What System Safety Engineering Can Learn from the Columbia Accident

Nancy G. Leveson, Ph.D.; MIT; Cambridge, MA
Joel Cutcher-Gershenfeld, Ph.D.; MIT; Cambridge, MA

Abstract

An accident investigation allows a view into an organization that is normally not possible. The strong system safety program established at NASA after the Apollo fire has evolved into a program in which the name remains but most of the important safety management and engineering functions have disappeared or are performed by contractors. The title remains, but the essence is gone.

Many of the dysfunctionalities in the system safety program at NASA contributing to the Columbia accident can be seen in other groups and industries. This paper summarizes some of the lessons we can all learn from this tragedy. While there were many factors involved in the loss of the Columbia Space Shuttle, this paper concentrates on the role of system safety engineering and what can be learned about effective (and ineffective) safety efforts. The information contained in this paper comes from the Columbia Accident Investigation Board (CAIB) report (ref. 2), the SIAT report (chartered in 1999 to evaluate the Shuttle program after a number of close calls) (ref. 9), the authors' personal experiences with NASA, and communications with current and former NASA system safety engineers.

Introduction

Viewing the Columbia accident from the perspective of system safety, this paper highlights the interdependent roles of culture, context, structure, and process in the accident. While the impact of the foam on the leading edge of the Shuttle wing was the precipitating event in the loss, the state of the NASA safety culture, system safety organizational structure, and safety engineering practices at NASA at the time made an accident almost inevitable. Understanding the political and social background, along with the context in which decisions were made, helps in explaining why bright and experienced engineers made what turned out to be poor decisions and what might be changed to prevent similar accidents in the future.

Background

Some history and background is required before plunging into the analysis. All accidents occur in a social and historical context that is important in understanding the loss. In the case of the Space Shuttle, political and other factors contributed to the adoption of a vulnerable design during the original approval process. In addition, unachievable promises were made with respect to performance in order to keep the manned space flight program alive. The success of the Apollo program and the *can-do* culture that arose during it—marked by tenacity in the face of seemingly impossible challenges—contributed to the belief that the unrealistic performance goals could be achieved if only enough effort were expended.

Budget pressures added to the performance pressures. The Space Shuttle program budget was cut 40% in purchasing power over the past decade. At the same time, the budget was occasionally raided to make up for Space Station overruns. The budget cuts came at a time when the Shuttle was aging and costs were increasing. The infrastructure, much of which dated back to the Apollo era, was falling apart. Uncertainty about how long the Shuttle would fly added to pressures to delay safety upgrades and investment in the Shuttle infrastructure.

Budget cuts without concomitant cuts in goals led to trying to do too much with too little. NASA's response to its budget cuts was to defer upgrades and to attempt to increase productivity and efficiency rather than to eliminate any major programs. By 2001, an experienced observer of the space program described the Shuttle workforce as "The Few, The Tired" (ref. 2).

The unachievable schedule pressures were heaped on top of the budget pressures. One goal for O'Keefe, the new NASA administrator, was to fix the budget problems. NASA was put "on probation." Promises were made that the Space Station would be "core complete" by February 2004. Screensavers were issued that counted down the time to the core complete date, creating a daily reminder of the deadline. Tying the Shuttle to the completion of the Space Station and the need for crew rotation increased the schedule pressures and the urgency of maintaining a predictable launch schedule. Previously, if a Shuttle was not ready to fly, the schedule could be altered and the ordering of flights changed. The need to complete the Station in a certain order, however, eliminated that flexibility. By late summer, 2002, a variety of problems had caused the core complete schedule to slip. Events gradually ate away at the schedule margin, and all slack was gone by December 2002. The belief persisted, among some managers anyway, that the schedule could still be met.

Safety Culture

Much of the CAIB report was devoted to problems in the NASA safety culture. Before examining these problems and their relationship to system safety, it is important to define what is meant by this term. We begin with the concept of "culture."

