IAC-19,D1,5,8,x51389

Space Program Advocacy Can Distort Project Management and Damage Systems Engineering

Harry W. Jones[a]*

[a] *Bioengineering Branch, Mail Stop N239-8, NASA Ames Research Center, Moffett Field, CA, 94035-0001, harry.jones@nasa.gov*
* Corresponding Author

Abstract

Over-optimistic project advocacy often causes exaggerated performance claims and underestimated costs and schedules. This can distort project management and damage systems engineering. NASA projects such as the space shuttle and Hubble are extreme examples. NASA's spectacular success in the Apollo moon landings seems to have produced overconfidence and carelessness, but also to have gained tolerance for unrealistic claims and forgiveness when they were proven wrong. Apollo risk analysis predicted many astronaut fatalities. This was believed but was potentially damaging to the Apollo program, so risk analysis was discontinued. The moon landings beat bad odds because Apollo obsessively reduced risk. Its success seemed to confirm that risk analysis was unreasonably pessimistic and that risk could be overcome by good engineering. This understanding caused risk to be increased during space shuttle engineering and led to an unnecessarily dangerous approach. The shuttle design placed a fragile spacecraft next to the fuel tanks and failed to provide crew escape or launch abort. These design decisions directly caused the Challenger and Columbia tragedies. After Challenger, risk analysis was re-established. The current rocket and capsule design does consider risk and the result strongly resembles Apollo. Apollo advocacy led NASA to abandon risk analysis and this was ultimate cause of the Shuttle tragedies.

Excessive advocacy that distorts risk, cost, and schedule could be prevented in an ideal organization that used systems engineering to make rational and fair decisions. However, most real organizations accommodate human and group needs using informal methods often described as "the system." Humans have biases, use innate decision making heuristics, instinctively rely on "gut feel," and establish deviant groups through groupthink. Expecting organizations to become totally rational is impractical, but specific problems such as neglecting risk and underestimating cost and schedule can be directly challenged with some hope of success.

Keywords: project advocacy, Apollo, shuttle, ideal organization, systems engineering, "the system"

Acronyms

CAIB = Columbia Accident Investigation Board
PRA = Probabilistic Risk Assessment

1. Introduction

NASA's spectacular success in the Apollo moon landings was achieved against very bad odds. Risk analysis predicted that the Apollo program would suffer many fatalities before the first man came back safely from the moon. This fear and the tragic Apollo 1 fire intensely focused the program on eliminating risk as much as possible. However, the expected loss of crew was thought to be damaging to public support of the Apollo program, so risk analysis was discontinued. Program advocacy abolished engineering risk analysis, with unfortunate future consequences.

The dramatic triumph of Apollo created overconfidence and encouraged increasing acceptance of risk in the space shuttle design. The shuttle was unnecessarily dangerous because it placed a fragile tile covered crewed spacecraft next to the fuel tanks and eliminated the crew escape and launch abort used on previous missions. These design decisions decreased the shuttle cost and weight to create economic justification and support for the program, but they added excessive risk. These design compromises contributed directly to the Challenger and Columbia tragedies.

After Challenger, risk analysis was reinstated and found that the designed-in probability of a fatal accident was about 1 in 100 launches, which was ultimately considered unacceptable. The current NASA launch system design is intended to reduce risk and the rocket and crew capsule designs are similar to Apollo's.

As in shuttle, program advocacy can distort systems engineering trade-offs and add excessive risk. The systems engineering process should be used to rationally, to openly balance risk with cost and other design requirements.

2. Apollo

The Apollo program was a spectacular 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. The last three Apollo flights were cancelled and Apollo achieved only six of the ten planned moon landings.

