

THE CHALLENGER TRAGEDY WAS CAUSED BY AN APOLLO MISTAKE, TERMINATING RISK ANALYSIS

Harry W. Jones⁽¹⁾

⁽¹⁾NASA Ames Research Center, Moffett Field, CA, 94035, harry.jones@nasa.gov:

ABSTRACT

NASA's attitude toward risk changed drastically between the Apollo and Space Shuttle design. [1] Apollo engineers were seriously alarmed about risk because of the fatal Apollo 1 fire and the fact that the estimated probability of another fatal accident was extremely high. The predictions were so appalling that management terminated risk analysis to avoid public apprehension. Because risk analysis was not done, the Space Shuttle design accepted excessively high and unknown risk. The immediate cause of the Challenger tragedy was the mistaken decision to launch in cold weather that impaired the O-ring seals, but the fundamental cause was the high risk of the shuttle design. Before Challenger, management asserted that the probability of a fatal accident was 1 in 100,000. Probabilistic Risk Analysis (PRA) found a roughly 1 in 100 chance of a shuttle failure.

1. APOLLO

During Apollo it was estimated that, "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." [2] After the Apollo 1 tragedy, the awareness of risk led to an intense effort to achieve safety. "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] A NASA Probabilistic Risk Analysis (PRA) found that the chance of success was "less than 5 percent." The NASA Administrator felt that "the numbers could do irreparable harm," and discontinued risk assessment. [3] NASA reduced its earlier intense focus on risk. The head of Apollo reliability and safety decided, "Statistics don't count for anything," and that risk is reduced by "attention taken in design." [3] The great and initially doubtful success of Apollo appeared to validate the neglect of PRA. Continuing to avoid risk analysis allowed shuttle decisions to increase the risk built into the design, and this inevitably produced tragic results.

Apollo 1

During a simulated countdown, lift off, 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. The NASA review board found there were many types of combustible materials near possible ignition sources in a pure oxygen atmosphere and that the severe fire hazard had not been identified. [4] Ignoring the fire risk produced the Apollo 1 accident. Later spacecraft designs used Earth normal atmosphere, reduced the combustibility of materials, and developed capabilities for escape and rescue. After Apollo 1, reliability was made a concern at all levels. The Apollo engineering culture encouraged open communications and gave working level engineers the ability to challenge a design at any time.

Apollo 13

On its flight to the moon, Apollo 13's oxygen tank 2 caught fire and exploded, damaging oxygen tank 1. The crew took refuge in the Lunar Excursion Module and made a precarious return to Earth. Due to a test procedure error, the tank thermostat switches had been operated at too high voltage, fusing them closed, allowing later tank operation at too high temperatures that damaged fan wiring insulation, permitting an in-flight electrical short that caused the fire and explosion. The review board found that the accident was due to this unusual sequence of events and the deficient design. [4] High technology systems have complex failure scenarios that are difficult to predict and diagnose.

Apollo risk summary

The extraordinary success of Apollo was due to the strong initial awareness of its high risk that led to conservative mission planning, cautious system and architecture choices, a meticulous attention to detailed design, and painstaking mission operations. Improving safety requires great effort to reduce risk in mission planning, system design, and operations.

Apollo's great difficulty and risk were obvious at the beginning and throughout the program. Unfortunately, the great achievements of Apollo and the suppression of discouraging risk analysis led to over confidence. The hazardousness of Apollo was forgotten. NASA came to believe that failure rate calculations were too pessimistic and risk was reduced by attention taken in design. [3]

The later Apollo abandonment of PRA and over confidence that careful design could eliminate risk was continued in shuttle design. A NASA safety analysis explained that shuttle "relies on engineering judgment

using rigid and well-documented design, configuration, safety, reliability, and quality assurance controls.” [3] Deemphasizing risk led shuttle to make risky design decisions that produced tragic results.

2. SPACE SHUTTLE

The Space Shuttle transported cargo and crew to orbit from 1981 to 2011. There were 133 successful missions and two tragic failures. At first the shuttle program over-optimistically promised rapid turnaround, frequent flights, and lower launch costs. But the worst mistake was believing that the shuttle was very safe.

