

A Silent Safety Program

Ronnie Goodin, CSP; NASA, Kennedy Space Center; Florida

Keywords: safety, critical review

Abstract

NASA's Columbia Accident Investigation Board (CAIB) referred 8 times to the NASA "Silent Safety Program." This term, "Silent Safety Program" was not an original observation but first appeared in the Rogers Commission's Investigation of the Challenger Mishap. The CAIB on page 183 of its report in the paragraph titled 'Encouraging Minority Opinion,' stated "The Naval Reactor Program encourages minority opinions and "bad news." Leaders continually emphasize that when no minority opinions are present, the responsibility for a thorough and critical examination falls to management. . . Board interviews revealed that it is difficult for minority and dissenting opinions to percolate up through the agency's hierarchy . . ." The first question and perhaps the only question is - what is a silent safety program? Well, a silent safety program may be the same as the dog that didn't bark in Sherlock Holmes' "Adventure of the Silver Blaze" because system safety should behave as a devil's advocate for the program barking on every occasion to insure a critical review inclusion. This paper evaluates the NASA safety program and provides suggestions to prevent the recurrence of the silent safety program alluded to in the Challenger Mishap Investigation. Specifically targeted in the CAIB report, "The checks and balances the safety system was meant to provide were not working." A silent system safety program is not unique to NASA but could emerge in any and every organization.

Principles developed by Irving Janis in his book, Groupthink, listed criteria used to evaluate an organization's cultural attributes that allows a silent safety program to evolve. If evidence validates Janis's criteria, then Janis's recommendations for preventing groupthink can also be used to improve a critical evaluation and thus prevent the development of a silent safety program.

Organization of this Analysis

The CAIB criticized NASA's safety program characterizing it as a "silent safety program" implying a loss of a critical evaluation during design evaluation or decision reviews. Irving Janis in his book, "Groupthink," discusses impact of loss of critical evaluation in historical case studies presented in the next (1st) section. The purpose of this historical path is to establish theory developed by Janis as the cornerstone of the analysis presented in the second section followed by a section listing recommendations to insure critical review thus thwarting both groupthink and a silent safety program. The fourth section summarizes the analyses and recommendations. The final two sections identify a baseline to compare the NASA safety program and personnel experience of the author introducing additional points to reinforce observations.

History

Failures of organizations to properly engage critical thinking often result in significant mistakes in decision or judgment by an individual or an organization. A symptom of loss of critical evaluation is a silent safety program which is one that does not bark. The study and lessons in this section demonstrate that no organization is exempt from making poor decisions. These historical mistakes are indirectly related to NASA implying that all organizations including NASA are not exempt from making poor decisions and set the stage for the upcoming analysis.

The system safety engineer works in failure space while as the design engineer works in success space. This logic or reverse way of thinking is a primary contribution of the system safety engineer for increasing the robustness of the design. Historical examples where decision illogic was evident follow an interesting pattern that can be related to critical evaluation offered to the project by system safety engineers: Early in his administration, John F. Kennedy led discussion with a predetermined end in mind thus discouraging critical points of view or critical evaluation that led to the "Bay of Pigs" disaster universally known as a perfect failure. But President Kennedy learned a lesson and later invited or demanded all opinions resulting in a great success a year and a half later with the Cuban Missile Crisis. "Kennedy was no longer so naive about seemingly authoritative military briefings or so insensitive to the

dangers of oversimplifying foreign-policy issues. . . Important procedural changes had been introduced into the organized policy-making process – changes calculated to prevent the policy-makers from accepting uncritically glib arguments put forth by enthusiastic proponents of an ill-conceived plan.” The Cuban Missile Crisis’ logic is consistent with the logic of the system safety/design engineer success space – failure space thought process producing a more resilient design.