Joseph Shea, the Apollo program manager, chaired the initial Apollo systems architecting team. A "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." [1]

This assessment led 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." [1]

However, explaining the high risk was not considered prudent. The NASA Administrator felt that if the risk calculations were made public, "the numbers could do irreparable harm." The Probabilistic Risk Assessment (PRA) effort was cancelled and NASA avoided doing numerical risk assessment as a result. [2]

2.1 Apollo 1

A fire occurred during a simulated flight conducted in the Apollo 1 capsule on the launch pad, and three astronauts died from smoke and flames before rescue was possible. Shea recalled an earlier fire discussion, "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.'" [3] "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." [4]

The cause of the Apollo 1 failure was a failure to anticipate a known hazard, a fire in a pure oxygen environment. Astronaut Frank Borman said, "none of us gave any serious consideration to a fire in the spacecraft." [5] The risk of fire was discounted, even though several fires in other pure oxygen atmospheres had caused deaths. Later spacecraft designs used Earth normal atmosphere, reduced the combustibility of materials, and developed capabilities for escape and rescue.

After the Apollo 1 fire, reliability was made central by an engineering culture 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." [5]

2.2 Apollo 11

Apollo 11 successfully landed on the moon in 1969. The high risks of the moon landing were well understood. Apollo 11's CM pilot Mike Collins described it as a "fragile daisy chain of events." [6] Collins and Neil Armstrong, the first man to step on the moon, rated their chances of survival at 50-50. [7]

A major factor in the success of Apollo was the extreme attention paid to reliability and crew safety. The initial awareness of high risk led to careful mission planning, diligent attention to reliable design, and careful mission operations. The policy was to speak and to listen, to always bring up issues that were not fully understood. Apollo showed that an intense effort to reduce risk can achieve results far beyond reasonable expectation.

2.3 Apollo success leads to overconfidence

Unfortunately, this amazing success led to extreme overconfidence. The head of Apollo reliability and safety decided, "Statistics don't count for anything," and that risk is reduced by "attention taken in design." [2] This attitude was carried forward from Apollo to shuttle. A NASA safety analysis explained that shuttle "relies on engineering judgment using rigid and well-documented design, configuration, safety, reliability, and quality assurance controls." [2] It was also thought that, with the attention given to safety and reliability, "standard failure rate data are pessimistic." [2]

3. Shuttle

The space shuttle transported cargo and crew to orbit from 1981 to 2011. There were 133 successful missions and two tragic failures.

The shuttle program had much less congressional support than Apollo. It was necessary to 'sell' the program with exaggerated claims or by accepting unrealistic budget cuts. [8] [9] NASA promised rapid turnaround, frequent flights, and lower launch costs. Shuttle would pay for itself by launching all NASA, commercial, and military space systems.

3.1 Denying risk in shuttle

The emphasis on performance capability and cost blocked serious consideration of risk. 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." [2]

Shuttle risk 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." [10]

3.2 Over promising cost performance in shuttle

NASA overpromised what the shuttle would achieve. Shuttle would perform all NASA, military and commercial launches and the high number of launches would make it cost-effective.

"In keeping with agency survival instincts Fletcher and others engaged in political hype to sell their program. … Fletcher initially quoted sixty flights a year (with full payload), an utterly unrealistic figure but

politically essential if human space flight was to survive and compete with expendable launch vehicles for cost savings, and even turn a profit. Although the flight rates were reduced to fifty, agency personnel were still being asked to support a mythical figure. In the words of one subordinate, 'We had to argue that [the shuttle] was cheaper. It would be cheaper than all the expendable launch vehicles. It would be better than all the expendable launch vehicles. Well, there was a feeling that we were on the razor's edge. That if we said the wrong thing, or anything like that, the shuttle would be killed.' " [11]

3.3 NASA shuttle risk analysis was strongly distorted

A contractor study of shuttle risk found the solid-fuel rocket boosters had a failure rate of about 1 in 40. However, rather than use this 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. [2] An Air Force review noted that the "arbitrary assignment of risk levels apparently per sponsor direction" with "no quantitative justification at all." The Air Force found that the boosters' track record "suggest[s] a failure rate of around one-in-a-hundred." [2]

NASA's internal analysis also minimized risk. A failure in the solid rocket booster (the failure that destroyed Challenger) was assigned a probability of 1 in 100,000. [2] Even after the Challenger accident, the NASA chief engineer thought the actual risk "would be 10 to the minus 5 … based on engineering judgment." [2]

4. 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 and disintegrated the shuttle. The crew cabin hit the ocean at unsurvivable speed at 2 minutes and 45 seconds after the breakup.

