 ICES-2015-045

Reliability and Failure in NASA Missions: Blunders, Normal Accidents, High Reliability, Bad Luck

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

NASA emphasizes crew safety and system reliability but several unfortunate failures have occurred. The Apollo 1 fire was mistakenly unanticipated. After that tragedy, the Apollo program gave much more attention to safety. The Challenger accident revealed that NASA had neglected safety and that management underestimated the high risk of shuttle. Probabilistic Risk Assessment was adopted to provide more accurate failure probabilities for shuttle and other missions. NASA's "faster, better, cheaper" initiative and government procurement reform led to deliberately dismantling traditional reliability engineering. The Columbia tragedy and Mars mission failures followed. Failures can be attributed to blunders, normal accidents, or bad luck. Achieving high reliability is difficult but possible.

Nomenclature

CAIB = Columbia Accident Investigation Board
ISS = International Space Station
MCO MIB = Mars Climate Orbiter Mishap Investigation Board
ORU = Orbital Replacement Unit
PRA = Probabilistic Risk Assessment

I. Introduction

THIS paper discusses the history of reliability and failures in NASA. Reliability is important for achieving the desired mission performance and crew safety but it has sometimes been given insufficient attention in NASA programs. Achieving total reliability is obviously impossible with finite skill and effort, but a tragic failure involving loss of mission or loss of crew always suggests that reliability was not adequately considered.

The usual assumption seems to be that there is never any excuse for failure, that reliability is an absolute requirement, that the necessary effort should always be made to eliminate all risk. In practical situations, reliability is only one of many important factors in systems engineering and the appropriate level of reliability depends on the mission. The main concerns in a system development project are usually the system's performance, cost, and delivery date. These three factors, the iron triangle of project management, must necessarily be traded off one for another. Higher performance requires more money and development time, shorter schedule requires higher cost, etc. Usually reliability, maintainability, and operability, the so-called 'ilities, are important performance factors.

The need for reliability, the cost of improving it, and the trade-offs involved depend on the system and mission. Different NASA missions and programs have had different levels of reliability, but none has had zero probability of failure. After a failure occurs, it is often possible to identify some avoidable blunder that caused it. Some think that unavoidable system and organization complexity makes high technology accidents inevitable, "normal." Others argue that, since some risk must be accepted, accidents are expected and occur due to random bad luck. A few optimists believe that a high reliability organization can avoid blunders, normal accidents, and even bad luck.

II. NASA reliability and failure history

NASA and the space program are responsible for some of the earliest, best, and worst events in reliability history. Only the nuclear power industry has done as much to advance reliability theory or suffered such notable disasters. It is often suggested that nuclear power should be abandoned and nations known for good engineering have done so. Should humanity remain on Earth because space exploration is inevitably too risky?

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

A. NASA reliability and failure events

Table 1 shows the more prominent reliability and failure related events in NASA's history.

Table 1. NASA reliability and failure events.

Date	Mission	Event	Description	Cause	Result
1943	WWII rockets	Reliability theory origin	Reliability = product of subsystem reliabilities	High rocket failure rate	Reliability awareness
1950's	US rockets, defense systems	Early development	Reliability data, methods	High vacuum tube failure rate	Reliability programs
1961-1974	Apollo program	Kennedy speech	Man to moon and back	Gagarin in space, space race	
1966	Apollo program	Apollo 1	Fire kills three	Pure oxygen atmosphere	Intense focus on safety and reliability
1969	Apollo program	Apollo 11	First successful moon landing	Hard work, reliability focus, good luck	National pride and prestige
1970	Apollo program	Apollo 13	Oxygen tank explosion	Ground test damage, cascading failures	Re-realization of high risk
1972	Shuttle program	Initiated	Flew 1981-2011		
1986	Shuttle program	Challenger	Rocket explosion kills seven	O-ring leak, neglect of reliability	Refocus on risk and reliability
2003	Shuttle program	Columbia	Heat shield failure kills seven	Foam impact damage, neglect of reliability	Realization that Challenger problems unfixed
1992	Faster, better, cheaper	Simplify, standardize, use off-the-shelf	More robotic missions (16), more failures (6)	Reliability deemphasized due to high cost	Final rejection of faster, better, cheaper
1994	Military acquisition reform	Reinventing government	Reliability requirements and standards cancelled	High cost of procurement	Performance focus
1998	International Space Station (ISS)	Rely heavily on crew maintenance	Started 1984, first flew 1998	Reliability deemphasized	Excessive unplanned crew time
2005-2009	Constellation	Reliability for moon quick return, not Mars	Reduced reliability, testing	Reliability deemphasized	Moon designs not suitable for Mars