The Space Shuttle processing contractor, United Space Alliance (USA) initiated an internal audit program with an assigned role of a Devil’s Advocate which is also the role of the system safety engineer. The advantage of designating a Devil’s Advocate is that everyone recognizes it as a role and thus depersonalizes the questions and challenges from this position. After the Bay of Pigs fiasco, Kennedy instituted 2 devils advocates during the Cuban Missile Crisis: Robert Kennedy and Theodore Sorensen, neither being present in the Bay of Pigs planning sessions.

Regarding one group’s work in developing the Marshall Plan under President Truman: “They took very seriously their role as critical thinkers, not sparing each other the embarrassments and humiliation of having to listen to a pet idea being subjected to incisive criticism and sometimes hacked to pieces.” Kennan stated in his Memoirs, “So earnest and intent were the debates in our little body in those hairy days and nights that I can recall one occasion, in late evening, when I, to recover my composure, left the room and walked, weeping, around the entire building.” “Apparently a similar norm of open critical scrutiny took hold in Kennan’s policy-planning group. Adherence to this norm requires a delicate balance of mutual suspicion and mutual trust-suspicion about the soundness of each other’s arguments, combined with a basic attitude of trust that criticizing each other’s ideas will not be taken as an insult or lead to retaliation.”

The best documentation example for dissent resides in the United States legal system. The United States court system documents the dissenting comments of a judge who disagrees with the majority opinion. The legal system recognizes the importance of dissenting comments when decisions are challenged during future legal action. A valuable attribute of documenting dissenting comments in system safety management is that a more complete picture of the situation is recognized and recorded, and like the legal world, as the environment changes, design retrofit options are more easily evaluated when a complete package is available from system genesis.

Janis provides the above examples along with other examples of poor decision resulting from minimum critical evaluation in his book, Groupthink: Pearl Harbor, Johnson’s escalation of the Vietnam War, Truman’s escalation of the Korean conflict, and Watergate.

Analysis (Janis)

Assumptions:

- (1) A system safety engineer, by training and experience working in failure space thus becomes (or should become) a critical evaluator for the Program.
- (2) Psychological assessment and theory presented by Janis in Groupthink for prevention of groupthink can be reduced to loss of critical evaluation in decision making. And loss of critical thinking behavior by a Program’s system safety engineers results in a silent safety program.

The CAIB provided more than adequate evidence of the existence of a silent safety program within NASA prior to the Columbia accident in Chapter 7 of the CAIB report. The purpose of this analysis is not to validate the CAIB statements regarding NASA’s silent safety program. Janis listed the organizational preexisting conditions embedded within its culture that could lead to group oriented mistakes by a seemingly cohesive team. The assessment below is based on these pre-existing conditions postulated by Janis compared with evidence documented in the CAIB report to determine NASA’s cultural inclination to make team generated poor decisions resulting from minimum critical evaluation during the decision making process. If adequate CAIB evidence is available to validate Janis’ organizational pre-existing conditions, and assumption 2 is valid, then a safety engineer may use Janis’ recommendations listed in the next section to avert a silent safety program.

Janis’ Organizational Antecedent Conditions:

The Organizational Antecedent Conditions are organized into groupings:

A. Structural Faults of the Organization

1. Have the decision groups been insulated in any way?

Evidence: "The current Shuttle program culture is too insular (CAIB Page 187)."

Evidence: "At the time of the launch of STS-107, NASA retained too many negative (and also many positive) aspects of its traditional culture: flawed decision making, self deception, introversion and a diminished curiosity about the world outside the perfect place (CAIB page 118)."

2. Has there been a lack of tradition of impartial leadership?

Evidence: "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 Page 9)."

Evidence: "Another Deming principle was that checks and balances in an organization were unnecessary and sometimes counterproductive, and those carrying out the work should bear primary responsibility for its quality. It is arguable whether these business principles can readily be applied to a government agency operating under civil service rules and in a politicized environment. Nevertheless, Goldin sought to implement them throughout his tenure (CAIB Page 105-106)."