The Apollo program had strong congressional support and an extremely large budget. There was no need for exaggerated claims or unrealistic budget estimates. [5] shuttle was unpopular and the program’s existence was often threatened. To gain support for the shuttle, NASA had to inflate its promised performance. The shuttle would pay for itself by launching all US satellites, commercial, military, and scientific, and would boost the economy and jobs. [6] The number of launches per year and the cost savings per launch were greatly exaggerated.

The risk of Space Shuttle was generally neglected. NASA began to confuse desire with reality and estimated the risk as what would be thought acceptable without verifying that assessment. [3] Mission level PRA was avoided when possible and distorted when required. The engineering risk assessments were largely qualitative and bottom-up from at the system level. They included preliminary hazards analysis, failure modes and effects analysis with a critical items list, and other safety assessments. There was some quantitative analysis conducted for specific subsystems. [3] Safety was simply assumed rather than designed into the shuttle.

Shuttle Probabilistic Risk Analysis (PRA)

Despite NASA’s reluctance, three PRA’s were done for shuttle. PRA was required because shuttle was to launch Galileo which contained plutonium that could be dispersed in a launch accident. The first study found the greatest risk was in the solid-fuel rocket boosters, which had a launch failure rate of about 1 in 40. Rather than use this historical data, NASA made an “engineering judgment” and “decided to assume a failure probability of 1 in 1,000” or even 1 in 10,000. [3] The Air Force noted that this 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.” They study found that the boosters’ track record “suggest[s] a failure rate of around one-in-a-hundred.” [3] NASA Johnson Space Center conducted its own internal safety analysis. A failure in the solid rocket

booster, the failure that destroyed Challenger, was assigned a probability of 1 in 100,000. [3]

Challenger

The Challenger broke up at 73 seconds after launch 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 flaw in the O-ring design and the potential for a flare blow-by had been known for years but redesign was delayed and the risk incorrectly accepted. Immediately before the flight, engineers had warned of the danger of launching in much colder than previous launch temperatures. After Challenger, future shuttle missions were usually limited to building the space station.

Columbia

The Columbia astronauts perished when the shuttle heat shield failed on reentry. The Columbia Accident Investigation Board (CAIB) found the cause was a breach in the thermal protection tiles on the leading edge of the left wing caused by insulating foam which separated and struck the wing. It was noted that the shuttle design provided no crew escape and no possibility for the crew to survive. [7]

Shuttle risk summary

The Challenger launch decision is a famous example of organizational disfunction and management failure. The final management failure is explained as a last-minute breakdown of communication, shown by the inability of engineers to have their O-ring concerns accepted and the launch delayed. The organizational disfunction is explained by Diane Vaughn’s gradual “normalization of deviance,” when safety issues gradually became neglected due to a production culture and short launch schedules. [8] The suggested cure is management led culture change to establish safety in shuttle operations. The CAIB found that Columbia was lost due to similar organizational problems which had not been cured after Challenger. [7]

Better communications and more attention to the warnings given by partial failures might have prevented the shuttle tragedies, but the true fundamental cause of the Challenger and Columbia disasters was that the shuttle design was excessively dangerous. The Space Shuttle simply was not designed to have a known and tolerable risk. Unlike the hardened Apollo capsule heat 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. Unlike Apollo, the shuttle had no launch abort or crew escape systems. Avoiding these

design errors could have directly prevented the Challenger and Columbia accidents.

The fundamental cause of the shuttle tragedies was the choice by the Apollo-era NASA administrator to escape the very negative outlook produced by conservative risk analysis. Accepting increasing risk was then forced by the political necessity to achieve launch cost savings. Ultimately the shuttle was considered too risky to fly and shuttle was cancelled after the space station was completed, eliminating US crew launch capability for a decade.

3. ACCEPTED SHUTTLE FAILURE ANALYSIS

The Rodgers report established a generally accepted analysis of shuttle failures that the CAIB confirmed.