B. NASA reliability and failure events

Reliability analysis was invented for rockets during world War II and used variously in NASA's Apollo, shuttle, and robotic explorer programs. It was substantially deemphasized in the faster, better, cheaper era but still retains a subsidiary role in safety and systems engineering.

1. Reliability theory origin

Reliability theory was first developed by military rocket engineers who were experiencing high failure rates. It is usually credited to Robert Lusser who worked on the German V1, which was the rival of von Braun's V2. Lusser joined von Braun's rocket program in Huntsville. There he showed that that the reliability of a system is equal to the product of the reliability of its in-series components, a formula called Lusser's law. A surprising implication was that, because unmanned missiles have many more components operating in series than do piloted aircraft, missile component reliability must be orders of magnitude higher than aircraft component reliability. Based on his reliability calculations, Lusser announced that von Braun's Apollo program plans to reach the Moon would fail and he returned to Germany. (Wikipedia, Robert Lusser) (Coutinho, 1964) Because conservative component failure rates produced an incorrect very small probability of mission success for Apollo, NASA deemphasized quantitative

reliability analysis. (Paté-Cornell and Dillon, 2001) It is now thought that Lusser's law was based on earlier V1 work by Eric Pernchka (Verma et al., 2010)

2. Early development

The classical age of reliability began in the 1950's. At first, vacuum tubes were common in electronics but they were very unreliable. In the 1960's, the military handbook MH-217 included electronic failure rates and methods for reliability prediction. In the 1970s and 1980's failure rate data became available for mechanical, automotive, and telecommunications parts. Predicting, improving, and demonstrating reliability was a major activity. (Denson, 1998)

3. The Apollo program

After the Soviet launch of Sputnik in 1957 and especially after Gagarin became the first man in space in 1961, competition in space exploration became an important part of the cold war. In 1961 before a joint session of Congress, President Kennedy set the United States the goal of "landing a man on the moon by the end of the decade and returning him safely to earth." Kennedy mentioned safety, but it was third after the moon goal and the 1969 deadline. Apollo had been designed to surpass Soviet space successes that implied US inferiority.

4. Apollo 1

During a simulated countdown, liftoff, and flight conducted in the Apollo 1 capsule on the launch pad, the astronauts reported a fire. They 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.

The NASA administrator established an all government, nearly all NASA review board that blocked all other 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." (Benson and Faherty, 1978, ch. 18)

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 review board, stated "none of us gave any serious consideration to a fire in the spacecraft." (Benson and Faherty, 1978, ch. 18) The Apollo 1 fire was unexpected, unpredicted even though several fires in 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." (Oberhettinger, 2007)

5. Apollo 11

Apollo 11 successfully landed on the moon on the first attempt. The US achieved a fabulous triumph 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 awareness of risk not seen in shuttle. The Apollo 1 and 13 failures, unlike the later Challenger and Columbia failures, were due to unpredicted rather than observed and ignored problems. The Apollo success showed that by intense effort, a dedicated organization can achieve results far beyond reasonable expectation.

6. Apollo 13

Apollo 13 was on its way to the moon when crew heard a 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. (Benson and Faherty, 1978, ch. 22)

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 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." (Benson and Faherty, 1978, ch. 22)

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.

7. The shuttle program

The space shuttle, NASA's next major human program, did not use the Apollo hardened capsule and launch accident crew escape approaches later readopted. The shuttle program mistakenly promised rapid turn around and lower launch costs. It restricted all space launches to shuttle until after Challenger. But the worst mistake was believing that the shuttle was safe.