The most common definition of a culture is a shared set of norms and values. A somewhat different definition defines it as a way of looking at and interpreting the world and events around us (our mental model) and of taking action in a social context. Social anthropology conceives culture as an ongoing, proactive process of reality construction (ref. 10). In this latter conception of culture, organizations are socially constructed realities that rest as much in the heads of members as in sets of rules and regulations. Organizations are sustained by belief systems that emphasize the importance of rationality. Morgan calls this the *myth of rationality* and it helps in understanding why, as in the Columbia accident, it appears that leaders often ignore what seems obvious in retrospect. The myth of rationality ``helps us to see certain patterns of action as legitimate, credible, and normal, and hence to avoid the wrangling and debate that would arise if we were to recognize the basic uncertainty and ambiguity underlying many of our values and actions" (ref. 10).

Linking anthropological and organizational perspectives on culture, Schein (ref. 11) presents a three-tiered model consisting of cultural artifacts that are visible on the surface; a middle level of stated rules, values, and practices; and an often invisible, but pervasive, underlying level of deep cultural assumptions. Culture change is difficult, Schein notes, because it requires change at all three levels and each is progressively harder to address.

Safety culture is the subset of an organizational or industry culture that reflects the general attitude and approaches to safety and risk management. It is important to note that trying to change culture without changing the environment in which it is embedded is doomed to failure. Superficial fixes that do not address the set of shared values and social norms, as well as deeper underlying assumptions, are likely to be undone over time. Perhaps this partially explains why the changes at NASA after the Challenger accident were over time dismantled or became ineffective. Both the Challenger accident report and the CAIB report note that system safety was "silent" and ineffective at NASA. Understanding the pressures and other influences that have twice contributed to a drift toward an ineffective NASA safety culture is important in creating an organizational infrastructure and other cultural factors that will resist pressures against applying good safety engineering practices and procedures in the future.

The safety culture at NASA has changed a great deal over time. In the early days of NASA and during the Apollo era, the belief was prevalent that risk and failure were normal parts of space flight. At the same time, the engineers did everything they could to reduce it (ref. 8). People were expected to speak up if they had concerns, and risks were debated vigorously. "What if" analysis was a critical part of any design and review procedure. Some time between those early days and the Columbia accident, the culture changed drastically. The CAIB report notes that at the time of the Columbia loss "Managers created huge barriers against dissenting opinions by stating preconceived conclusions based on subjective knowledge and experience, rather than solid data." An indication of the prevailing culture can be found in the reluctance of the debris assessment team—created after the launch of Columbia to assess the damage caused by the foam hitting the wing—to adequately express their concerns. Members told the CAIB that "by raising contrary points of view about Shuttle mission safety, they would be singled out for possible ridicule by their peers and managers" (ref. 2).

What about the system safety engineers? Isn't it their role to ensure that concerns are raised? After the Apollo 204 fire in 1967 in which three astronauts died, Jerome Lederer (then head of the Flight Safety Foundation and an early pioneer in system safety) was hired to create a system safety program at NASA. One question is whether system safety was ever fully accepted in the NASA engineering culture. McCurdy notes that the external oversight on

NASA after the fire was resented by many NASA employees (ref. 8). Was the imposition of a system safety program upon the agency also resented and never fully accepted? The Challenger accident report stated that system safety engineers were not part of the decision-making process by the time of the Challenger accident. For example, no system safety engineer participated in the infamous teleconference with the Morton-Thiokol engineers the night before the launch. The same "silence" is noted in the CAIB report, for example, "Safety personnel were present but passive and did not serve as a channel for voicing of concerns or dissenting opinions. Safety representatives attended meetings of the [committees established to consider the foam event] but were merely party to the analysis process and conclusions instead of an independent source of questions and challenges." Either system safety was never fully accepted by NASA engineers or it slid into ineffectiveness over the years.

Context for Decision Making

Decisions are always easy to criticize in hindsight when more information is available as a result of the accident. Psychologists call this common phenomenon *hindsight bias*. To understand why accidents occur, however, it is necessary to evaluate decisions in the context in which they are made, with respect to the information available at the time the decision is made, along with the organizational factors influencing the interpretation of the data and information available.

Some technical factors are important in understanding the decision-making context. There are about 20,000 critical items on the Shuttle, of which 5,396 are tracked. Of these, 4,222 are classified as criticality 1/1R, which means they could lead to the loss of the Shuttle (the "R" means the component is redundant). Waivers are granted when a critical component cannot be redesigned or replaced: 3,222 of the critical items had waivers at the time of the accident. The CAIB report notes that more than 36 percent of these waivers had not been reviewed in ten years. Foam shedding had been occurring for 20 years and was among the thousands of waivers. It had not been ignored, but each fix that had been proposed and tried failed to solve the problem. It is easy to see the foam shedding as critical after the accident, but it is much more difficult before the fact.

