. Although Cooper modernized the plants with new equipment to support the assembly lines with hope of speeding up the work, the processes were still heavily labor intensive. The modernization of the plants did improve production. However, more people were getting injured and were out sick. Cooper's workers' compensation costs and health care premiums were skyrocketing and taking an unexpected toll on the bottom line of the financial statements of many of the divisions.

Senior management recognized the gravity of the situation and asked the Risk Management Department to find ways to reduce injuries, lower the number of sick days that people were taking, and reduce workers' compensation costs. To do this, the Risk Management Department had to look at the way each worker performed his or her task and improve where possible the interaction between

the workers and the equipment. The name of the department was then changed to Risk Management and Ergonomics.

ERGONOMICS

According to Wikipedia:

> Ergonomics is the science of designing the workplace environment to fit the user. Proper ergonomic design is necessary to prevent *repetitive strain injuries*, which can develop over time and can lead to long-term disability.
> The International Ergonomics Association defines ergonomics as follows:
>
> > Ergonomics (or human factors) is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance.
> >
> > Ergonomics is employed to fulfill the two goals of health and productivity. It is relevant in the design of such things as safe furniture and easy-to- use interfaces to machines.
> >
> > Ergonomics is concerned with the "fit" between people and their technological tools and environments. It takes account of the user's capabilities and limitations in seeking to ensure that tasks, equipment, information and the environment suit each user.
> >
> > To assess the fit between a person and the used technology, ergonomists consider the job (activity) being done and the demands on the user; the equipment used (its size, shape, and how appropriate it is for the task), and the information used (how it is presented, accessed, and changed). Ergonomics draws on many disciplines in its study of humans and their environments, including *anthropometry, biomechanics, mechanical engineering, industrial engineering, industrial design, kinesiology, physiology and psychology.*[1]

Ergonomics includes the fundamentals for the flexible workplace variability and compatibility with desk components that flex from individual work activities to team settings. Workstations provide supportive ergonomics for task-intensive environments.

Outside the discipline, the term "ergonomics" is generally used to refer to physical ergonomics as it relates to the workplace (as in, e.g., ergonomic chairs and *keyboards*). Ergonomics in the workplace has to do largely with the safety of employees, both long and short term. Ergonomics can help reduce costs by improving safety. This would decrease the money paid out in workers' compensation. For example, over 5 million workers sustain overextension injuries per year.

---

[1] Wikipedia contributors, "Human factors and ergonomics," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=Human_factors_and_ergonomics&oldid=754937541.

FIGURE V Ergonomics in the Workplace

Through ergonomics, workplaces can be designed so that workers do not have to overextend themselves and the manufacturing industry could save billions in workers' compensation (see Figure V).

Workplaces may either take the reactive or proactive approach when applying ergonomics practices. Reactive ergonomics is when something needs to be fixed and corrective action is taken. Proactive ergonomics is the process of seeking areas that could be improved and fixing the issues before they become a large problem. Problems may be fixed through equipment design, task design, or environmental design. Equipment design changes the actual, physical devices used by people. Task design changes what people do with the equipment. Environmental design changes the environment in which people work but not the physical equipment they use.

QUESTIONS

1. Was the original intent of creating the Risk Management Department correct in that it was designed to protect corporate assets? In other words, was this really risk management?
2. Are the new responsibilities of the department, specifically ergonomics, a valid interpretation of risk management?
3. Can the lowering of health care costs and workers' compensation costs be considered as a project?
4. How successful do you think Cooper was in lowering costs?