8. 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." (Rodgers Commission, 1986, v. 1, ch. 5)

The flaw in the O-ring design and the potential for flare blow-by had been known for many years and had been ignored and the risk improperly minimized. This has been labeled "normalization of deviance." (Hall, 2003) Before the flight, engineers had warned about the danger of launching in much colder than previously experienced temperatures.

After the Challenger investigation, the Rodgers Commission member and Nobel physicist Richard Feynman provided "Personal Observations on Reliability of Shuttle."

> "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. What are the causes and consequences of this lack of agreement? …
>
> 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.
>
> One reason for this may be an attempt to assure the government of NASA perfection and success in order to ensure the supply of funds. The other may be that they sincerely believed it to be true, demonstrating an almost incredible lack of communication between themselves and their working engineers. …
>
> For a successful technology, reality must take precedence over public relations, for nature cannot be fooled." (Rodgers Commission, 1986, v. 2, app. F)

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. (Vaughan, 1996)

Initial qualitative assessments of shuttle reliability were based on expert judgment rather than reliability analysis. After Challenger, probabilistic risk analysis (PRA) was adopted and applied to the space shuttle, space station, and some unmanned space missions. (Paté-Cornell and Dillon, 2001) Current NASA programs will use an Apollo style capsule and launch abort system to improve crew safety.

9. Columbia

The Columbia astronauts died 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. (CAIB, 2003, p. 9)

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 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." (CAIB, 2003, v. I, ch. 7, p. 178)

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." (CAIB, 2003, v. I, ch. 8, p. 195)

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. (Boin and Schulman, 2008)

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." (CAIB 2003, p. 180) The CAIB found that organizational changes could "minimize risk and limit the number of accidents." (CAIB 2003, p. 182) The CAIB recommended that "responsibility and authority for decisions involving technical requirements and safety should rest with an independent technical authority." (CAIB 2003, p. 184)

10. NASA better faster cheaper

In 1992, the then new NASA administrator, Dan Goldin, initiated the faster, better, cheaper approach. NASA launched sixteen faster, better, cheaper missions between 1992 and 1999, including "five missions to Mars, one mission to the moon, three space telescopes, two comet and asteroid rendezvous, four Earth-orbiting satellites, and one ion propulsion test vehicle." (McCurdy, 2001) Better, faster, cheaper emphasized simplification, standardization, and the use of commercially available components. Nine out of the first ten missions succeeded, including the Mars Pathfinder. But in 1999, four out of five missions failed, including two highly publicized JPL Mars missions. In September 1999, the Mars Climate Orbiter failed due to the mistaken use of English rather than metric units in the navigation system. In December 1999, the Mars Polar Lander was lost while landing, possibly due to a software problem.

The Mars Climate Orbiter Mishap Investigation Board (MCO MIB) investigated the Mars Climate Orbiter failure and also reviewed the results of seven other failure investigation boards. They found that several important failure causes recurred.

> "(I)nadequate reviews, poor risk management and insufficient testing/verification were each found in six of eight separate mission failure investigations. Inadequate communications were cited in five of the eight cases. … inadequate safety/quality culture … cited in three of the eight investigations." (MCO MIB, 2000, p. 33)

The MCO MIB concluded that, "Most mission failures and serious errors can be traced to a failure to follow established procedures." (MCO MIB, 2000, p. 36)

The loss of six missions in sixteen suggested that the faster, better, cheaper approach increased the risk of failure. Criticism was high. NASA was forced to abandon faster, better, cheaper.

Not all agreed. McCurdy analyzed the sixteen faster, better, cheaper missions and found that, "Engineers and other experts can reduce the cost of spaceflight and the time necessary to prepare missions for flight. Moreover, they can do so without significant loss of reliability. They can also do so with only modest reductions in spacecraft capability." (McCurdy, 2001) He believed that faster, better, cheaper increased risk only when cost was cut without reducing complexity. More missions were flown and more was learned from experience than before. (Paxton, 2007) Some also strongly argue that faster, better, cheaper was very cost effective. "NASA delivered 10 successful missions (and six failures) for less than the price of one." (Ward, 2012) (Ward, 2010)

