# NASA's Understanding of Risk in Apollo and Shuttle

Harry W. Jones[1]
*NASA Ames Research Center, Moffett Field, CA, 94035-0001*

**Mathematical risk analysis was used in Apollo, but it gave unacceptably pessimistic results and was discontinued. Shuttle was designed without using risk analysis, under the assumption that good engineering would make it very safe. This approach led to an unnecessarily risky design, which directly led to the Shuttle tragedies. Although the Challenger disaster was directly due to a mistaken launch decision, it might have been avoided by a safer design. The ultimate cause of the Shuttle tragedies was the Apollo era decision to abandon risk analysis.**

## Nomenclature

*CAIB* = Columbia Accident Investigation Board
*GAO* = Government Accountability Office
*PRA* = Probabilistic Risk Assessment

## I. Introduction

THIS paper discusses the changing views of risk over time in NASA's Apollo and Space Shuttle programs. Risk was an acknowledged problem early in Apollo, but risk estimates were disturbingly high and risk analysis was discontinued. Risk analysis was avoided or distorted in Shuttle, leading to an unnecessarily risky design.

The story of the Challenger tragedy is well known but not well understood. The O-rings in the Shuttle solid rocket boosters had experienced erosion on previous flights and the weather was much colder than for earlier launches. The engineers were unable to prove to management that the launch was unsafe. They were overruled and the disaster followed. The accident investigation focused on the events immediately preceding the tragedy, finding a pressure to launch, communication problems between management and engineering, and the "normalization of deviance" shown by the neglect of the increasing erosion of the O-rings. The immediate cause of the Challenger tragedy was the badly mistaken decision to launch, but a more fundamental cause was the poor safety and reliability of the Shuttle design itself. Before Challenger, management thought that the chance of an accident was 1 in 100,000. Afterwards, Probabilistic Risk Analysis (PRA) found a roughly 1 in 100 chance of a Shuttle failure. The number of planned Shuttle flights was greatly reduced. Attempts were made to strengthen the NASA safety culture, but the Columbia tragedy, due to recurring but neglected ice damage to the heat shields, was again attributed to poor safety culture and the normalization of deviance. The second tragedy again confirmed the Shuttle's roughly 1 in 100 risk and the Shuttle program was ultimately terminated. Later launch designs reverted to the safer Apollo configuration, with a hardened capsule, launch abort escape, and the crew placed above the rocket tanks and engine. The ultimate cause of the Challenger tragedy was neglect of risk in Shuttle design.

## II. The Apollo program

The Apollo program grew out of the cold war between the US and the Soviet Union. In 1957 the Soviet Union launched the first man-made satellite, then placed the first animal, first man, and first woman in orbit, and also conducted the first space walk. The Soviet launch of Sputnik was a significant cold war event, since it demonstrated that the Soviets had intercontinental ballistic missiles. Kennedy was elected president after promising to close the "missile gap." He had to deal with confrontations over Berlin and Cuba and Khrushchev's promise that "we will bury you." Apollo was motivated by the need to surpass Soviet space successes that implied US weakness. In 1961 before a joint session of Congress, Kennedy stated that, "I believe that this nation should commit itself to achieving the goal, before this decade is out, of landing a man on the Moon and returning him safely to Earth."[1] Kennedy mentioned safety, but it was third after the decade time limit and the moon destination. The goal was set and achieved and the

[1] Systems Engineer, Bioengineering Branch, Mail Stop N239-8.

Soviets were decisively beaten in the space race. The first moon landing will be remembered as a space milestone long after the cold war is a footnote to history.

The Apollo program was a success, but not a perfect success. Apollo 1 was a tragedy with an amazingly negligent cause, that the possibility of a fire was simply dismissed. Apollo 13 was a close call that demonstrated the high risk inherent in complex systems. Apollo 13 returned without landing and the last three Apollo flights were cancelled to support Skylab and to divert the NASA budget to new programs. The Apollo program achieved only six of the ten planned moon landings.