The Rodgers Commission report

The Rodgers Commission identified failures in communication that led to incomplete and misleading information, conflicts between engineering and management judgment, and an inadequate management structure that allowed safety problems to bypass key managers. [1] [9]

The Nobel physicist Richard Feynman in an appendix to the Rodgers Commission report found enormous differences in the estimated probability that a shuttle would fail with loss of life. The working engineers estimate was about 1 in 100 while the management estimate was 1 in 100,000. He found that, "the management of NASA exaggerates the reliability of its product, to the point of fantasy." [9] In response to the Rodgers Commission report, NASA redesigned the solid rocket boosters and created a new Office of Safety, Reliability and Quality Assurance that reported directly to the administrator. After Challenger, PRA was reinstated 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. [10]

In her investigation of the Challenger disaster, Diane Vaughan found that, because of difficult goals and limited resources, NASA's Apollo safety culture had become a "culture of production" that emphasized productivity, efficiency, obeying orders, and following rules rather than solving problem or worrying about safety. The result was "the normalization of deviance," the routine acceptance of what should have been alarming indications of potentially serious failures. Blocked communications, what Vaughan called "structural secrecy," prevented effective action. [8]

The CAIB report

The Columbia Accident Investigation Board (CAIB) found that the post-Challenger changes in NASA management and culture had been ineffective and the

problems responsible for Challenger had not been fixed. The Rodgers Commission had recommended independent oversight and direct authority over safety in NASA, but safety and reliability still depended on other programs for funding. [7]

The CAIB emphasized the organizational practices detrimental to safety, the barriers that prevented communication of critical safety information, the lack of integrated management, and the informal chain of command that were immediate contributors to the shuttle failures. The CAIB noted that the shuttle program manager was responsible for achieving safe, timely launches at acceptable costs so that some compromise of safety was inevitable. An independent safety assurance organization and a learning organization culture were needed to "more safely and reliably operate the inherently risky Space Shuttle." [7]

Accepted Shuttle analysis summary

In the Challenger tragedy, 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 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. Attempts were made to strengthen the NASA safety culture, but the Columbia tragedy, due to recurring but neglected foam damage to the heat shield tiles, was again attributed to poor safety culture and the normalization of deviance. The key recommendation was to improve safety by improving NASA organization, culture, and operations.

4. DIANE VAUGHN'S FURTHER ANALYSIS

Diane Vaughn developed a surprising explanation of the Challenger tragedy, later supported the CAIB which used her analysis, and did further analysis leading to her unexpected conclusion that top management was to blame. Diane Vaughn reconsidered the accepted Challenger accident analysis including her own and provided this significantly different explanation.

The Rodgers Commission report had found that NASA managers were under pressure to launch on time and had deliberately gone ahead with a launch that they had been warned was risky. Furthermore, in doing so they had bypassed the required safety procedures. It was generally believed that self-serving and unethical managers had caused the tragedy. In [8] Vaughn contradicted the supposed facts and motivations described in the Rodgers Commission report. She concluded that the accident was caused by mistakes, not

misconduct. Vaughn had developed a theory that misconduct in complex organizations was due to competitive pressures to violate rules if the pressures were not effectively blocked by the organization or environment. At first Challenger seemed to fit this theory but the facts did not support this analysis. Actions that appeared to be rule violations did conform to the rules, contrary to the Rodgers Commission findings. (The rules can be considered unsatisfactory, a possibility not mentioned by Vaughn.) Vaughn noted that the actions that the Commission, the press, the public, and she at first thought were rule violations were sincerely believed to be according to the rules by those making the decisions. [9]

This observation led to Vaughn to a different explanation of Challenger, the concept of the normalization of deviance. The underlying cause of the Challenger disaster was the repeated choice to fly the shuttle with a known O-ring problem. NASA became so accepting of O-ring erosion that it was considered normal and nonthreatening. A planned O-ring redesign had low priority and a long delay. Although there was pressure to launch, the usual launch readiness procedures were followed. The O-ring problem was identified as an "acceptable risk" using the standard safety process. A "waiver" is a decision based on a formal risk assessment, not as the Rodgers commission thought, a decision to simply ignore a launch constraint. High technology operations require a trade-off between cost, schedule, and safety. Bureaucratic decision making and goal compromises including safety are normal and necessary. Even after the loss of Challenger and the widespread impression of mismanagement, the key decision makers defended their acceptance of the O-ring risk as correct and justified. "It was conformity, not deviance, that caused the disaster." [11]

Vaughn found that the Rodgers report misled the public about the causes of the accident and that this prevented everyone from realizing that the causes of failure were not eliminated, and another disaster could occur. By blaming unethical, self-servingly rational middle managers, public attention was diverted from the top NASA administrators who had the actual responsibility for the disaster. [12] This was the most acceptable explanation "for NASA because the cure was easy: fire and retire responsible managers, fix the decision-making structure and the technology, and go on. The program could not survive public awareness that the technology was as risky as it really was." [12]