The presidentially appointed Rogers Commission identified failure causes in NASA's management culture and decision-making processes. "failures in communication … a conflict between engineering data and management judgments, and a NASA management structure that permitted internal flight safety problems to bypass key shuttle managers. [12]

The flaw in the O-ring design and the potential for flare blow-by had been known for some years but had been accepted as normal in flight readiness reviews. This has been called "the normalization of deviance." [13] Before the flight, engineers had warned about the danger of launching in much colder than previously experienced temperatures, but cold weather was not identified as a formally recognized reason to delay launch.

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

"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. … the management of NASA exaggerates the reliability of its product, to the point of fantasy." [12]

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. [13]

5. Columbia

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

"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." [14]

The CAIB's emphasis was on the organizational practices detrimental to safety and the barriers that prevent communication of critical safety information. An independent program technical authority and an independent safety assurance organization were recommended to "more safely and reliably operate the inherently risky Space Shuttle." [14]

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." [14]

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." [14] NASA had a good safety culture during Apollo but lost it before Shuttle. NASA had lost the ability to recognize and repair threats that were obvious in hindsight. [15]

6. The true lessons of the shuttle failures

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, shown by 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 serious safety issues gradually became accepted due to short launch schedules and pressure to launch. The cure would be a management led culture change, emphasizing safety in shuttle operations. {13] [14]

Management readily accepted the need to emphasize safety and to lead a safety culture change, but was not aware that misleading program promotion limited systems engineering and caused pervasive unawareness of risk.

The real problems have been mistaken. The true causes of the Challenger and Columbia disasters are complex and evolved over decades.

The sequence of events leading to the shuttle tragedies began during the Apollo era. Risk analysis was abandoned during Apollo to avoid public disapproval. Shuttle was designed without explicit mathematical computation of risk using PRA. It was over confidently assumed that engineering design was all that was needed for reliability. Choices were made to improve performance and reduce cost that clearly increased risk, such as abandoning crew escape and launch abort. Other aspects of shuttle advocacy, such as projecting an impossibly high number of flights to justify projected launch cost savings, increased time pressure and led to operational acceptance of increased risk.

When the statistically predictable failures occurred, the failure investigations focused on the lowest organizational level and the last decision points where the tragedies could have been avoided by some extraordinary action. But the time to redesign the o-rings or try to prevent foam loss and damage was in the past. Redesign is difficult in a supposedly operational system. The shuttle design was largely fixed, and the post-tragedy recommendations were to improve NASA organization, culture, and operations.

And yet the initial cause of the shuttle tragedies was the choice by the Apollo-era NASA administrator to avoid the negative impact of risk analysis. Subsequently the shuttle was designed to cut cost and increase performance at the expense of higher 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, and unlike Apollo, the shuttle had no crew escape or launch abort system. These design compromises directly contributed to the Challenger and Columbia accidents. The early fundamental management and design errors were ignored in favour of blaming operational organizations and people who with luck might have beaten the high probability of a failure. After Challenger, NASA restored risk analysis. Realistic estimates of the probability of space shuttle failure are roughly 1 in 100. [16] Ultimately, it was generally accepted that the shuttle design itself was too risky to continue to fly and the program was cancelled.

7. Key problem indicators

The history of the shuttle problems is unique and complicated and it has been analyzed in many books and articles. However, many project failures unfold in a similar pattern of a challenging underfunded goal, exaggerated promises of performance, underestimated cost and schedule, neglect of risk, formation of a committed ingroup, and inability to understand criticism until events forced the acceptance of reality.

7.1 NASA similarly over-sold Hubble

Hubble shows some of the same issues. "Prior to launch, NASA exaggerated the telescope's potential. Specifically NASA described the high quality photographs that would be the product of the experiment and how extraordinary these pictures would be. The problem was that NASA knew the telescope could not do what it claimed." The mirror had been mis-shaped and the final assembly was not tested to save cost. The mirror problem "was more glaring because of the exaggerated expectations." [7]

"NASA's poor public relations exacerbated the problems caused by the telescope's spherical aberration. To a great extent, NASA brought the crisis on itself. It oversold the telescope before it was deployed; it failed to developed a clear plan for dealing with first-light images and early release of photographs; it provided misleading flight reports; and it reported prematurely and incorrectly that the Hubble could not produce photographs. NASA's poor handling of the Hubble, coupled with its poor handling of the Challenger explosion, suggests the agency must improve its crisis communications if it hopes to maintain the trust and support of Congress and the American people into the

twenty-first century." [18] Shuttle launched the Hubble and performed four repair and upgrade missions. Without shuttle, Hubble would have been a failure due to its exaggerated promises and neglect of testing to reduce risk.