As mentioned earlier, the launch pressures were tremendous and were among other things tied to the Space Station and the promise of core complete by February 2004. The schedule pressure created a mindset that dismissed all concerns. This type of culture is often called a c*ulture of denial* where risk assessment is unrealistic and credible risks and warnings are dismissed without appropriate investigation. Managers began to listen only to those who provided confirming evidence that supported what they wanted to hear. For example, during the Columbia flight, the Mission Management Team leaders accepted the conclusion of a thermal tile expert (although not an expert on the reinforced carbon/carbon leading edges of the Shuttle wing) that any potential damage was not a safety issue while dismissing the concerns of the Debris Assessment Team specifically tasked with evaluating the potential damage.

Overconfidence and complacency are common in a culture of denial. The SIAT report in 1999 concluded that the Space Shuttle Program was using previous success as a justification for accepting increased risk. William Readdy in 2001 wrote that "The safety of the Space Shuttle has been dramatically improved by reducing risk by more than a factor of five" (ref. 2). It is difficult to imagine where this number came from as safety upgrades and improvements had been deferred while, at the same time, the infrastructure continued to erode. The unrealistic risk assessment was also reflected in the 1995 Kraft report, which concluded that "the Shuttle is a mature and reliability system, about as safe as today's technology will provide" (ref. 3). A recommendation of the Kraft report was that NASA "should restructure and reduce overall safety, reliability, and quality assurance elements." The CAIB notes a perception that NASA had overreacted to the Rogers Commission recommendations after the Challenger accident, for example, believing that the many layers of safety inspections involved in preparing a Shuttle for flight had created a bloated and costly safety program. The Kraft report dismissed expressed concerns about safety by labeling those who made them as part of an unneeded "safety shield conspiracy." This accusation of a "conspiracy" by those expressing safety concerns is a powerful demonstration of the attitude toward system safety at the time.

Reliance on past success became a substitute for sound engineering practices and for accepting increased risk. Either the decision makers did not have or they did not use inputs from system safety. "Program management made erroneous assumptions about the robustness of a system based on prior success rather than on dependable engineering data and rigorous testing" (ref. 2).

System Safety Organizational Structure

Organizational theorists believe that structure drives behavior. Much of the dysfunctional behavior related to this accident can be traced to an inadequate system safety organizational structure at NASA. For example, the CAIB report notes “confused lines of responsibility, authority, and accountability in a manner that almost defies explanation.” Code Q, the headquarters branch created after the Challenger accident to oversee quality, including safety, was given responsibility and accountability for safety, but never given the authority necessary to execute that responsibility effectively. Another section of the CAIB report notes that “The Shuttle Manager … is responsible for overall Shuttle safety and is supported by a one-person safety staff.” Lower budgets led to cuts in system safety. As a result, system safety at each of the centers was greatly understaffed; at times one system safety engineer supported an entire center.

There are some basic principles important to providing an effective system safety organizational structure (ref. 4):

1. System safety needs a direct link to decision-makers and influence on decision-making (*influence and prestige*);
2. System safety needs *independence* from project management (but not engineering);
3. System safety needs direct communication channels to most parts of the organization (*oversight and communication*).

Influence and Prestige: System safety is organized at most NASA centers as a weak matrix structure (ref. 6). The structure is a “weak matrix” in that there is only a dotted line relationship between system safety and the projects. System safety is managed by the Safety and Mission Assurance or Safety, Reliability and Quality Assurance Office at the center and can then be “purchased” by a project. Important checks and balances do not operate in such a weak matrix structure. More important, the existence of the matrix structure on paper may give a false sense of security, even while the influence and prestige of the activity has deteriorated.

In this case, the placement of system safety in the quality assurance organization, often one of the lower prestige groups in the engineering pecking order, separated it from mainstream engineering and limited its influence on engineering decisions. The CAIB report notes that “We expected to find the [Safety and Mission Assurance] organization deeply engaged at every level of Shuttle management, but that was not the case.” System safety engineers are often stigmatized, ignored, and sometimes actively ostracized. “Safety and mission assurance personnel have been eliminated [and] careers in safety have lost organizational prestige” (ref. 2).