Vaughn's explanation of the Challenger decision used three specifically identified factors, the production of culture that accepted risk, a culture of production that compromised safety, and structural secrecy that concealed the seriousness of the O-ring problem. She found that the Rodgers Commission made mistakes due to time constraints, limited information sharing, and post-disaster hindsight that biased the Commission's

attitude and selection of material and witnesses toward blaming middle management. The Commission did not understand how the NASA culture had operated to produce the Challenger launch decision. The Commission's theory was that unethically calculating managers had decided to act wrongly, using the self-serving rational-choice explanation of human behavior. Vaughn found that although rules were not violated, harm was done. NASA's actions were generally considered deviant, not following expected standards. The need for the shuttle to be a commercial success led not only to compromises but even misrepresentations of safety, cost, and schedule. The cultural belief in acceptable risk allowed NASA to continue launching despite increasing concern about safety as O-ring damage continued. The organization structure and limited role of safety concealed the seriousness of the O-ring problems. [11]

The analysis of the Columbia Accident Investigation Board (CAIB) report, to which Vaughn contributed, found that the Challenger and Columbia accidents had the same cause and were explained by her theory developed for Challenger. The basic question was identical in structure. Why did NASA continue to fly with known O-ring erosion (or known foam debris strikes) in the years preceding the Challenger (or Columbia) launch, and why did managers conclude that launching in very cold temperatures (or with debris strikes) was not a threat to safety, despite the concerns of the engineers? The CAIB and Vaughn found that both accidents resulted from a similar failure of NASA's organizational system and that the causes of Challenger had not been fixed. [13]

The CAIB considered the fundamental question as to whether individual knowledge and motivation or organizational structure and culture determines decisions. NASA and the military believe in individual leadership within a hierarchical organization and usually assign the blame for failures to individuals. Sociologists and organizational theorists instead often believe that most individual actions are socially and organizationally determined. CAIB discussions reflected an understanding that the causes of the accidents were in NASA's organizational system and that other managers in the same position would have acted the same. The CAIB emphasized that organizational and cultural changes were necessary to reduce the chance of another accident. Accidents could not be completely prevented because of unchangeable shuttle design factors. Even though the organizational and cultural causes of the Shuttle accidents were documented in the CAIB report and a Congressional hearing, most people still accept the theory that the faulty shuttle decisions were made by individual actors making rational decisions that were unethical and self-serving. [13]

5. HIGH RELIABILITY THEORY (HRT) AND NORMAL ACCIDENT THEORY (NAT)

The CAIB evaluated NASA's performance considering the two well-known but partly conflicting theories of reliability and failure. These are High Reliability Theory (HRT) and Normal Accident Theory (NAT). [7] NAT asserts that accidents are normal. Technically complex and tightly coupled systems will inevitably have accidents that cannot be predicted or prevented. HRT was developed to counter NAT. It claims that accidents can be avoided by good organizational design, a safety culture, and an obsessive determination to prevent failure. High technology organizations seem to naturally assume something like the optimistic HRT rather than the pessimistic NAT. The CAIB used the HRT approach to conclude that the cause of the shuttle accidents was that "NASA's safety system had failed." [14] The safety system should prevent accidents. To the contrary, NAT indicates that shuttle is risky and that shuttle accidents would unavoidably occur at the historical rate of about 1 in 100 launches. More attention to safety will prevent some but not all accidents in a high-risk system. Risk must be analyzed, reduced by simplifying design, and neutralized by careful operations. Much can be done to minimize known risks and create additional capacity to deal with unanticipated events, but preventing all disasters is impossible. [14]

The Rodgers and CAIB reports found that NASA did not meet the requirements of a High Reliability Organization (HRO). The acceptance of increasing risk demotivated NASA from investigating anomalies occurring on successful flights. Past success was taken as a justification continue flying without redesign. Flawed decision-making ignored engineering doubts because there was no solid engineering evidence to prove that the risks were significant. A broken safety culture made NASA susceptible to schedule pressure. "The CAIB, in summary, explicitly concluded that NASA had failed to prevent what was judged to be a preventable disaster. CAIB judged that NASA is not a High Reliability Organization, which, presumably, would have prevented both disasters." [14] The NASA of the Apollo era seems to have been a High Reliability Organization, [14] but the NASA that designed the shuttle did not avoid the implications of Normal Accident Theory. In hindsight, every accident could have been prevented, but looking forward most seem very unlikely and cannot be convincingly predicted. The Rodgers and CAIB reports exhibited two common analytic flaws, hindsight bias suggesting that the causes of the accidents were obvious and discounting statistical base rates that showed the chance of disaster was roughly 1 in 100.