### A. Appreciating and deemphasizing risk in Apollo

Joseph Shea, the Apollo program manager, chaired the initial Apollo systems architecting team. The "calculation was made by its architecting team, assuming all elements from propulsion to rendezvous and life support were done as well or better than ever before, that 30 astronauts would be lost before 3 were returned safely to the Earth. Even to do that well, launch vehicle failure rates would have to be half those ever achieved and with untried propulsion systems."[2]

The high risk of the moon landing was understood by the astronauts. Apollo 11's Command Module pilot Mike Collins described it as a "fragile daisy chain of events."[3] Collins and Neil Armstrong, the first man to step on the moon, rated their chances of survival at 50-50.[4]

The awareness of risk let to intense focus on reducing risk. "The only possible explanation for the astonishing success – no losses in space and on time – was that every participant at every level in every area far exceeded the norm of human capabilities. "[2]

However, this appreciation of the risk was not considered appropriate for the public. During Apollo, NASA conducted a full Probabilistic Risk Assessment (PRA) to assess the likelihood of success in "landing a man on the Moon and returning him safely to Earth." The PRA indicated the chance of success was "less than 5 percent." The NASA Administrator felt that if the results were made public, "the numbers could do irreparable harm." The PRA effort was cancelled and NASA stayed away from numerical risk assessment as a result.[5]

### B. Apollo 1

During a simulated countdown, liftoff, and flight conducted in the Apollo 1 capsule on the launch pad, the astronauts reported a fire. The three astronauts died from smoke and flames before escape or rescue was possible. National news commentators and senators blamed the inflexible, meaningless goal of putting a man on the moon before 1970.

Joseph Shea recalled a fire discussion a few months before, "I got a little annoyed, and I said, 'Look, there's no way there's going to be a fire in that spacecraft unless there's a spark or the astronauts bring cigarettes aboard.'"[6] "Deeply involved in the investigation of the 1967 Apollo 1 fire, Shea suffered a nervous breakdown as a result of the stress that he suffered. He was removed from his position and left NASA shortly afterwards."[7]

The NASA administrator established an all government, nearly all NASA review board that limited outside access to information. The review board found that:

> "The fire in Apollo 204 was most probably brought about by some minor malfunction or failure of equipment or wire insulation. This failure, which most likely will never be positively identified, initiated a sequence of events that culminated in the conflagration. Those organizations responsible for the planning, conduct and safety of this test failed to identify it as being hazardous. … The Command Module contained many types and classes of combustible material in areas contiguous to possible ignition sources. … The Command Module Environmental Control System design provides a pure oxygen atmosphere. ... This atmosphere presents severe fire hazards."[8]

The review board recommended that NASA continue the program to the reach the moon by 1969, but make safety more important than schedule. Congress investigated and noted that there was no investigation of possible weakness in the managerial structure causing the failure. However, they confirmed the review board's recommendation to proceed to the moon with safety first.

The cause of the Apollo 1 failure was a failure to anticipate a known hazard. Astronaut Frank Borman, on the NASA review board, stated "none of us gave any serious consideration to a fire in the spacecraft."[8] The Apollo 1 fire was unexpected, unpredicted even though several fires in other pure oxygen atmospheres had caused deaths. Later spacecraft designs used Earth normal atmosphere, considered the combustibility of materials, and developed capabilities and procedures for escape and rescue.

After the tragedy of the Apollo 1 fire, the reliability of Apollo was made central by an engineering culture that encouraged an environment of open communications, attention to detail, and ability to challenge technical assumptions. "Anyone could challenge a design at any time. … Reliability was a concern at all levels."[9]

### C. Apollo 11

Apollo 11 successfully landed on the moon on the first attempt in 1969. The US achieved a fabulous goal and the Soviets were decisively beaten in the cold war space race.

A major factor in the success of Apollo was the extreme attention paid to reliability and crew safety with emphasis on communications, teamwork, and paying attention to details. The policy was to speak and to listen, to always bring up issues that were not fully understood. Apollo had an unusual and pervasive awareness of risk. The Apollo success showed that by intense effort, a dedicated organization can achieve results far beyond reasonable expectation.