Criticism of Goldin's management and faster, better, cheaper became even more intense after the Columbia accident. The CAIB quoted Goldin in 1994, "When I ask for the budget to be cut, I'm told it's going to impact safety on the Space Shuttle ... I think that's a bunch of crap." A news headline was, "NASA responds to the Columbia Accident Report: Farewell to Faster - Better – Cheaper." (Cowing, 2003)

11. Military acquisition reform

The NASA faster, better, cheaper initiative and military acquisition reform were part of the reinventing government movement of the 1990's. In 1994, the US military required that equipment acquisition use performance based specifications rather than design standards and methods. "Design standards including MH-217 were identified as barriers to use of commercial processes and major cost drivers in defense acquisitions." (Denson, 1998) The military standards used in reliability engineering were all cancelled. (Jackson and Das, 2001) MH- 217 data had been used not only to estimate reliability but in misguided attempts to prove that reliability goals were met. (Fragola, 1996) Component based reliability prediction does not account for the failures caused by sloppy requirements and frequent errors in design, manufacturing, and operations. (Denson, 1998)

NASA similarly renounced reliability standards. "Risk can also be managed as a resource: the new way of managing better, faster, cheaper programs encompasses upfront, knowledge-based risk assessment." (Lalli, 1998) Reliability assessments were to be based on similar systems and reliability improvement efforts. Reliability engineers insisted, against the criticism and disestablishment of their field that, "quantitatively estimating reliability requires empirical data and models using those data." (Denson, 1998)

12. International Space Station (ISS)

The International Space Station (ISS) was understood to "require high reliability and availability … but even with these requirements satisfied, long life and complexity would make equipment failure and repair inevitable." The solution was "placing as much emphasis on maintainability as reliability in design." (Fragola and McFadden, 1995) The ISS provides Orbital Replacement Units (ORU's) so that the crew can replace the subsystems that are likely to fail. The ISS goal was not failure and maintenance free operation, but rather to take advantage of the presence of the crew to sustain the availability of a long term operational facility. Unfortunately, the crew time needed to maintain systems has been much greater than originally estimated and has significantly reduced the time available for more productive work. (Russell and Klaus, 2006) Higher reliability and less maintenance and crew time would have been better.

13. Constellation

The NASA Constellation program planned to return to the moon and then go on to Mars. Although the moon was to be the test bed for Mars, the lunar base reliability approach was only suitable for the moon, not Mars. The lunar base would achieve high availability by providing spares and having the crew do maintenance, just as on ISS. The loss of a few months lunar base availability due to an unreparable failure was considered acceptable, since a lunar crew could easily and quickly return to Earth. Only mission time would be lost. For a long distance, long duration mission such as a Mars visit, an on-demand crew return is not possible. A failure would loose the crew as well as mission time. Mars systems must have much higher reliability, maintainability, and redundancy. A different reliability approach is required for Mars than than for the moon. (Jones, 2010-6287) (Green and Watson, 2008-7779) (Green and Spexarth, 2009-6427) (Mulqueen et al., 2009-6683) (Jones, 2015-047)

III. Four explanations of reliability and failure: blunders, normal accidents, high reliability, bad luck

There are two well developed but opposed theories of technological failures that were considered by the CAIB. Normal Accident Theory says that, because of complexity, high technology accidents are unavoidable, but High

Reliability Theory says that, with sufficient effort, accidents can be prevented. However, it seems that most actual failures are due to simple obvious blunders or plain bad luck. These four explanations of technical reliability and failure are summarized in Table 2.

Table 2. Four explanations of reliability and failure.

	Blunders	Normal accidents	High Reliability	Bad Luck
Failure cause	Accidents are dumb mistakes	Accidents are inevitable	Accidents are preventable	Accidents are expected but random
Safety priority	"Safety first" is said and forgotten	Safety is only one of many goals	Safety must be the actual main priority	Safety and cost are a trade-off
Safety approach	Bureaucratic rules and checks	Simplify or abandon dangerous technology	Open, critical high reliability organization	Optimize safety and cost
NASA examples	Apollo 1, Challenger, Columbia, Mars Climate Orbiter	Apollo 13	Apollo program	Faster, better, cheaper, ISS

The NASA reliability and failure events can be classified as blunders, normal accidents, high reliability, or bad luck.