The Rogers Commission report on the Challenger accident observed that the safety program had become “silent” and undervalued. A chapter in the report, titled “The Silent Safety Program,” concludes that a properly staffed, supported, and robust safety organization might well have avoided the communication and organizational problems that influenced the infamous Challenger launch decision. It appears that at the time of the Columbia accident, the same conditions existed, despite the attempts to change them in the aftermath of the Challenger accident. Either the attempts to change the underlying problems had been ineffective or the same or similar conditions had reversed the efforts. The Columbia accident report concludes that, once again, system safety engineers were not involved in the important safety-related decisions. The isolation of system safety from the mainstream design engineers added to the problem. “Structure and process places Shuttle safety programs in the unenviable position of having to choose between rubber-stamping engineering analyses, technical errors, and Shuttle program decisions, or trying to carry the day during a committee meeting in which the other side almost always has more information and analytical ability” (ref.2).

Independence: “NASA does not have a truly independent safety function with the authority to halt the progress of a critical mission element” (ref. 2). In essence, the project manager “purchases” safety from the quality assurance organization. This arrangement raises conflict of interest concerns. “Given that the entire safety and mission assurance organization depends on the Shuttle Program for resources and simultaneously lacks the independent ability to conduct detailed analyses, cost and schedule pressures can easily and unintentionally influence safety deliberations” (ref. 2). The amount of system safety effort applied is limited to what and how much the project manager wants and can afford. “The Program now decides on its own how much safety and engineering oversight it needs” (ref. 2).

The problems are exacerbated by the fact that the Project Manager also has authority over the safety standards applied on the project. NASA safety "standards" are not mandatory. In essence they function more like guidelines than standards. Each program decides what standards are applied and can tailor them in any way they want.

Before the Columbia accident, NASA had no independent safety review mechanism external to the programs, like the Navy WSESRB and other independent review groups. After the accident, NASA established a NASA Engineering and Safety Center (NESC), but it has not yet established any procedures for system safety review of all programs and does not, surprisingly, have system safety engineering as a component of the center.

There are safety review panels and procedures *within* individual NASA programs, including the Shuttle program. Under various types of pressures, including budget and schedule constraints, the independent safety reviews and communication channels within the Shuttle program degraded over time and were taken over by the Shuttle Program office. An example is the SSRP, originally called the Senior Safety Review Panel and currently titled the System Safety Review Panel. The SSRP was established in 1981 to review technical data associated with new hazards and to review the technical rationale for hazard closures. The office of responsibility for this panel was Safety, Reliability and Quality Assurance (SR&QA). The SSRP members and chair were originally from the safety organizations associated with the Shuttle program.

Over time the nature and purview of the SSRP changed. First, the Shuttle Program asked to have some people support the panel on an advisory basis. This evolved after a few years to having program representatives serve on the panel. Eventually, they began to take leadership roles. By 2000, the Office of Responsibility had shifted from SR&QA to the Space Shuttle program office. The representatives from the program elements outnumbered the safety engineers on the panel, the chair had changed from the JSC Safety Manager to a member of the Shuttle Program office (violating a NASA-wide requirement for the chairs of such boards), and limits were placed on the activities of the panel. There was even a proposal (which was not implemented because of the uproar over it) to take away the voting privileges of the safety engineering members of the panel. Basically, what had been created as an independent safety review process had lost its independence and became simply an additional program review panel with added limitations on the things it could review—for example, the reviews were limited to "out-of-family" issues, thus effectively omitting those, like the foam, that were labeled as "in-family".[1]

Oversight and Communication| Many aerospace accidents have occurred after the organization transitioned from oversight to "insight" (ref. 5). The Kraft report in 1995 concluded that given the maturity of the Shuttle, NASA could change to a new mode of management with less NASA oversight. A single contractor (USA) was given responsibility for Shuttle safety (as well as reliability and quality assurance), while NASA was to maintain insight into safety and quality assurance through reviews and metrics. One problem with this division of responsibilities was that it created a conflict of interest between the Program and the contractor goals (ref. 9). In addition, years of workforce reductions and outsourcing had "culled from NASA's workforce the layers of experience and hands-on systems knowledge that once provided a capacity for safety oversight" (ref. 2).