### D. Apollo 13

Apollo 13 was on its way to the moon when crew heard a loud bang and reported, "Okay, Houston. Hey, we've got a problem here." Panel readings indicated a loss of fuel cell oxygen and the attitude control thrusters were firing to counteract oxygen venting into space. As both oxygen tanks became empty, the crew sought refuge in the lunar module.[8]

The investigation identified the physical causes and the sequence of events of the failure. Oxygen tank 2 had two protective thermostat switches on its heater that were designed for 28 volts dc, but a procedure change allowed them to be operated at 65 volts dc during tank pressurization. When the tank temperature rose above limits during pressurization a few days before launch, the thermostat switches were fused closed and failed to open to turn off the tank heater. The intense heat in the tank damaged Teflon insulation on the fan motor wire. The later in-flight accident occurred when starting the fans in oxygen tank 2 caused an electrical short circuit through the damaged insulation on the fan motor wires and the insulation caught fire. The fire in oxygen tank 2 caused it to suddenly rupture and damage tank 1, causing it to also leak.

The review board found that:

> "The total Apollo system of ground complexes, launch vehicle, and spacecraft constitutes the most ambitious and demanding engineering development ever undertaken by man. For these missions to succeed, both men and equipment must perform to near perfection. … the accident was not the result of a chance malfunction in a statistical sense, but rather from an unusual combination of mistakes, coupled with a somewhat deficient and unforgiving design."[8]

A test procedure mistake was made and not caught by review. The Apollo 13 failure was an illustration of the high technology failures that occur in complex systems.

### E. Apollo risk summary

At the beginning of Apollo, its great difficulty and risk were obvious. Numerical estimates of the probability of success were given as either 3 in 30 or 5%. This awareness of risk led to great conservatism in defining the mission scenario and overall systems architecture. However, openly reporting the expected high risk was not politically feasible. The head of Apollo reliability and safety decided, "Statistics don't count for anything," and that risk is reduced by "attention taken in design." This design-oriented view that neglected use of probability numbers was carried forward from Apollo to Shuttle. A NASA safety analysis for Galileo explained that Shuttle "relies on engineering judgment using rigid and well-documented design, configuration, safety, reliability, and quality assurance controls." It was also thought that, with the attention given to safety and reliability, "standard failure rate data are pessimistic."[5]

The great and initially unexpected success of Apollo appeared to validate the final Apollo approach to risk, which was to to avoid computing and reporting the probability of failure and to assume that good design would reduce risk far below previous experience. Neglecting the historical base rate is a well known fundamental flaw in prediction.[10] The Shuttle experience described later illustrates the predictive value of historical base rates.

The success of Apollo was due to three things, the initial probabilistic awareness of high risk that led to conservative mission and architecture planning, diligent attention to design, and careful mission operations. Success requires attention to risk in planning, design, and operations, since neglecting risk in any phase can lead to failure. Following the later Apollo approach of deemphasizing risk led Shuttle into risky mission and architecture planning and to negligent operations, with tragic results.

## III. The Shuttle program

The Space Shuttle was NASA's next major human program after Apollo. The Shuttle transported cargo and crew to orbit from 1981 to 2011. There were 133 successful missions and two tragic failures. The Shuttle program mistakenly promised rapid turn around, frequent flights, and lower launch costs. But the worst mistake in Shuttle was believing that the Shuttle was safe.

Shuttle was developed in a very different atmosphere than Apollo. The Apollo program had strong congressional support and an extremely large budget. "This meant that Administrator Webb did not have to 'sell' the program to his

political overseers with exaggerated claims or by acquiescing to unrealistic budget compromises. And so, the freedom of the agency to provide realistic cost estimates and enjoy relatively smooth relations with White House and Congress gave 'NASA engineers a fighting chance to accomplish their mission without any cost overruns.'"[11] [12]

Developing the Shuttle in the 1970's, NASA had to adjust to a new reality. It had been "above the wearisome battle for resources that typified other public enterprises." Now it pushed the economy and jobs.[12] NASA overpromised on what the Space Shuttle could accomplish on half the initial budget. It would pay for itself launching satellites and carrying out science experiments. The number of possible launches and the potential cost savings were greatly exaggerated.