A. Blunders

NASA Administrator Mike Griffin reviewed the lessons of Apollo 1, Challenger, and Columbia on a NASA Day of Remembrance:

> "These losses carry an inevitable and awful guilt … there are no smart accidents. Every one is the result of human frailty, of things done or not done that are, in retrospect, obviously wrong. … We won't again put a crew in a cabin with high-pressure oxygen and no escape route. We won't again accept a joint design that is somehow "OK" because, even though its primary o-ring fails routinely, its secondary o-ring remains mostly intact. And we will never again believe that foam moving at high speed is, after all, just foam. … when we investigate, we always find that there were people who did see the flaw, who had concerns which, had they been heard and heeded, could have averted tragedy. But in each case the necessary communication -- hearing and heeding -- failed to take place. It is this failure of communication, and maybe the failure of trust that open communication requires, that are the true root causes we seek." (Griffin, 2008)

The Apollo 1, Challenger, and Columbia accidents were due to blunders, dumb mistakes, things so obvious in hindsight that we are certain not to do them again. But the secret of success is not simply making rules to avoid all our past mistakes. There is an infinity of possible dumb mistakes and amazing new ones are made all the time. Griffin emphasizes the need for trust and communication that are characteristic of high reliability organizations.

B. Normal Accident Theory

Charles Perrow developed Normal Accident Theory after the Three Mile Island nuclear accident. The interactive complexity and tight coupling between subsystems, such as found in nuclear power plants, leads to unpredictable interactions. This means that accidents are inevitable and can be considered "normal." Because there is not enough time and understanding to control minor incidents and small failures, they can spread to disrupt entire system. Because failures are very damaging, trial-and-error learning can not be used to gain knowledge of the system. Organizational complexity and bureaucratic routine compound the problem. (Perrow, 1984) Normal Accident Theory "asserts that the perfect operation of complex and dangerous technology is beyond the capacity of humans, given their inherent imperfections and the predominance of trial-and-error learning in nearly all human undertakings." (Boin and Schulman, 2008) "Organizations that aspire to failure-free performance are inevitably doomed to fail because of the inherent risks in the technology they operate." (CAIB, 2003, p. 180) The Apollo 13 failure was due to a complex chain of events of the kind emphasized in Normal Accident Theory. The fact that the last three Apollo flights were cancelled and shuttle program terminated suggest that the possibility of a fatal accident can affect mission decisions.

C. High Reliability Theory

In a rebuttal to the pessimism of Perrow's Normal Accident Theory, other researchers developed High Reliability Theory, the concept that some organizations can operate dangerous technical systems with reliability and safety far beyond anything that can reasonably be expected. Examples include nuclear submarines, air traffic

control, and aircraft carriers. The High Reliability Theory researchers claim that high reliability organizations can be developed by implementing the appropriate structure, behaviors, and attitudes.

A high reliability organization is dedicated to ensure that failures will never happen, that they will be prevented by sparing no effort or cost. All threats to safety, even minor anomalies, glitches, and off-nominal sensor indications, are immediately given top priority and dealt with. All design and operations decisions are considered primarily based on their impact on safety. (Boin and Schulman, 2008) High-reliability organizations typically have one single clear purpose, extreme hierarchy, high accountability, tight coupling, multiply redundant data and control paths, problem searching, rapid feedback, and continuous learning. (Casler, 2014)

It has been argued that NASA is not and can never be a high reliability organization. NASA is a public agency in a difficult political environment and has multiple conflicting goals, and so it simply cannot afford to prioritize safety over all other objectives. (Boin and Schulman, 2008) (Casler, 2014) But McCurdy argues the contrary, "Perrow's theory predicts that humans should not be able to create nearly error-free institutions managing risky technologies in natural surroundings. The existence of such institutions, including NASA during its moon landing years, contradicts the theory." (McCurdy, 2001) The success of the Apollo program illustrates the possibility, and the difficulty, of achieving a high reliability organization.

D. Bad luck

Future events are uncertain and unpredictable, so they seem subject to chance. Past events are clear and obvious, so they seem necessary and inevitable. The same events are viewed as unpredictable before they occur and inevitable after. Future mission planners can usually accept that all risks cannot be identified and eliminated. Mission failure investigators almost always identify convincing failure causes.