8. The solution is obvious – systems engineering

NASA, like most project organizations, has a systems engineering process that begins with stakeholder requirements, develops technical requirements, plans design and test, determines cost and schedule, and considers reliability, safety, and risk. The obvious and frequently repeated recommendation to avoid project disasters is simply to do the engineering right.

It has proved practically impossible to actually implement the ideal form of systems engineering. The reports of the Challenger and later Columbia investigations recommended establishing independently reporting and funded safety organizations, but this has been difficult to implement. Projects are done by an actual human political process that is different from the ideal systems engineering process.

9. The ideal organization and the real system

The ideal organization, a company or a bureaucracy, is intended to be a machine rationally designed to accomplish its goal, maximizing profit or administering some activity. The organization is typically a hierarchical structure of roles and functions that are filled and performed by human beings.

The structural aspect of organizations is the most common way of explaining them. Organizations are designed, and their structure is created, to do a task. The usual diagnosis of failing organizations is that they are not doing their job because they are not using the right structure.

Organizational theorists have explained that the human and political aspects of groups are as important as the structural view. Humans have different capabilities and needs and use both rational and instinctive decision processes. They usually work in groups and teams with various formal and natural means of interaction. The necessary process of project selection and resource allocation generates conflict and introduces power, politics, and ethical dilemmas. [19]

From the rational point of view, organizations are deliberately constructed to attain specific goals. Natural system theorists claim that the behaviours shared by all social groups are more important. There is often a difference between the publicly stated rational goals and the real goals of the organization. Most important, organizations are social groups that seek to adapt, gain support, and survive. [20]

NASA, like other organizations that deal with unique, complex, poorly structured problems, tends to be flexible and informally managed. Work gets done by bypassing the formal structure. In such highly flexible organizations, "the political games that result are played without rules." [21]

People usually would prefer to act rationally and to play by the rules, so much so that they tend to ignore the obvious human and political aspects of organizations. This can create expectations far from reality.

It has been claimed that the textbooks on organizational design describe ideal fantasy organizations. "Organizational reality more closely approximates a snakepit than the bland picture most texts convey." [22] Working students were told about both a textbook ideal fantasy organization and a realistic political "snakepit" where "nobody really knows what is going on." Most students felt they were working in a snakepit but they wanted to be taught the ideal fantasy. The students believed in the ideal organization as "an article of faith." "Since the organizational idea is a fantasy, believing in it requires the creation of an illusion and shielding it from reality." [22] "Defense of the organization … (is) a righteous and virtuous action." [22]

10. Everyone knows about "the system"

When managers do illogical things, when the organization makes unrealistic decisions, people who ask why are often told, "It's the system." When actions are taken that seem unjustified and questions are asked, we hear, "The system isn't fair."

In contrast, the ideal organization is rational and just, open to criticism and willing to explain and discuss issues. An ideal organization and the real system seem to be two fundamentally opposed things, but in fact they represent two inescapable aspects of all organizations. Any organization has rational goals and structure, and intuitive people and politics. Many details about the environment and the organization determine if the goals are achieved, people fulfilled, and process approved. Both successful and failed organizations are built with similar ideas and human materials. And the same organization can go from fantastic success to unbelievable failure, Apollo to shuttle.

11. "The system" has deep complicated origins

The ideal organization, especially the ideal project organization, can be built and guided by excellent texts and handbooks on project management and systems engineering. "The system" emerges from individual psychology and group behaviour and is largely learned by participation and is controlled using intuition. There are no teachers or text books for "the system." System participants know how to play the game but cannot explain it. Behaviour is monitored and deviations punished.