**A. Denying risk in Shuttle**

Shuttle was politically unpopular and the program's very existence was threatened. The initial design of the Shuttle emphasized capability and cost without mention of risk. "During the early Shuttle studies, there was a debate over the optimal Shuttle design that best balanced capability, development cost, and operational cost."[13] There was a need for over-optimistic advocacy. A retired NASA official stated, "some NASA people began to confuse desire with reality. … One result was to assess risk in terms of what was thought acceptable without regard for verifying the assessment. … Note that under such circumstances real risk management is shut out."[5]

The risk of Space Shuttle was generally neglected. "Although every knowledgeable observer recognized that there was some potential for a major Shuttle failure, the press and the broader public in the early 1980s paid little attention to the risks of human spaceflight. Even those close to the Shuttle system let down their guard. As one successful launch followed another, some engineers and flight directors began to submerge their concerns about troublesome items that lay on the critical path to a safe launch."[14]

Following the final Apollo neglect of risk, top level mission and system wide PRA was avoided. The Space Shuttle risk assessments were all qualitative at the system level. They included preliminary hazards analysis, failure modes and effects analysis with critical items list, and various safety assessments. There was some quantitative analysis conducted for specific subsystems.[5] The Space Shuttle requirements for safety were too simplistic. Subsystems were to "fail-operational after the failure of (the) most critical component" and to "fail-safe for crew survival the failure of (the) two most critical components."[15]

Safety was simply assumed rather than designed into the Shuttle.

> "The final shortcoming was that the Shuttle was designed as if it had the inherent operating safety of an airliner. It was not equipped with any provision for crew rescue in case of booster failure during ascent to orbit, or being stranded in orbit, or structural failure during re-entry. The crew was not even provided with spacesuits, despite the lessons of the Soviet space program. This seemed an extraordinary act of engineering hubris, given that contemporary military aircraft were equipped with pressure suits and ejection seats. But the weight problem also meant that there was no margin for crew safety measures without (to NASA) unacceptable impact to the net payload. … Following the Columbia disaster, NASA finally realized it could not make the Shuttle safe. The only way to continue American manned spaceflight would be to develop a replacement manned spacecraft with an escape system, and meanwhile fly the Shuttle as little as possible."[16]

**B. NASA Shuttle PRA's**

Three PRA's were done on Shuttle. PRA was required because Shuttle was to be used to launch Galileo to Jupiter, and Galileo contained plutonium in a thermonuclear generator which could be dispersed by an accident. The first contractor study done for NASA found the risk of losing a Shuttle during launch was between 1 chance in 1,000 and 1 in 10, 000. The greatest risk was in the solid-fuel rocket boosters, which had a failure rate of about 1 in 40. However, rather than use the historical data, the NASA sponsor made an "engineering judgment" and "decided to assume a failure probability of 1 in 1,000" or even 1 in 10,000.[5]

A second study for the Air Force noted that the earlier study involved both gathering failure data "and the disregarding of that data and arbitrary assignment of risk levels apparently per sponsor direction" with "no quantitative justification at all." After reanalyzing the data, the study found that the boosters' track record "suggest[s] a failure rate of around one-in-a-hundred."[5]

NASA Johnson Space Center conducted its own internal safety analysis for Galileo in 1985. The Johnson authors went through failure mode worksheets assigning probability levels. A failure in the solid rocket booster (the failure that destroyed Challenger) was assigned a probability of 1 in 100,000.[5]

Even after the Challenger accident, the NASA chief engineer in a hearing on the Galileo thermonuclear generator said: "We think that using a number like 10 to the minus 3, as suggested, is probably a little pessimistic." He thought the actual risk "would be 10 to the minus 5." The number was derived "based on engineering judgment."[5]

## C. Challenger

The Challenger broke up at 73 seconds into flight when an O-ring in the right solid rocket booster failed and allowed a flare to reach the external fuel tank, which separated so that aerodynamic forces disintegrated the Shuttle. The crew cabin hit the ocean at unsurvivable speed at 2 minutes and 45 seconds after the breakup.

NASA's internal investigation was initially conducted in secrecy and was suspected of covering up relevant information. The presidentially appointed Rogers Commission identified failure causes in NASA's management culture and decision-making processes.

> "testimony reveals failures in communication that resulted in a decision to launch (Challenger) based on incomplete and sometimes misleading information, a conflict between engineering data and management judgments, and a NASA management structure that permitted internal flight safety problems to bypass key Shuttle managers."[17]

The flaw in the O-ring design and the potential for flare blow-by had been known for many years but had been ignored and the risk improperly minimized. This has been labeled "normalization of deviance."[18] Before the flight, engineers had warned about the danger of launching in much colder than previously experienced temperatures.