Some risk must be accepted. This means that failures will occur with some probability. What failures occur, where and when, then seems a matter of chance. Nevertheless, the specific failure causes can usually be identified in hindsight. "Risks are always deemed acceptable until they change from a "risk" to a "failure mode"." (Paxton, 2007)

As it was argued in justifying faster, better, cheaper, it is possible to treat risk as a resource that can be traded off against cost or performance. Supporters still claim that the many faster, better, cheaper missions were much more cost effective than the previous few high cost, high reliability flagship missions. The mission failures should be considered the cost of doing business in a less expensive, more efficient way. However, the final consensus is that the six in sixteen actual failure rate of the faster, better, cheaper missions showed that the risk was unacceptable.

Decision making under conditions of risk can be a pure mathematical calculation, if the payoffs and probabilities are known. The bettor computes the odds, places a bet, rolls the dice, and wins or looses. A good bet is simply one the bettor would make again because the odds indicate he or she should come out ahead in the long term. A good decision is justified by the facts known before it was made, not by the result determined by chance afterward.

Small deterministic gambles are simple mathematical problems, but high risk decisions with unknown odds depend on the decision maker's risk tolerance. NASA missions are highly visible and unique. The impact of a failure is high, far beyond the loss of the money invested. This makes NASA very risk adverse. It seems that failures cannot be accepted as a reasonable cost of doing business, as due to bad luck following a decision to accept some degree of risk.

What would it take to prove that a NASA mission failure was due to bad luck? Suppose some acceptable probability of failure was decided on and the failures actually occurred at that rate. Then the failures would clearly be expected and occur due to random bad luck, even though any particular failure would have some particular cause. The faster, better, cheaper mission failures were attributed to the faster, better, cheaper approach, but also to general causes, the culture, and specific blunders. However, given that faster, better, cheaper deliberately deemphasized reliability and accepted higher risk to increase the number and pace of missions, the high mission failure rate can be treated as a predictable cost of the approach. The actual failures should be attributed to expected random bad luck as much as to specific causes.

IV. Conclusion

Safety and reliability received strong emphasis in early days when frequent critical rocket failures occurred, and also after the Apollo 1 disaster occurred. At other times such as the "better, faster, cheaper" era, reliability has been deemphasized because of the cost and time required to implement it and because of its essentially conservative and even negative view of programs. If large long term projects have their actual flights many years or even decades away, the decision makers who cut reliability efforts now will be long gone if the program's luck runs out. Failures and accidents produce resolutions to reform, to reestablish a strong safety and reliability function, but the need for higher reliability is more easily acknowledged than implemented. The actual effort to improve reliability is easily

deferred to the future. This is wrong. Reliability is a fundamental intrinsic property of system architecture and subsystem technology that must be considered from the beginning of design.

NASA's variable support of safety and reliability is partly justified by the different priorities and risks of its different missions. The emphasis on reliability is subject to systems engineering trade-offs, but budget and delivery pressures can divert attention from attention the actual high cost of failure. Variable emphasis on reliability is justified but the right stress is necessary.

No one theory can fully explain the success or failure of high technology space efforts. Mistakes, system complexity, and risk taken with bad luck all cause failures. If we choose challenging space exploration goals with their unavoidable risks, we must build high reliability organizations and develop dedicated people to staff them.

NASA's Apollo program exemplified a high reliability organization. Safety is a key priority. Open discussion, debate, and even dissent are encouraged. Potential problems and undiscovered errors are sought out and escalated until solved. Minority opinions and worst case scenarios are deliberately developed. Independent review groups and multiple information flows are carefully established.

Most NASA programs fall short of this ideal. People naturally strongly dislike having their assumptions questioned or being reminded of potential problems such as accidents and failures. The typical project always insists that everything is under control, all is well. Organizations easily lapse into a fantasy world that denies the real world threats to safety and reliability. But "nature cannot be fooled."

References

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

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

CAIB, Columbia Accident Investigation Board, Vol. I, August 2003.

Casler, J. G., "Revisiting NASA as a High Reliability Organization," Public Organization Review 14:229–244, 2014.