Evidence: "Shuttle managers did not embrace safety-conscious attitudes. Instead, their attitudes were shaped and reinforced by an organization that, in this instance, was incapable of stepping back and gauging its biases. Bureaucracy and process trumped thoroughness and reason (CAIB page 181)."

3. Are there a lack of norms requiring methodical procedures?

Evidence: "In our view, the NASA organizational culture had as much to do with this accident as the foam (CAIB Page 97)."

Evidence: "By the eve of the Columbia accident, institutional practices that were in effect at the time of the Challenger accident – such as inadequate concern over deviations from expected performance, a silent safety program, and schedule pressure – had returned to NASA (CAIB Page 101)."

Evidence: "The Board concludes that NASA's current organization does not provide effective checks and balances, does not have an independent safety program, and has not demonstrated the characteristics of a learning organization (CAIB Page 12)."

4. Is there homogeneity of members' social background and ideology?

Evidence: "The current Shuttle program culture is too insular (CAIB Page 187)."

B. Provocative Situational Context

1. Is there high stress from external threats with low hope of a better solution than the Leader's?

Evidence: "In the course of selling the Space Shuttle Program within these budget limitations, and therefore guaranteeing itself a viable post-Apollo future, NASA made bold claims about the expected savings to be derived from revolutionary technologies not yet developed (CAIB Page 22)."

Evidence: {1991} "This move was in reaction to a perception that the agency had overreacted to the Rogers Commission recommendations – for example, the notion that the many layers of safety inspections involved in preparing a Shuttle for flight had created a bloated and costly safety program (CAIB Page 107)."

Evidence: Quoting the 1995 Kraft Report, "NASA should "restructure and reduce the overall Safety, Reliability, and Quality Assurance elements – without reducing safety" (CAIB Page 108)."

Evidence: "As more employees have departed, the workload and stress [on those] remaining have increased, with a corresponding increase in the potential for impacts to operational capacity and safety (CAIB Page 110)."

Evidence: At times, the pressure to meet the flight schedule appeared to cut short engineering efforts to resolve the foam-shedding problem (CAIB page 130)."

Evidence: ". . . it became apparent that the complexity and political mandates surrounding the International Space Station Program, as well as Shuttle Program management's responses to them, resulted in pressure to meet an increasingly ambitious launch schedule (CAIB page 131)."

Evidence: "The Space Station Program and NASA were on probation, and had to prove they could meet schedules and budgets (CAIB page 131)".

Evidence: "Shuttle and Station managers worked diligently to meet the schedule. Any necessary change they made on one mission was now impacting future launch dates. They had a sense of being under the gun (CAIB page 134)."

Evidence: "After STS-107, the tempo was only going to increase. The vehicle processing schedules, training schedules, and mission control flight staffing assignments were all overburdened (CAIB page 135)."

Evidence: "Program managers estimated that Node 2 launch would be one to two months late. They were slowly accepting additional risk in trying to meet a schedule that probably could not be met (CAIB page 138)."

Evidence: "No one at NASA wants to be the one to stand up and say, "We can't make that date." (CAIB page 138)"

Evidence: "Little by little, NASA was accepting more and more risk in order to stay on schedule (CAIB page 139)."

Evidence: Finding "F6.3-15 There were lapses in leadership and communication that made it difficult for engineers to raise concerns or understand decisions (CAIB page 171)."

Evidence: ". . . the Shuttle Program's *ability to manage risk was being eroded* "by the desire to reduce costs (CAIB page 179);"

2. Is there low self esteem temporarily induced by:
 - a. Recent failures that make members' inadequacies salient
 - b. Excessive difficulties on current decision-making tasks that lower each member's self-efficacy.

Evidence: "As the investigation [Rogers Commission] continued, it revealed a NASA culture that had gradually begun to accept escalating risk, and a NASA safety program that was largely silent and ineffective (CAIB Page 25)."

c. Moral dilemmas: Apparent lack of feasible alternatives except ones that violate ethical standards

Evidence: "More troubling, the pressure of maintaining the flight schedule created a management atmosphere that increasingly accepted less-than-specification performance of various components and systems, on the grounds that such deviations had not interfered with the success of previous flights (CAIB Page 24)."