The system is not a creation of reason. It cannot be corrected by facts and logic. It cannot be replaced by an ideal organization simply by logical argument.

The system is created by the dynamic operation of individual psychology and group behaviour. The general drivers of group sociology seem unavoidable but some specific actions such as exaggeration and deception can be directly opposed. Understanding the group needs that are met by "the system" and the direct causes of specific unwelcome actions can help establish more reasonable and honest behaviour.

12. Rational organization versus instinctive system

The rational organization and the instinctive system reflect the two basically different kinds of human thinking, logical and intuitive. Reason and instinct are the basis of two conflicting political and ethical views of human life. [23] [24]

Rational thinking supports a liberal bias, the hope that reason and fairness can create a better society. The liberal inclination is questioning and egalitarian. It emphasizes freedom and equality, ethics and fairness. Individuals are responsible for their behaviour and should exert inner directed self-control. [24]

Intuitive thinking supports a conservative bias, the hope that loyalty and respect can preserve the existing society. The conservative inclination is accepting authority and being loyal to the group. Individuals can depend on the group to guide their behaviour and should accept other directed group control. [24]

Liberal and conservative thinking are conflicting moral systems. "Moral systems are interlocking sets of values, virtues, practices, identities, institutions, technologies and evolved psychological mechanisms that work together to suppress or regulate self-interest and make cooperative societies possible." [24]

Liberal values are an ethics of individualism, autonomy, freedom. Conservative values are an ethics of community, conformity, duty. Liberal values are the foundation of modern science and democracy. A liberal bias supports innovation, internationalism, individualism, independent thinking, encouragement of diversity, providing rational critique.

Conservative values support traditional religion and may accept a `more authoritarian organization. A conservative bias supports tradition, patriotism, human instinct, groupthink, enforcing conformity, suppressing dissent. Although both liberal and conservative values are needed, they are in continuing conflict.

13. Instinctive behaviour in NASA projects

The political and ethical bias of an organization strongly affects the behaviour of the people in it. Individuals in a liberal organization will try to work rationally and those in a conservative organization will tend to operate instinctively. NASA's decisions in the shuttle and Hubble programs reflect many instinctive problems in decision making.

Some of NASA's problematic program actions can be explained as caused by specific instinctive procedures. Such direct explanations can suggest how we might avoid similar problems in the future. A piecemeal approach to restoring rationality may be more effective than simply recommending that NASA become a rational organization and do good systems engineering. The official ideal description of NASA already requires this.

Examples of the use of traditional, instinctive, and intuitive decision making are given below following a typical project time line. Obviously these problems are not found only in NASA projects, but are universal nearly inescapable human and group behaviours. But NASA symbolizes the nation's and much of the world's aspiration for rational scientific progress in space. NASA should set examples of great success rationally achieved. We have done it before and we can do it again. We first must solve the human and social problems that get in the way.

14. Examples of irrational thinking in projects

A typical project timeline is used as a basis to describe project behaviour. Questionable actions are identified and causes are suggested at sequential steps.

14.1 Project concept

NASA project concepts include a moon landing, space plane, space telescope, space station, moon colony, Mars visit, etc. These concepts all existed before NASA and it seems that all the great projects were adopted as goals in NASA's early days. The overconfidence bias is presuming that you can do more than practically reasonable. NASA was not very confident during Apollo but its fantastic success led to overconfidence in shuttle. The availability bias limits attention to the obvious and acceptable, such as the traditional project ideas. The potential for military use of space has been little recognized until lately.

14.2 Project purpose

The projects have clear direct purposes but also higher level goals. Apollo aimed to place a man on the moon but also to beat the Soviets. Shuttle was to provide space transportation but also to continue the admirable American progress in space. Beyond the rational direct goal, psychology and politics impose further goals. Organizations are usually impelled to survive and even expand, driven by the self-interest bias. Rational project planning usually includes an end date rather than the unlimited survival urged by the self-interest bias.

14.3 Project customer

Since Apollo NASA has proposed its own legacy projects, so there are no paying customers to set requirements and reject unnecessary desirements. A customer provides a reality check. The self-interest bias makes it seem reasonable to follow your own goals rather than serve others' objectives. The military has been a potential customer, but NASA has avoided military involvement to preserve its image as civilian and scientific, open and peaceful. NASA's push to have shuttle meet military launch needs led to damaging design compromises.