The Nobel physicist Richard Feynman provided "Personal Observations on Reliability of Shuttle" as an appendix to the Rogers Commission report on the Challenger accident.

> "It appears that there are enormous differences of opinion as to the probability of a failure with loss of vehicle and of human life. The estimates range from roughly 1 in 100 to 1 in 100,000. The higher figures come from the working engineers, and the very low figures from management. …An estimate of the reliability of solid rockets was made by the range safety officer, by studying the experience of all previous rocket flights. Out of a total of nearly 2,900 flights, 121 failed (1 in 25). ... NASA officials argue that the figure is much lower. They point out that these figures are for unmanned rockets but since the Shuttle is a manned vehicle 'the probability of mission success is necessarily very close to 1.0.' … It would appear that, for whatever purpose, be it for internal or external consumption, the management of NASA exaggerates the reliability of its product, to the point of fantasy.[17]

The neglect of O-ring and tile damage, the normalization of deviance, and the fantastic exaggeration of Shuttle reliability are well documented. [17] [18] [19] There is an even more obvious but usually unmentioned reason for the failures of Shuttle. The Space Shuttle simply was not designed to minimize risk. Unlike the hardened Apollo capsule, the Shuttle crew compartment was fragile, unlike the Apollo command module, the Shuttle crew compartment was next to rather than above the dangerous rockets, and unlike Apollo, the Shuttle had no launch abort system. These design errors can be considered the root causes of the Challenger and Columbia accidents. These early fundamental design errors have been deemphasized in favor of blaming operational people who by extraordinary action might have beaten the bad odds. These design errors are implicitly acknowledged by the fact that NASA's post Shuttle rocket and crew vehicle designs replicate the Apollo approach.

In response to the Rogers Commission's recommendations, NASA redesigned the solid rocket boosters and created a new Office of Safety, Reliability and Quality Assurance reporting directly to the administrator.

In her investigation of the Challenger disaster, Diane Vaughan found that, because of difficult goals and limited resources, NASA's Apollo safety culture became a "culture of production" that emphasized productivity, efficiency, obeying orders and following rules rather than problem solving or concern about safety. The result was "the normalization of deviance," the acceptance of what should have been alarming indications of incipient failure. Blocked communications, Vaughan's "structural secrecy," prevented effective action.[18]

Initial qualitative assessments of Shuttle reliability were based on expert judgment rather than reliability analysis. After Challenger, PRA was adopted and applied to the Space Shuttle, space station, and some unmanned space missions. NASA then developed realistic estimates of probability of Space Shuttle failure, roughly 1 in 100.[20]

## D. Columbia

The Columbia astronauts perished when the Shuttle heat shield failed on reentry. The Columbia Accident Investigation Board (CAIB) reported:

> "The physical cause of the loss of Columbia and its crew was a breach in the Thermal Protection System on the leading edge of the left wing, caused by a piece of insulating foam which separated from the left bipod ramp … and struck the wing ... During re-entry this breach in the Thermal Protection System allowed superheated air to penetrate through the leading edge insulation and progressively melt the aluminum structure of the left wing, resulting in … break-up of the Orbiter. This breakup occurred in a flight regime in which, given the current design of the Orbiter, there was no possibility for the crew to survive. … The organizational causes of this accident are rooted in the Space Shuttle Program's history and culture, including the original compromises that were required to gain approval for the Shuttle, subsequent years of resource constraints, fluctuating priorities, schedule pressures, mischaracterization of the Shuttle as operational rather than developmental, and lack of an agreed national vision for human space flight. Cultural traits and organizational practices detrimental to safety were allowed to develop, including: reliance on past success as a substitute for sound engineering practices (such as testing to understand why systems were not performing in accordance with requirements); organizational barriers that prevented effective communication of critical safety information and stifled

professional differences of opinion; lack of integrated management across program elements; and the evolution of an informal chain of command and decision-making processes that operated outside the organization's rules.[19]

The physical cause of the Columbia tragedy was identified and it was noted that the Shuttle design provided no crew escape and no possibility for the crew to survive. The CAIB's emphasis was on the organizational practices detrimental to safety, the barriers that prevent communication of critical safety information, the lack of integrated management, and the informal chain of command that were immediate contributors to the failure. The goal of the prescribed independent program technical authority, the independent safety assurance organization, and the learning organization culture is to "more safely and reliably operate the inherently risky Space Shuttle."