According to NAT, a well-designed rational hierarchical organization may cause accidents during normal operation. The formal shuttle launch decision process

required quantitative data, not engineering concerns, to cancel a launch. NASA had no method to identify and investigate the serious concerns of respected engineers if they were not supported by engineering data. Informal and self-suppressed low-level discussions of these concerns were discovered by the Rodgers and CAIB investigations. Preventing concerns from being brought up ensures that early tentative warning signals will be missed.

HRT requires every even minor anomaly to be explained and corrected. This can only be done if the organization is given the necessary funding and support and if individuals are free to raise problems, as in Apollo era NASA. "A sense of dread must exist with regard to the potential consequences of disaster. A widely shared understanding is required that such disasters (think of a nuclear explosion) must be prevented at all costs." [14] After the Apollo 1 fire, after the initial calculations showed alarmingly high risk, NASA felt the fear of failure. HRO's are distinguished by a pervasive safety culture. NASA must take risks, but they should be responsible risks considering performance, cost, and schedule. [14] For the highest reasonably possible safety, NASA should reestablish the culture of a High Reliability Organization that it had in the Apollo era.

The story of the shuttle is simple. Two fatal accidents occurred because, instead of calculating the risk, the shuttle adopted unsafe design approaches and removed safety provisions, producing a high-risk system with a 1 in 100 chance of failure. Any specific failure might have been predicted and prevented, but the expected high failure rate is due to many unpredictable complex failure scenarios, each with small probability.

6. THE SYSTEMS APPROACH TO SAFETY

Leveson and coauthors have suggested using an alternative systems approach to safety that goes beyond NAT and HRT. They find that these theories have narrow definitions, ambiguous concepts, and confuse reliability with safety. NAT is too pessimistic and HRT too optimistic. [15] [16]

Complex high-risk systems have several sources of risk and different risks predominate in different systems. Aircraft carriers are examples of HRO's and their risk is due to the difficulty of their tasks, launching and landing planes. This risk is reduced by extremely well planned and frequently practiced operational routines. Failures are usually blamed on the pilot. HRO underestimates the problems of complexity and uncertainty. The Shuttle also has high operational risk in launching and landing, but much of the risk is due to the complexity of engineering and decision-making emphasized by NAT. NAT underestimates the potential of organizational methods to cope with complexity and uncertainty. [16] The shuttle was designed with intrinsic

high risk and the bureaucratic decision-making process suppressed risk analysis and made it easy to ignore risk indicators. If safety were the only goal, aircraft and spacecraft would never fly. A mission should measure risk and do justifiable trade-offs to determine how much risk will be allowed.

Leveson and coauthors alternative systems view of safety includes top-down systems thinking applied to an integrated technical, organizational, and social system. The usual view of accidents as causal chains of hardware failures and human errors is abandoned. Cause and effect models cannot account for the indirect multiple causes and feedback that can create accidents in complex systems. "Accident models based on systems theory consider accidents as arising from the interactions among system components and usually do not specify single causal variables or factors." [16] Both NAT and HRT overemphasize redundancy because they misunderstand the cause of accidents, since both theories mistakenly assume all accidents are caused by component failures. The systems approach asks what went wrong with the system that produced the accident, including organizational, cultural, and human factors. [15]

Reference [15] examined NASA's plans to return humans to the Moon and go on to Mars and demonstrated how tradeoffs among safety, performance, schedule, and budget can be evaluated. The analysis and simulation included the entire system from Congress and the Executive Branch down to management and engineering. It found that attempting to speed up development gave little improvement in schedule because of the resulting increases in rework, but a speed-up greatly reduced the safety of the resulting design. Early emphasis on safety improved schedule and budget due to fewer problems being discovered later in design and test, which was a surprise to managers but not engineers. [15]