14.4 Project planning

Project planning is subject to many intuitive biases. The overall problem is optimism and overconfidence. The project deliverable's performance is greatly over estimated. The proposed budget and schedule are insufficient. The budget and schedule include only the obvious necessary tasks that are noticed due to the availability bias, that that our attention is captured by the obvious. This is related to the myopia basis, that our vision is short sighted. The possibility that errors, failures, and rework can feedback to explode the budget and schedule is not considered. Good budget and schedule planning uses historical experience to establish an expected baseline. Ignoring established base rates is a common cognitive failure. People dislike the discomfort of thinking about risk. Potential events with high negative impact can be ignored if they have low probability. The instinctive bias toward risk aversion can lead to unawareness and denial of risk.

14.5 Project advocacy

Over-optimistic performance, budget, schedule, and risk assessment are often unintentional mistakes, but they can be deliberate deceptions to advocate the project. A deliberate low bid can be used to win a contract, with change orders and even bail outs expected to make it profitable. In some cases a low bid can be knowingly accepted by a customer to gain higher level approval. Over selling is justified as necessary for survival, to gain approval, as known and accepted, and because everybody does it. People tend to respond to a competitive situation where failure is possible by the formation of a closed competing group that resorts to deception and concealment. Cooperative internally trusting groups conduct distrust and conflict with other groups. This is natural instinctive group behaviour, since project group survival requires securing funding against rival groups. Management may think it better to allow deceptive competition than to enforce cooperation.

14.6 Project conduct

Since the original project planning was more intuitive than rational, it seems natural to proceed using engineering judgment, trusting to the expertise of respected managers and engineers. Expertise is built up through years of subject area experience. It manifests itself as intuition or "gut feel," creating a feeling of right understanding and certainty. It is difficult to explain an intuitive conviction, but it is impossible to ignore. Instinct and intuition are the opposite of rational analysis. Unfortunately intuitive judgment does not transfer from one area to another; it is specific to the situation where it was subconsciously learned. The Apollo engineers working on shuttle were certain that engineering judgment could ensure reliability, but Apollo had minimized overall mission risk while shuttle accepted increased risk to meet other goals. In shuttle, rational overall risk analysis was abandoned in favour of misleading intuitive judgment. Overconfidence and taking an inside view of the project leads to ignoring past experience and rejecting criticisms from outside.

14.7 Project defence

After a project is approved, progress may fall short compared to the optimistic best case plan. There is a need for continuing project advocacy and defence. There is a tendency to conceal or down play problems so the previous claims can be maintained. Rational economic analysis says that sunk costs, everything spent on the project so far, cannot be recovered and should not affect future project decisions. The logical directive is, "Sunk costs should be ignored," but this is rarely followed. The decision to support and work on a project is a shared group commitment. Cancelling a project for practical reasons can seem a betrayal of trust, and leaving it can seem disloyal. Appearing untrustworthy can damage reputations. Management buy-in is a good predictor of project success.

14.8 Project group fantasy

A project team tends to become a coherent group with shared interests and ideas. The group can adopt its own shared world view that sharply diverges from outside opinion and even from clear facts. This situation has been described as "groupthink." [25] A self-isolated coherent group with a strong goal can develop an illusion of correctness and invulnerability. Rationalizations are developed to reject criticism. Members are pressured to conform, and they may have to compromise their own ideals of rationality and ethics to support their group.

14.9 Nonrational project thinking summary

The conduct of many projects exhibits many kinds of questionable non-ideal thinking. There are simple human drives, such as self-interest and conformity.

There are instinctive cognitive heuristics, such as the availability bias and ignoring probability and base rates. There is instinctive reliance on expertise and the creation of deviant groups through groupthink. The operation of natural human and group psychology can produce "the system," the effective informal arrangement bypassing the ideal rational organization structure.