The CAIB found that the post-Challenger changes in NASA management and culture were ineffective.

> "(T)he Rogers Commission … recommendations centered on an underlying theme: the lack of independent safety oversight at NASA. … NASA's response to the Rogers Commission recommendation did not meet the Commission's intent: the Associate Administrator did not have direct authority, and safety, reliability, and mission assurance activities across the agency remained dependent on other programs and Centers for funding."[19]

The CAIB believed that Columbia and Challenger were both lost because of similar failures in NASA's organizational system. "(T)he causes of the institutional failure responsible for Challenger have not been fixed."[19] NASA during Apollo had a good safety culture but lost it before Shuttle. NASA had lost the ability to recognize and repair threats that were obvious in hindsight.[21]

Interestingly, the CAIB evaluated NASA's performance using the two well known theories of reliability and failure. The CAIB observed that "Though neither High Reliability Theory nor Normal Accident Theory is entirely appropriate for understanding this accident, insights from each figured prominently in the Board's deliberation."[19] The CAIB found that organizational changes could "minimize risk and limit the number of accidents."[19] It noted that one individual, the Shuttle program manager, was responsible for achieving safe, timely launches at acceptable costs and so a compromise of safety was expected no matter who was in the position. The CAIB recommended that "responsibility and authority for decisions involving technical requirements and safety should rest with an independent technical authority."[19] The GAO recently found that NASA's commercial crew program has still not implemented the separation of programmatic and safety authority that was recommended in the CAIB report. "(T)he program's chief safety and mission assurance officer is dual hatted to serve simultaneously in a programmatic position as well as the program's safety technical authority. This approach creates an environment of competing interests.[22]

The CAIB concluded, "The Shuttle is now an aging system but still developmental in character. It is in the nation's interest to replace the Shuttle as soon as possible."[19]

### E. Shuttle risk summary

The Challenger tragedy is frequently taught as a conspicuous case of management failure. The focus is on the Challenger launch decision. The immediate cause is usually described as a last minute failure of communication, leading to the inability of engineers to have their O-ring concerns heard and acted on. The longer term organizational cause is the gradual "normalization of deviance," when safety issues gradually became neglected due to a production culture and short launch schedules. The cure would be a management led culture change, emphasizing safety in Shuttle operations.[18] [19] The real problem has been mistaken. The true fundamental cause of the Challenger and Columbia disasters occurred decades earlier.

The design of the Shuttle design produced a system that was excessively and unnecessarily dangerous. The Space Shuttle simply was not designed for minimum risk. Unlike the hardened Apollo capsule head shield, the Shuttle crew compartment used fragile tiles, unlike the Apollo crew module, the Shuttle crew compartment was next to rather than above the dangerous rockets, and unlike Apollo, the Shuttle had no launch abort system. These design errors directly led to the Challenger and Columbia accidents. These early fundamental design errors are deemphasized in favor of blaming operational people who with luck and diligence might have beaten the high probability of a failure. These design errors are implicitly acknowledged by the fact that the current rocket and crew vehicle designs are similar to the safer design configuration of Apollo, with a hardened crew capsule, the crew capsule above the rocket and fuel, and a launch abort system.

One reason that the Space Shuttle was not designed for minimum risk is that probabilistic risk analysis was not used in its initial design. The probability of failure was not computed for the alternate designs and not compared to traditional expendable rockets. Although risk analysis had helped improve Apollo safety, it was abandoned as too negative during later Apollo development and was thought too pessimistic after the success of Apollo. A high probability of failure was built into the Shuttle design, but this was not generally realized until after Challenger.