The trend toward bureaucracy and the reliance on contracting required more effective communications and more extensive oversight processes, but these apparently were not present. A report written before the Columbia accident notes a "general failure to communicate requirements and changes across organizations" (ref. 9). The CAIB found that "organizational barriers … prevented effective communication of critical safety information and stifled professional differences of opinion." It was "difficult for minority and dissenting opinions to percolate up through the agency's hierarchy" (ref. 2).

For effective communication of safety information, there must be a culture of openness and honesty where everyone's voice is valued. Employees need to feel they will be supported by management if they raise safety concerns; managers need to display leadership on safety issues and eliminate barriers to dissenting opinions. Apparently, the Shuttle culture did not have these characteristics.

[1] An *in-family* problem, according to a Shuttle program standard (NSTS 08126), is defined as a reportable problem that was previously experienced, analyzed, and understood (or at least thought to be understood).

System Safety Practices

The CAIB report describes system safety engineering at NASA at the time of the Columbia accident as “the vestiges of a once robust safety program.” Some of the changes that had occurred over the years:

- *Reliability engineering was substituted for system safety*. FMEA/CIL became the primary analysis method. Hazard analyses were performed but rarely used. NASA delegated safety oversight to USA, and USA delegated hazard analysis to Boeing. As of 2001, “the Shuttle program no longer required Boeing to conduct integrated hazard analyses.” Instead, Boeing performed analysis only on the failure of individual components and elements and was not required to consider the Shuttle as a whole (ref. 2), i.e., system hazard analysis was not being performed. The CAIB report notes “Since the FMEA/CIL process is designed for bottom-up analysis at the component level, it cannot effectively support the kind of `top-down’ hazard analysis that is needed … to identify potentially harmful interactions between systems.”

- *Standards were watered down and not mandatory* (as noted earlier).

- *The safety information system was ineffective.* Good decision-making about risk is dependent on having appropriate information. Without it, decisions are often made on the basis of past success and unrealistic risk assessment, as was the case for the Shuttle. Lots of data was collected and stored in multiple databases, but there was no convenient way to integrate and use the data for management, engineering, or safety decisions (ref. 1, 2).

- *Inadequate safety analysis was performed when there were deviations from expected performance.* The Shuttle standard for hazard analyses (NSTS 22254), specifies hazards be revisited only when there is a new design or the design is changed: There is no process for updating the hazard analyses when anomalies occur or even for determining whether an anomaly is related to a known hazard.

- *Hazard analysis, when it was performed, was not always adequate.* The CAIB report notes that a “large number of hazards reports contained subjective and qualitative judgments, such as `believed’ and `based on experience from previous flights’ this hazard is an accepted risk.” The hazard report on debris shedding (the proximate event that led to the loss of the Columbia) was closed as an accepted risk and was not updated as a result of the continuing occurrences (ref. 2). The process laid out in NSTS 22254 (“Methodology for Conduct of Space Shuttle Program Hazard Analyses”) allows hazards to be closed when a mitigation is *planned*, not when the mitigation is actually implemented.

- *There was evidence of “cosmetic system safety.”* Cosmetic system safety is characterized by superficial safety efforts and perfunctory bookkeeping; hazard logs may be meticulously kept, with each item supporting and justifying the decisions made by project managers and engineers (ref. 4). The CAIB report notes that “Over time, slowly and unintentionally, independent checks and balances intended to increase safety have been eroded in favor of detailed processes that produce massive amounts of data and unwarranted consensus, but little effective communication” (ref. 2).

Migration toward an Accident

It is common for organizations to migrate to states of heightened risk over time. Clearly, at the time of both the Challenger and Columbia accidents, the Shuttle system safety program was inadequate to prevent a tragedy. “By the eve of the Columbia accident, inadequate concern over deviations from expected performance, a silent safety program, and schedule pressure had returned to NASA” [CAIB]. Understanding enough about these accidents to prevent future ones requires not only determining what was wrong at the time of the losses, but also why the fixes instituted after the Challenger loss became ineffective over time or, perhaps, never were effective. Some were probably doomed from the beginning, such as placing the new safety group at NASA headquarters in the quality organization instead of within engineering and not providing the fledgling organization with the authority necessary to effectively carry out its charge. Other factors arose (or re-arose) over time due to inadequate resolution of the ongoing performance and budget pressures.