Evidence: "In the aftermath of the Challenger accident, these contradictory forces prompted a resistance to externally imposed changes and an attempt to maintain the internal belief that NASA was still a "perfect place," alone in its ability to execute a program of human space flight. Within NASA centers, as Human Space Flight Program managers strove to maintain their view of the organization, they lost their ability to accept criticism, leading them to reject the recommendations of many boards and blue-ribbon panels, the Rogers Commission among them. External criticism and doubt, rather than spurring NASA to change for the better, instead reinforced the will to "impose the part line vision on the environment, not to reconsider it," according to one authority on organizational behavior (CAIB Page 102)."

Summary of Janis' antecedent conditions: The evidence produced by the CAIB confirms that cultural or organizational conditions existed in NASA that led NASA to make decisions without adequate critical evaluation thus resulting in an apparent silent safety program.

Recommendations to Improve Critical Decision Making or Prevent a Silent Safety Program

The current NASA process for project management [Risk Management – NPG 7120.5] possesses boundless potential for contribution to our knowledge management system. By its very nature, each risk has to be fully documented with an evaluation of the risk's relative quantitative value along with management or design options and a range of consequences for both the baseline and each option, thus offering direct countermeasures to the seven indicators of poor decision making acknowledged by Janis.

The analysis section listed Janis' preexisting organizational tendencies leading to groupthink or loss of critical evaluation. Evidence from the CAIB report indicates NASA's loss of critical evaluation (a silent safety program). Therefore Janis' nine recommendations listed below offer countermeasures to prevent loss of critical evaluation:

- "1. The leader of a policy-forming group might assign the role of critical evaluator to each member, encouraging everyone to give high priority to airing his objection and doubts openly. This practice may need to be reinforced by the leader's acceptance of criticism of his own judgments in order to discourage the members from soft-pedaling their disagreements.
2. The key leaders in an organization's hierarchy, when assigning a policy-planning mission to any group within their organization, might adopt an impartial stance instead of stating preferences and expectations at the outset. This practice requires each leader to limit his briefings to unbiased statements about the scope of the problem and the limitations of available resources, without advocating any specific proposal he would like to see adopted, so as to allow the conferees to develop an atmosphere of open inquiry and explore impartially a wide range of policy alternatives.
3. The organization might routinely follow the administrative practice of setting up several independent policy-planning and evaluation groups to work on the same policy question, each carrying out its deliberations under a different leader. This would prevent the appraisal of policy alternatives from remaining in the hands of one insulated group, a prime condition that fosters miscalculations based on concurrence-seeking tendencies.

4. Throughout the period when the feasibility and effectiveness of policy alternatives are being surveyed, the policy-making group should from time to time divide into two or more subgroups to meet separately, under different chairpersons, and then come together to hammer out their differences.
5. Each member of the policy-making group should discuss periodically the group's deliberations with trusted associates in his or her own unit of the organization and report back their reactions.
6. One or more outside experts or qualified colleagues within the organization who are not core members of the policy-making group should be invited to each meeting on a staggered basis and should be encouraged to challenge the views of the core members.
7. At every meeting devoted to evaluating policy alternatives, at least one member should be assigned the role of devil's advocate.
8. Whenever the policy issue involves relations with a rival nation or organization, a sizable block of time (perhaps an entire session) should be spent surveying all warning signals from the rivals and constructing alternative scenarios of the rivals' intentions.
9. After reaching a preliminary consensus about what seems to be the best policy alternative, the policy-making group should hold a 'second chance' meeting at which the members are expected to express as vividly as they can all their residual doubts and to rethink the entire issue before making a definitive choice."

Analysis Summary

The criteria developed by Janis to evaluate organization tendencies toward groupthink or loss of critical evaluation combined with the evidence from the CAIB report suggest an internal cultural basis that led to NASA's "silent safety program."