The sequence of events leading to the Shuttle tragedies and responses began decades earlier during the Apollo era. Risk analysis was abandoned during Apollo in favor of engineering design for reliability. The Shuttle was designed without explicit mathematical consideration of risk. Choices were made to improve performance and reduce cost that

inadvertently increased risk. When the statistically predictable failures occurred, the failure investigations focused on the lowest organizational level and the last moments when the tragedies could have been avoided by some extraordinary saving action. Although some design changes were made, the Shuttle design was largely fixed, and the main recommendations were to improve NASA organization, culture, and operations. And yet the ultimate cause of the Shuttle tragedies was the choice by the Apollo-era NASA administrator to avoid the negative impact of risk analysis. This was deemed necessary to avoid damaging the Apollo program. Other aspects of Shuttle advocacy, such as projecting an impossibly high number of flights to justify projected launch cost savings, also show distortions justified by political necessity. Ultimately, it was generally accepted that the Shuttle was too risky to continue to fly and the program was cancelled.

## IV. Conclusion

The risk to safety should always be a major concern in human space flight. NASA's attitude toward risk was very different at different times in Apollo and Space Shuttle. The Apollo program expected that many lives would inevitably be lost. Because of this, Apollo planned its mission and built its systems to minimize risk. Nevertheless, the danger of a pure oxygen atmosphere and the possibility of a fire were casually ignored and the tragic Apollo 1 fire occurred. Responsive efforts created a safety culture. The Apollo 13 near tragedy occurred because an incorrectly planned test damaged an oxygen tank, but Apollo 1 was the only fatal accident.

The amazingly favorable safety record of Apollo led to overconfidence, ignoring risk, and inevitable disasters in Shuttle. The earlier emphasis on safety risk analysis was forgotten by the Shuttle program. High risk choices were made that directly lead to the later Shuttle fatalities. The crew cabin used fragile tiles rather than a strong heat shield. The crew cabin was placed next to rather than above the rocket engines. The launch abort system was eliminated. NASA management believed and testified to Congress that the Shuttle was very safe, with a 1 in 100,000 chance of an accident.

The devastating loss of Challenger let to drastic reassessments. Risk analysis was restored. The actual chance of an accident was 1 in 100, not the originally claimed 1 in 100,000. The Challenger investigation faulted the Challenger launch decision, which due to the urgency to launch, ignored concerns about the rocket booster O-ring failure that caused the accident. Future Shuttle missions were mostly restricted to building the space station. The much later Columbia accident was thought to echo Challenger, since once again the failure signs and warnings were ignored.

The Shuttle was cancelled after the space station was completed because of its high risk. NASA's latest Apollo-like designs directly reverse the risky choices of Shuttle. The crew capsule with heat shield is placed above the rockets and a launch abort system will be provided.

This brief overview suggests two observations. First, the most important thing is the organization's attention to risk. To achieve high reliability and safety, risk must always be a prime concern. Second, the risk to safety must be considered and minimized as far as possible at every step of a program, through mission planning, systems design, testing, and operations. At any time and place, some safety risk can be introduced or an existing one ignored. Everyone in a program should be constantly alert for potential risks, even outside their own responsibility. In a safety culture, any anomaly, even a temporary sensor glitch, is traced to its cause, understood, and corrected, no matter what.

Intuitively people often think that a mission is like a chain of many links. Any link can fail. The weakest links are top priority and improving others is wasted effort. This works well enough, but risk analysis provides a better insight. If there are many causes of failure, the overall probability of failure is the sum of all the failure rates, not the highest individual failure rate. Risk is a resource to be capped and optimized. The risk budget sets how much to spend. Optimization accepts risk in the most cost-effective way. If the biggest risk is too difficult and expensive to reduce, a smaller risk might be reduced more cheaply, and the overall risk reduced at less cost.

Different program phases require different risk reduction reduction methods. Defining the mission scenario and system architecture can benefit from Probabilistic Risk Analysis. System design can use engineering judgment and safety design techniques. During operations, failure reporting and anomaly investigation are important.

A short sighted accident investigation would tend to blame the people closest to the accident. It is true that whatever the design problems, a lucky and skillful operator might save the day. The Shuttle investigations found a bad safety culture affected launch decisions. The Shuttle itself was a given, so its intrinsic high risk was ignored as the fundamental cause of the accidents. The true cause of the Shuttle tragedies was a negligent high risk design.