Leveson and coauthors also described the modeling, analysis, and engineering of a safety culture. [17] They performed a PRA on the proposed NASA Independent Technical Authority by creating a model of the NASA manned space safety culture. The model included safety engineering, reviews, and decision-making as well as the risk factors that led to the shuttle accidents. They used a systems approach that included nonlinear, indirect, and feedback relationships that better describe complex systems behavior than traditional sequential causal chains. Major accidents occur after an organization has gradually moved into a state of higher risk because of declining concern for safety, as seen in both shuttle tragedies. Creating a dynamic control model of this process allows the identification of systemic risk indicators. Most risk indicators are lagging since they begin to increase only after the risk has already become large. Lagging indicators include the accumulated number of outstanding waivers, the

resources provided for safety activities, schedule lag and schedule pressure, the number of accidents and close-calls, and the perception of risk level by management. Leading indicators are much more useful in taking steps to reduce future risk. Key quantitative leading indicators are the numbers of uninvestigated and unsolved problems and the fraction of all outstanding problem reports being actively investigated. Some qualitative leading indicators of risk are limited experience, knowledge, skill in the safety management and staff, reduced safety resources, poor quality of safety analyses and incident investigations, and limited power and authority of the safety organization. [17]

7. FURTHER DEVELOPMENTS

NASA's latest Apollo-like rocket designs directly reverse the risky choices of shuttle. Having a hardened crew capsule, the crew capsule above the rocket and fuel, and a launch abort system implicitly acknowledges the safer design configuration of Apollo.

The CAIB found that the shuttle program manager was responsible for safety, schedule, and cost so a compromise of safety was unavoidable. The CAIB recommended that responsibility for safety should rest with an independent technical authority. [7] The GAO found that NASA's commercial crew program had not implemented this separation. [18]

8. SUMMARY

The Challenger and Columbia tragedies can be explained using direct cause and effect, but NAT and HRT provide deeper insight. Minimizing serious accidents requires designing safer systems and operating these systems more carefully.

Two direct causes – carelessness and too risky to fly

One explanation of the shuttle tragedies is that the partial O-ring failures and foam-caused tile damage were disregarded, leading to mistaken decisions to fly. Middle management negligence and the lack of a safety culture were blamed. The other explanation is that fatal accidents were inevitable because the shuttle is a high-risk system with a 1 in 100 chance of failure. The shuttle design removed safety provisions without calculating the increasing risk. The immediate causes of the accidents were badly mistaken decisions to ignore failure warnings, but the original cause was the poor safety and reliability of the shuttle design itself.

Accident theory safety guidance

The two direct causes of the shuttle tragedies, operational carelessness and a design too risky to fly, are the core concerns of the two major accident theories, HRO and NAT. HRO suggests that accidents caused by human errors can be eliminated by organization design

while NAT claims that high risk is unavoidable in complex and highly connected technical systems. NAT and HRT are essentially contradictory approaches developed for different kinds of systems, but each is very useful in understanding different aspects of space system safety. The inspiration for NAT was a nuclear reactor failure. NAT emphasizes human errors due to limited span of comprehension and poor decision-making capability. These errors are more common in dealing systems having high complexity indicated by many parts, many interconnections, and the potential for unknown linkages and failure cascades. NAT analysis is top-down, based on safety objectives and realistic historical base rates as used in PRA. NAT is so pessimistic, suggesting inevitable disaster, that it discourages high technology projects with serious risks having low probability. The insights of NAT suggest that PRA and other safety and hazard analysis be used to guide design and operations to reduce complexity and increase safety. The options and trade-offs concerning safety should be generally understood and accepted. Designing and operating the shuttle based on fantastically underestimated risk was an unbelievable error.

The counter reaction to NAT used aircraft carriers and nuclear submarines as examples of HRO's. These systems have long histories, many current operational instances, a stable environment, and repeated identical operations. HRO emphasizes the possible achievement of safety by establishing the right organization, culture, and individual awareness. In a safety culture, any anomaly, even a temporary sensor glitch, is traced to its cause, understood, and corrected, no matter what. HRO emphasizes cause and effect and individual responsibility. HRT analysis is bottom-up, based on individual actions and their consequences. HRT is optimistic. Human understanding is sufficient to solve our problems. Reliability expectations, like cost and schedule estimates, are based on idealistic model where nothing goes wrong. Cost, schedule, and failure rates are usually higher than expected. The insights of HRT suggest that a safety culture can be established where all safety questions are investigated and everyone takes responsibility to solve them. This includes potential design problems and unexpected operational incidents.