Irving Janis lists the following defects in group decision-making under what he calls "groupthink" that refers to a deterioration of mental efficiency, reality testing, and moral judgment that results from in-group pressures." He lists ". . . seven major defects in decision-making contribute to failures to solve problems adequately." These seven defects are listed for information only. This analysis did not seek out evidence regarding these defects because the CAIB addressed the Columbia mishap causes whereas the scope of this analysis' is evaluation of the NASA culture seeking the origins of a "silent safety program" and to suggest countermeasures.

- First, the group's discussions are limited to a few alternative courses of action (often only 2) without a survey of the full range of alternatives.
- Second, the group does not survey the objectives to be fulfilled and the values implicated by the choice.
- Third, the group fails to reexamine the course of action initially preferred by the majority of members from the standpoint of non-obvious risks and drawbacks that had not been considered when it was originally evaluated.
- Fourth, the members neglect courses of action initially evaluated as unsatisfactory by the majority of the group.
- Fifth, the members make little or no attempt to obtain information from experts who can supply sound estimates of losses and gains to be expected from alternative courses of action.
- Sixth, selective bias is shown in the way the group reacts to factual information and relevant judgments from experts, the mass media, and outside critics.

- Seventh, the members spend little time deliberating about how the chosen policy might be hindered by bureaucratic inertia, sabotaged by political opponents, or temporarily derailed by the common accidents that happen to the best of well laid plans.”

Baseline

The Department of the Army’s safety program in its Major Command, Army Material Command (AMC), is used as a baseline to compare with NASA’s safety program. The scope of this evaluation is limited to a system safety program which is that arm of safety committed to the design and operation of systems or hardware. Two system safety engineering attributes are listed: Critical evaluation, and dissent. However, these two attributes represent somewhat of a marriage and are yoked together – one exits not without the other, and if one suffers, both suffer.

The Army Material Command (AMC) laid the groundwork for its system safety program in 1969 when it opened an engineering training center providing specialized training at the graduate level to recent college engineering graduates in fields not sponsored by university engineering schools. System safety engineering was one of the four fields of special study. Texas A&M University co-developed and sponsored this program with the Army. Two years of specialized training was provided before these young engineers were given their first assignment. Army personnel designated a unique series “803” for these safety engineers. This 803 series was extremely difficult to enter. During the career development of the system safety engineers, they were constantly exposed to and working in failure space and thus became *critical evaluators* by their very nature. Although all these safety engineers did not become a natural critical evaluator, most did as their career matured. From this Army system safety program, system safety engineers were fed throughout the Federal sector and into industry. NASA got a share of system safety engineers from this Army system safety program which one NASA manager described as “the Army mafia.” This paper was reviewed by eight system safety engineer/managers with experience with both NASA and the Army.

Personal Experience

Previous sections dealt with an organization’s cultural attributes that could contribute to decisions that lack critical review. A silent safety program and loss of critical review become interdependent. This section considers traits that may silence the safety engineer at the moment when a critical observation is crucial. Because this paper is written to system safety engineers from a system safety engineering point of view, first person is used to cover this section. Even though I believe critical evaluation typically evolved as an inherent attribute of the system safety engineer, all of us fail sometime during our career. I fail and hate myself when it happens because I owe more to the project office and more to myself. The challenge is to minimize the number and impact of these failures through cross communication taking heart from one another’s’ failings to fortify ourselves so each of us can stand alone if necessary providing the critical assessment against mounting pressure to fall in line. My first failure happened early during my career at my first assignment with the Army Aviation Command which covered 1977-1980, over 25 years ago and I recall it as if it were yesterday. The CH-47, a mid-size cargo helicopter with 2 sets of rotor blades, experienced a series of failures where the rear cargo door fell off the aircraft during flight. Army and contractor engineers worked frantically to generate fix after fix as the aircraft lost more than 40 rear cargo doors. None of these earlier mishaps resulted in propagation of the damage beyond the door simply falling off. But the last failed door got caught in the rotor wash and was pulled up into the blades. Risk creep is the single predictable failing. NASA even has a name for repeated acceptance of a waived requirement – “In family.” Well, luckily no one suffered injuries as I recall. But I was on the team, the system safety engineer whose purpose was to offer a critical review and I failed to do so. The Challenger Launch Decision by Diane Vaughn, laid out the baby steps where small compromise after small compromise was made until the dreadful day where the Challenger was lost due to engineering judgment and decision. I believe, had I been that system safety engineer assigned to Shuttle Solid Rocket Motors, I likely would have concurred with each of these seeming small steps, and furthermore, I believe many of the safety engineers with whom I have worked in research and development would have approved each of these design decisions as well. It is because of events such as Challenger, that system safety engineers need to weigh into these decisions to keep the critical evaluation alive and well for both the safety engineer and the design team.