## References


[1] Cortright, E. M., ed., *Apollo Expeditions to the Moon*, ch. 2.1, Gilruth, R. R., "I Believe We Should Go to the Moon," https://history.nasa.gov/SP-350/ch-2-1.html, accessed Aug. 1, 2018.

[2] Rechtin, E., Systems Architecting of Organizations, CRC Press, Boca Raton, 2000.

[3] Howell, E., "Apollo 11 Moon Landing Carried Big Risks for Astronauts, NASA," space.com, July 19, 2014, https://www.space.com/26576-apollo-11-moon-landing-risks.html, accessed Feb. 2, 2018

[4]McKie, R., "How Michael Collins became the forgotten astronaut of Apollo 11," July 18, 2009, https://www.theguardian.com/science/2009/jul/19/michael-collins-astronaut-apollo11, accessed Feb. 7, 2018.

[5] Bell, T. E., and Esch, K., "The Challenger Disaster: A Case of Subjective Engineering," Jan. 28, 2016 (June 1989), https://spectrum.ieee.org/tech-history/heroic-failures/the-space-Shuttle-a-case-of-subjective-engineering, accessed July 24, 2018.

[6] Shea, J. F., Edited Oral History Transcript, NASA Johnson Space Center Oral History Project, 1998, https://www.jsc.nasa.gov/history/oralhistories/SheaJF/SheaJF11-23-98.htm, accessed Feb. 2, 2018.

[7] nasa.wikia, Joseph Francis Shea, NASA Johnson Space Center Oral History Project Biographical Data Sheet, 2006, http://nasa.wikia.com/wiki/JosephFrancisShea, accessed Feb. 6, 2018.

[8] Benson, C. D., and Faherty, W. B., "Moonport: A History of Apollo Launch Facilities and Operations," NASA Special Publication-4204 in the NASA History Series, 1978. http://www.hq.nasa.gov/office/pao/History/SP-4204/contents.html

[9] Oberhettinger, D., NASA Public Lessons Learned Entry: 1806, Capture of Apollo Lunar Module Reliability Lessons Learned: Program/Engineering Management, 9/25/2007.

[10] Kahneman, D., *Thinking, Fast and Slow*, Farrar, Straus, and Giroux, New York, 2011.

[11] McCurdy, H. E., *Faster, Better, Cheaper: Low-Cost Innovation in the U.S. Space Program*, The Johns Hopkins University Press, 2001.

[12] Mahler, J. G., *Organizational Learning at NASA: The Challenger and Columbia Acci*dents, Georgetown University Press, Washington, DC, 2009.

[13] Wikipedia, Space Shuttle design process, https://en.wikipedia.org/wiki/Space_Shuttle_design_process, accessed July 25, 2018.

[14] Williamson, R. A., "Developing the Space Shuttle: Early Concepts of a Reusable Launch Vehicle," in Logsdon, J. M., editor, *Exploring the Unknown: Selected Documents in the History of the U.S. Civil Space Program*, NASA SP-4407, 1995.

[15] Camarda, C, Space Shuttle Design and Lessons Learned Presentation, March 2014, https://www.researchgate.net/publication/296652080SpaceShuttleDesignandLessonsLearned, accessed July 18, 2018.

[16] Encyclopedia Astronautica, Space Shuttle, www.astronautix.com/s/spaceShuttle.html, accessed July 19, 2018.

[17] Rogers Commission, *Report of the Presidential Commission on the Space Shuttle Challenger Accident*, 1986. http://history.nasa.gov/rogersrep/genindex.htm

[18] Vaughan,, D., *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*, University of Chicago, 1997.

[19] CAIB, *Columbia Accident Investigation Board*, Vol. I, August 2003.

[20] Paté-Cornell, E., and Dillon, R., "Probabilistic risk analysis for the NASA Space Shuttle: a brief history and current work," Reliability Engineering & System Safety, V. 74, 3, December 2001.

[21] Boin, A., and Schulman, P., "Assessing NASA's Safety Culture: The Limits and Possibilities of High-Reliability Theory," Public Administration Review November-December, 2008.

[22] Government Accountability Office (GAO), NASA COMMERCIAL CREW PROGRAM, GAO-18-476, July 2018.