Apollo's successful moon landing is often used as an example of extraordinary human capability. The fact that it was done on the first attempt and repeated several times without loss of life in space reinforces its impact.

Apollo showed how to achieve safety in space, but NASA ignored the lesson. Although the theories had not yet been developed, Apollo's awareness of high risk was like that in NAT while its safety culture was the one recommended by HRO. Apollo conducted PRA and concluded that the risk was high for many fatalities before reaching the moon. Upper management, middle management, and working engineers were aware of the

risk of failure. Many lived with an ever-present troubling sense of fear. This led to conservatism in defining the mission scenario and overall architecture. There was emphasis on communications, teamwork, and paying attention to details. The policy was to always bring up problems that were not fully understood.

NASA's attitude toward risk was very different in Apollo and Space Shuttle. NASA had a good safety culture during Apollo but lost the ability to recognize and repair obvious threats before shuttle. [1] The amazingly favorable safety record of Apollo led to overconfidence and ignoring risk, which produced the inevitable disasters in shuttle. The failure investigations blamed the middle managers running operations who might have intervened against policy. Some design changes were made, but the shuttle was simply too risky.

The Challenger tragedy was caused by an Apollo mistake, terminating risk analysis in shuttle design and operations. Upper and middle management denied risk and engineers' realistic fear of risk was ignored.

9. REFERENCES

1. Jones, H.W., "NASA's Understanding of Risk in Apollo and Shuttle," 10.2514/6.2018-5235, AIAA SPACE and Astronautics Forum and Exposition, 17-19 September 2018, Orlando, FL.
2. Rehtin, E., *Systems Architecting of Organizations*, CRC Press, Boca Raton, 2000.
3. 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.
4. 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>
5. McCurdy, H. E., *Faster, Better, Cheaper: Low-Cost Innovation in the U.S. Space Program*, The Johns Hopkins University Press, 2001.
6. Mahler, J. G., *Organizational Learning at NASA: The Challenger and Columbia Accidents*, Georgetown University Press, Washington, DC, 2009.
7. CAIB, *Columbia Accident Investigation Board*, Vol. I, August 2003.
8. Vaughan, D., *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*, University of Chicago, 1997.

9. 17 Rodgers Commission, Report of the Presidential Commission on the Space Shuttle Challenger Accident, 1986.
<http://history.nasa.gov/Rodgersrep/genindex.htm>
10. 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.
11. Vaughan, D., "[Theorizing disaster: Analogy, historical ethnography, and the Challenger accident](#)," Ethnography, SAGE, London, 2004.
12. Vaughn, D., "The Challenger Space Shuttle Disaster: Conventional Wisdom and a Revisionist Account," in Ermann, M. D, and Lundman, R. J., (eds) Corporate and governmental deviance: Problems of organizational behavior in contemporary society, Oxford University Press, 2002.
13. Vaughan, D., "[NASA revisited: Theory, analogy, and public sociology](#)," vol. 112, No. 2, American Journal of Sociology, 2006.
14. Boin, A., and Schulman, P., "Assessing NASA's Safety Culture: The Limits and Possibilities of High-Reliability Theory," Public Administration Review November-December, 2008.
15. Leveson, N., Dulac, N., Marais, K., and Carroll, J., "[Moving beyond normal accidents and high reliability organizations: A systems approach to safety in complex systems](#)," Organization studies, 2009.
16. [Marais, K., Dulac, N., and Leveson, N., "Beyond normal accidents and high reliability organizations: The need for an alternative approach to safety in complex systems,"](#) Engineering Systems Division Symposium, MIT Cambridge, MA, 2004.
17. Leveson, N., Dulac, N., Cutcher-Gershenfeld, J., Barrett, B., Carroll, J., Zipkin, D., and Friedenthal, S., "Modeling, analyzing, and engineering safety culture," First Conference of the International Association for the Advancement of Space Safety, Nice, October, 2005.
18. Government Accountability Office (GAO), NASA COMMERCIAL CREW PROGRAM, GAO-18-476, July 2018.