15. Fighting "the system"

As mentioned, the solution is obvious. Organizations should adhere to their ideals of open, rational, and fair decision making. Projects should follow the standard procedures for good management and systems engineering. Open discussion and rational critique should be encouraged and outside opinions sought. Such a drastic change seems unlikely, but the organizational ideal can motivate some improvements. Most people prefer to be rational and honest and want to work in a rational and honest organization, but some are forced to conform to a non-ideal system.

Any of the many obvious departures from ideal project behaviour can be singled out and directly challenged. The most important error has been neglecting safety due to the instinctive denial of risk. Since Challenger, PRA has been required for NASA projects. As suggested by the accident review boards, safety should be the responsibility of an independent group and should take precedence over budget and schedule. Another serious problem is the underestimation of cost and schedule due to overconfidence and myopia, ignoring experience and base rates. Outside independent review of cost and schedule needs to be made more effective. Management decision making should be more rational and professional. The use of judgment, expertise, and gut feeling, which seems unavoidable, should be checked by open rational analysis that is freely debated. The management and group commitment to troubled projects, which also seems unavoidable, should be limited by mandatory rational processes for project evaluation and termination.

Making improvements is easier when obvious serious problems occur and workable solutions are available. Given that human and group behaviour is largely not rational, achieving a totally rational organization is impossible, but small useful steps toward rationality can be made in some specific areas.

15. Discussion

Management is responsible. Upper management is responsible not just in theory, not just for making a reasonable effort, upper management is responsible for the actual project results. In the case of shuttle, the top level decisions to discontinue risk analysis, to use engineering judgment, and to accept increasing risk led to disaster.

The shuttle tragedies are similar to shock-producing disasters in other government, industrial, financial, and religious organizations. Most people suspect deliberate organizational wrongdoing, while upper management is certain that lower level employees made mistakes. The wrongdoers are exposed and the organization is repaired. But similar problems continue to occur in the same way. Sally Ride observed that Columbia had echoes of Challenger. [14] Both occurred through neglect of a known risk and both resulted in a recommendation to improve safety.

Bad decisions are caused by innate human and group psychological limitations that inhibit direct rational understanding of complex reality. Humans have conflicting goals, are subject to many biases, use ineffective decision making heuristics, are compelled by unreliable intuition, and develop unrealistic group belief systems.

16. Conclusions

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 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. The amazingly favourable safety record of Apollo led to overconfidence, accepting greater risk, and inevitable disasters in shuttle. The earlier emphasis on reducing risk was forgotten by the shuttle program. High risk choices were made that directly lead to the later shuttle fatalities.

References

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

[2] 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.

[3] 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.

[4] 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.

[5] Oberhettinger, D., NASA Public Lessons Learned Entry: 1806, Capture of Apollo Lunar Module

Reliability Lessons Learned: Program/Engineering Management, 9/25/2007.

[6] 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.

[7] 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.

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

[9] Mahler, J. G., Organizational Learning at NASA: The Challenger and Columbia Accidents, Georgetown University Press, Washington, DC, 2009.

[10] 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.

[11] Trento, J. J., Prescription for Disaster: From the Glory of Apollo to the Betrayal of the Shuttle, Crown, New York, 1987.[13]

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

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

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

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

[16] 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.

[17] Zaremba, A. J., Crisis Communication: Theory and Practice, Routledge, London and New York, 2015.

[18] Kauffman, J., "NASA in Crisis: The Space Agency's Public Relations Efforts Regarding the Hubble Space Telescope," Public Relations Review 23, no. 1, (Spring 1997) 1-10.

[19] Bolman, L. G., and Deal, T. E., Reframing Organizations, Wiley, 2003.

[20] Scott, W. R., Organizations: Rational, Natural, and Open Systems, Prentice-Hall, Upper Saddle River, NJ, Fifth Edition, 2003.

[21] Mintzberg, H., The Structuring of Organizations, Prentice-hall, Englewood Cliffs, N.J., 1979.

[22] Schwartz, H. S., Narcissistic Process and Corporate Decay: The Theory of the Organization Ideal, New York University Press, New York, 1990.

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

[24] Haidt, J., The Righteous Mind: Why Good People Are Divided by Politics and Religion, Pantheon, New York, 2012.

[25] Janis, I. L., Groupthink, Houghton Mifflin, Boston, 1982.