Figure 1 shows a simplified system dynamics model of the Columbia loss. The loops in the figure represent feedback control loops where the "+" and "-" on the loops represent polarity or the relationship (positive or negative) between state variables: a positive polarity means that the variables move in the same direction while a negative polarity means that they move in opposite directions. There are three main variables in the model: safety, complacency, and success in meeting launch rate expectations.

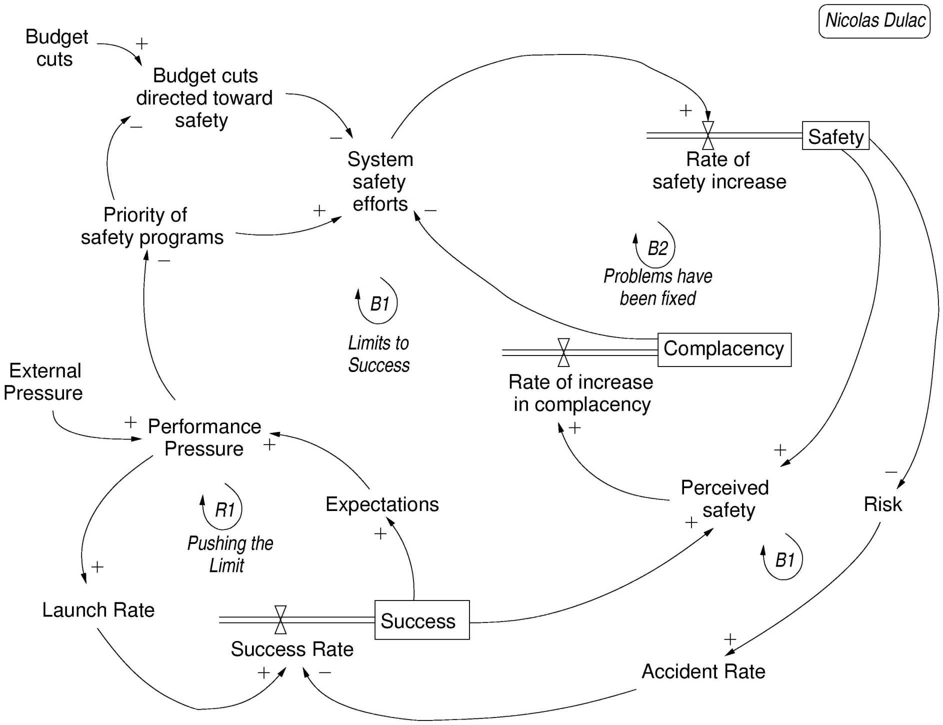

Figure 1 – A Simplified System Dynamics Model of the Columbia Accident[2]

The control loop in the lower left corner of the model, labeled R1 or *Pushing the Limit*, shows how as external pressures increased, performance pressure increased, which led to increased launch rates and thus success in meeting the launch rate expectations, which in turn led to increased expectations and increasing performance pressures. This, of course, is an unstable system and cannot be maintained indefinitely—note that the larger control loop, B1, in which this loop is embedded, is labeled *Limits to Success.* The upper left loop represents part of the safety program loop. The external influences of budget cuts and increasing performance pressures reduced the priority of system safety procedures and led to a decrease in system safety efforts. The combination of this decrease along with loop B2 (*Problems have been fixed*) in which fixing problems increased complacency, which also contributed to the reduction of system safety efforts, eventually led to a situation of (unrecognized) high risk.

One thing not shown in the figure is that these models also can contain delays. While reduction in safety efforts and lower prioritization of safety concerns may lead to accidents, accidents usually do not occur for a while so false confidence is created that the reductions are having no impact on safety. Pressures increase to reduce the safety program efforts and priority even further as the external performance and budget pressures mount.

Complacency is an important variable in the model. Every system safety engineer is well aware of the peculiarity of this field wherein the more successful one is in preventing accidents and incidents, the more others are convinced that the safety engineering efforts were not needed.