Coutinho, J. de S., "Wither Reliability," AIAA Paper 1964-249, AIAA 1st Annual Meeting, Washington, DC, 1964.

Cowing, K., NASA Responds to the Columbia Accident Report: Farewell to Faster - Better – Cheaper, Space Ref, September 15, 2003, http://www.spaceref.com/news/viewnews.html?id=864, accessed Jan. 16, 2015.

Denson, W., "The History of Reliability Prediction," IEEE Transactions on Reliability, vol. 47, no. 3-SP, pp. 321-8, September, 1998.

Fragola, J. R., "Reliability and risk analysis database development: an historical perspective," Reliability Engineering and System Safety 51 pp. 125-136, 1996.

Fragola, J. R., and McFadden, R. H., "External maintenance rate prediction and design concepts for high reliability and availability on space station Freedom," Reliability Engineering and System Safety, 49, pp. 255 -273, 1995.

Green, J., and Spexarth, G., "A Mars-Forward Approach to Lunar Supportability Planning" AIAA-2009-6427, AIAA SPACE 2009 Conference & Exposition, Pasadena, California, 14 - 17 September 2009.

Green, J., and Watson, J. K., "Supportability and Operability Planning for Lunar Missions," AIAA 2008-7779, San Diego, California, 9 - 11 September 2008.

Griffin, M. D., "Message from the Administrator Day of Remembrance," Jan. 28, 2008, http://www.spaceref.com/news/viewsr.html?pid=26844, accessed Jan. 21, 2015.

Hall, J. L., "Columbia and Challenger: organizational failure at NASA," Space Policy 19 239–247, 2003.

Jackson, A., and Das, R., "Finding Answers to Space Industry's Top 10 Reliability Problems, Proceedings of the Annual Reliability and Maintainability symposium (RAMS), 2001.

Jones, H., "Diverse Redundant Systems for Reliable Space Life Support," submitted ICES 2015-047, 45th International Conference on Environmental Systems, 2015.

Jones, H., "Life Support Dependability for Long Space Missions," AIAA 2010-6287, 40th ICES (International Conference on Environmental Systems), 2010.

Lalli, V. R., "Space-System Reliability: A Historical Perspective," IEEE Transactions on Reliability, vol. 47, no. 3-SP, pp. 355-9, September, 1998.

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

MCO MIB, Mars Climate Orbiter Mishap Investigation Board, Report on Project Management in NASA, March 13, 2000. ftp://ftp.hq.nasa.gov/pub/pao/reports/2000/MCO_MIB_Report.pdf

Mulqueen, J., Griffin, B., Smitherman, D., and Maples, D., "Benefits of Using a Mars Forward Strategy for Lunar Surface Systems," AIAA 2009-6683, AIAA SPACE 2009 Conference & Exposition, Pasadena, California, 14 - 17 September 2009.

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

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.

Paxton, L. J., " 'Faster, better, and cheaper' at NASA: Lessons learned in managing and accepting risk," Acta Astronautica 61, pp. 954 – 963, 2007.

Perrow, C., *Normal Accidents: Living with High-Risk Technologies*, New York: Basic Books, 1984.

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

Russell, J. F. and Klaus, D. M., "Maintenance, Reliability and Policies for Orbital Space Station Life Support Systems," Reliability Engineering and System Safety, Vol. 92, No. 6, pp. 808-820, 2006.

Vaughan,, D., *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*, University of Chicago, 1996.

Verma, A. K., Ajit, S., and Karanki, D. R., *Reliability and Safety Engineering*, Springer, London, 2010.

Ward, D, "Faster, Better, Cheaper Revisited: Program Management Lessons from NASA," Defense AT&L: March-April 2010.

Ward, D, "Faster, Better, Cheaper: Why Not Pick All Three?" National Defense, April 2012. http://www.nationaldefensemagazine.org/archive/2012/April/Pages/Faster,Better,CheaperWhyNotPickAllThree.aspx, accessed Jan 16, 2015.

Wikipedia, Robert Lusser, http://en.wikipedia.org/wiki/Robert_Lusser, accessed Jan.15, 2015.