One good example of critical evaluation of a safety engineer/manager was during a Shuttle launch. The Kennedy Space Center Safety representative responsible for safety input during the launch countdown process, standing alone, held up the launch during resolution of a safety issue until all risks were understood and clearly stated and

accepted. Unimaginable pressure was put on this safety manager from a huge and costly launch team as the entire team is suggesting solutions and ideas to keep the launch process moving along. That one safety manager who withstood this pressure was a career system safety engineer/manager who was the first NASA employee to be sent to and graduated from the Army system safety training school. This type of critical evaluation is what system safety engineers contribute. Lack of evidence of this type of critical evaluation led the CAIB to the following conclusion, "The Naval Reactor Program encourages minority opinions and bad news. Leaders continually emphasize that when no minority opinions are present, the responsibility for a thorough and critical examination falls to management. Alternate perspectives and critical questions are always encouraged. In practice, NASA does not appear to embrace these attitudes (CAIB Page 183)."

Conclusion

NASA's present Administrator, Mike Griffin, identified the Agency's approach to correct the shortcomings identified by the CAIB, "Many have said that the PM should "own" the technical requirements for safe and reliable operations. That was the case with Challenger and Columbia. NASA is expected to change that." The new NASA approach, "The independent Safety and Mission Assurance (SMA) group assures compliance with the safe operations requirements controlled by the Technical Authority. At NASA, as prerequisites to flight, the Technical Authority certifies that the established requirements will support safe operations. The PM certifies that the requirements for safe flight have been met. SMA certifies that the PM has complied with the requirements. These three independent inputs give the Administrator the confidence that everyone has properly exercised Authority, Responsibility and Accountability (AR&A)". Mike Griffin further clarified the S&MA role, "Nowhere (in my experience) does Engineering "delegate" the "make it safe" responsibility to SMA." This clarification of all roles assures or demands that the SMA voice be no longer silent.

The ultimate goal of this paper is to warn the safety engineer of the danger of loss of critical evaluation using the example of NASA's Columbia mishap to both validate the evaluation criteria established by Janis and encourage use of Janis' administrative tools to improve an organization's critical review process.

Dissenting Comments or Minority Opinion

No dissenting comments from the eight system safety managers/engineers who reviewed this paper.

References

1. Janis, Irving, *Groupthink*, 2nd edition, Houghton Mifflin Company, 1982, pages 9-10, 14, 139, 141, 166-167, 169-170, and 172.
2. Columbia Accident Investigation Board, Volume 1, August 2003.

Biography

James Ronald (Ronnie) Goodin, CSP., Safety, SAE, Kennedy Space Center, FL 32899, USA, telephone - (321) 861-4131, email - ronald.goodin-1@nasa.gov.

Ronnie Goodin has 31 years of system safety and industrial safety engineering experience with both DOD and NASA.

BS Aerospace Engineering from Mississippi State University
Graduate from the Army DARCOM Safety Intern Center

10 years in system safety with the Department of the Army; time split between the Army Aviation Command and the Army Safety Center

21 years with NASA,
NASA HQ: 1 year
KSC: 20 years