[2] Nicolas Dulac, a Ph.D. student at MIT, created this model for the author.

The model shown is not unique to the Columbia accident—it applies equally to the Challenger loss and to many major accidents. One can use such models to hypothesize and evaluate solutions to prevent repetition of the same factors. For example, one way to eliminate the instability in the model shown in Figure 1 is to anchor the safety efforts by, perhaps, implementing externally enforced standards to prevent schedule and budget pressures from leading to reductions in the safety program (ref. 7). Other solutions are also possible. Alternatives can be evaluated for their potential effects using a more complete system dynamics model than shown here. More comprehensive models than shown here also have the potential to act as the proverbial "canary in the coal mine" to identify metrics useful to detect when risk is increasing to unacceptable levels.

Conclusions

Accidents can be viewed through many different lenses. This paper looks at the Shuttle Columbia loss from the point of view of what system safety engineers can, in particular, learn from it and apply to their own organizations. The factors discussed are not unique to NASA alone; many are common in other aerospace and non-aerospace environments. Over the years, system safety engineering at NASA has ceased to play an effective role in the manned space program. Changes are needed to recreate a strong system safety program at NASA. Superficial changes, however, without changing the systemic factors that have led to the program becoming ineffectual over time will not provide long-term safety. Understanding these systemic factors is the first step in fixing them.

Acknowledgements

This research was partially supported by a NASA Ames grant from the Engineering for Complex Systems Program, NAG2-1543. The authors would also like to acknowledge the very helpful discussions by a group of MIT faculty and graduate students about the Columbia accident and the accident report. The group included (alphabetically) Betty Barrett, Alexander Brown, John Carroll, Abe Dane, Nicolas Dulac, Lydia Fraile, Karen Marais, and Sheila Widnall.

References

1. Aerospace Safety Advisory Panel, The Use of Leading Indicators and Safety Information Systems at NASA, NASA Headquarters, March 2003.

2. Harold Gehman (Chair), *Columbia Accident Investigation Report*, August 2003.

3. Christopher Kraft, Report of the Space Shuttle Management Independent Review Team, February 1995, available online at http://www.fas.org/spp/kraft.htm.

4. Nancy Leveson, *Safeware: System Safety and Computers*, Addison-Wesley Publishers, 1995.

5. Nancy Leveson, "The Role of Software in Spacecraft Accidents," *AIAA Journal of Spacecraft and Rockets*, to appear July 2004.

6. Nancy Leveson, Joel Cutcher-Gershenfeld, Betty Barrett, Alexander Brown, John Carroll, Nicolas Dulac, Lydia Fraile, Karen Marais, "Effectively Addressing NASA's Organizational and Safety Culture: Insights from Systems Safety and Engineering Systems," Engineering Systems Symposium, MIT, April 2004.

7. Karen Marais and Nancy Leveson, "Archetypes for Organizational Safety," *2nd Workshop on the Investigation and Reporting of Accidents*, Williamsburg, VA September 2003.

8. Howard McCurdy, *Inside NASA: High Technology and Organizational Change in the U.S. Space Program*, Johns Hopkins University Press, October 1994.

9. Harry McDonald (Chair), Shuttle Independent Assessment Team (SIAT) Report, NASA, February 2000.

10. Gareth Morgan, *Images of Organizations*, Sage Publications, 1986.

11. Edgar Schein, *Organizational Culture and Leadership*, 2^{nd} Ed., Safe Publications, 1986.

12. William Rogers (Chair), The Rogers' Commission Report on the Space Shuttle Challenger Accident,

Biography

Nancy G. Leveson, Ph.D., Professor of Aeronautics and Astronautics and Professor of Engineering Systems, Massachusetts Institute of Technology, Room 33-334, 77 Massachusetts Ave., Cambridge MA 02139, telephone – (617) 258-0505, facsimile – (617) 253-7397, email – leveson@mit.edu, website: http://sunnyday.mit.edu

Joel Cutcher-Gershenfeld, Ph.D., Senior Research Scientist and Executive Director, Engineering Systems Learning Center, Massachusetts Institute of Technology, Room E-40-251, 1 Amherst St., Cambridge MA 02139, telephone – 617-253-5777, facsimile – 617-253-2107, email – joelcg@mit.edu