Observations on the Columbia Accident

Nancy Leveson

April 26, 2003

First, some background so you can evaluate and put my remarks in context. In the past 23 years, I have been involved with safety-critical projects in just about every industry.\(^1\) For example, I helped Ontario Hydro in Canada get the first nuclear power plant digital shutdown system certified and have similarly worked with the NRC in the U.S. and the IAEA (International Atomic Energy Agency) to establish standards for certifying nuclear power plants. I have been involved in some way on almost every attempted air traffic control system upgrade in the U.S. since the mid-1980s. I have been involved in various ways on all types of NASA and DoD (Navy, Air Force, and Army) projects. I even consult with Disney on amusement park ride safety. I have been teaching safety engineering in universities and in industry for two decades. I have been recognized for my activities both by the academic research community and by working engineers. While these remarks are obviously only my own opinions and observations, they are grounded in extensive experience.

With that introduction, let me start by saying that over the years I have never seen anything but the highest commitment to safety at all levels in NASA. The cultural problems at NASA do not include a disregard for safety or the type of complacency that can be described as the “Ford Pinto” attitude that cost-benefit analysis is a reasonable way to decide safety questions, i.e., that deaths are acceptable if the cost of preventing them exceeds the cost of dealing with the consequences. NASA engineers and management are almost obsessive about safety. They are, in addition, among the most dedicated to and excited about their jobs in the world, and I am honored to have the opportunity to interact with them. But as we learned from the ICBM systems in the 1950s (where system safety first arose as an engineering discipline), a commitment to safety is not enough: Achieving high levels of safety requires a planned, disciplined, and systematic approach to identifying, analyzing, and controlling hazards by building safety into the design from the very beginning and continuing to control hazards throughout the entire life cycle of the system. The complexity of the manned space program and other NASA missions is overwhelming and management of safety is critical.

A second observation that I have involves outside “experts” who are not engineers and have never worked on a safety-critical engineering project claiming after a widely publicized accident that certain things that preceded it—particularly heated discussions about the safety of particular aspects of the system—are somehow precursors of accidents in general and reflect negatively on the safety culture of the organization. This is what Dave Woods calls *hindsight bias* and others have referred to as *20/20 hindsight*. It is always easy after the fact to see the full ramifications of a problem or to ascribe special characteristics to what is in reality standard behavior. In virtually all of the safety-critical projects over the last 23 years in which I have been involved, there was continual discussion and disagreement about the safety of many specific aspects of the project. In just the past few months, I have been copied on emails every week (and sometimes every day) between NASA engineers on (unmanned) spacecraft projects strongly arguing detailed engineering decisions about which they feel passionately. Usually they only want my moral support and a

---

\(^1\)I include in the definition of safety-critical not only human death or injury or even physical damage but also loss of critical function or mission.
willing ear or are trying to educate me; occasionally they want me to enter the discussion. In fact, as an expert in safety, I would worry about any project in which this type of disagreement and heated discussion did not occur—and I would immediately sound an alarm that the project was in deep trouble. The problem is not the discussion or that the discussions did not all go up to the highest management levels (which would be impossible given their frequency). The problems arise when there is no organizational structure for illuminating, documenting, and resolving these disagreements in an effective way and no way to evaluate the seriousness of the issues and those that need to be reported.

Accidents happen, particularly when engineers are pushing the limits of complexity and technology and working in an incompletely understood and unforgiving environment such as space. Such engineering projects will never operate in an atmosphere of perfect knowledge and certainty. Risk is an inherent part of space exploration. But that does not mean that we can do nothing to prevent accidents or that we cannot and should not learn from our tragedies about how to reduce risk in the future.

So what are some of the lessons from Columbia? There are obviously many, so let me confine my remarks to those about which I feel most passionately and I rank the highest in terms of importance to preventing future losses.

In the early 1990s, I chaired a two-year study of the Space Shuttle software development processes. In the 1993 final report, I wrote that NASA had established one of the best system safety programs of its time after the Apollo fire in 1968. But nearly two decades later, the Rogers Commission report on the Challenger accident referred to a “Silent Safety Program” that had lost some of its effectiveness. I titled a chapter of my report “The Silent Safety Program Revisited,” and noted that many of the same symptoms were apparent in 1993.

Given my experiences since that time, including two years of reviewing the NASA manned space flight program as a consultant to ASAP, I have concluded that the NASA system safety program is no longer just silent but has effectively disappeared and exists in name only. That situation is perhaps worse than simply being silent or nonexistent because everyone thinks someone is doing system safety (after all, it’s in the title at each center and at headquarters) and certainly there are isolated efforts and a few bright spots, but a comprehensive effective program no longer exists and has effectively been dismantled over the years. Reliability engineering has been substituted in its place. Unfortunately, while necessary, reliability engineering does not provide safety assurance for systems where accidents often involve complex interactions among components (which may be operating according to specification) and factors beyond simple technical failures, such as uninformed management decision making and inadequate or poorly implemented procedures.

Many of the Shuttle upgrade projects involve software (CLCS, CAU, IVHM) so I have been involved in their review as a member of the ASAP “computer team.” None of these programs have a software safety process in place nor are they implementing the software safety standard (NASA-STD-8719.13). I have been told that most NASA standards are not made mandatory and very few are adopted in full. This seems to contradict the meaning of a standard. CLCS (Checkout and Launch Control System) came closest to implementing a system safety program: After the software was already operational and running the hypergolic maintenance facility, a true system safety effort was started. CLCS was canceled soon after that due to budget and other problems, although there had also been at least one serious safety incident in the few months the system was operational. A CAU (Cockpit Avionics Upgrade) hazard analysis was performed after the design was complete, but what I saw of it was unacceptable. The IVHM (Integrated Vehicle Health Management) project management, when asked about their hazard analysis, simply looked puzzled.

That response was not surprising because the S&MA program at Marshall appeared to have a strong occupational safety element but very limited system safety activities. Other centers also have some remnants of their original system safety programs, but their effectiveness has been reduced
by downsizing, trained people leaving, and project management that does not understand system safety engineering (what it is or why it is needed). I have been told by system safety engineers involved with the Shuttle program for a long time that the system safety organizations right before the Columbia accident and the resources provided were even smaller than before Challenger (when the programs had become “silent”).

I’ve found the practice of after-the-facts safety analyses pervasive at NASA—engineers go through the motions of doing system safety analysis only after the design is complete and it can be of no use to anyone. Many years ago, I was asked to provide input into the process of validating the safety of the ISS software requirements, which had not yet been generated. I learned soon afterward that the software was already at such an advanced stage (it was already running and being distributed to the developers of other ISS components to use in their designs and implementations), that a safety analysis of the requirements (indeed generating requirements at all) would be irrelevant. People involved in system safety at NASA have relayed similar experiences to me with other NASA projects where they finally get totally frustrated and ask themselves “Why are we doing this when the system is already built?”

My company was once given a contract to analyze the safety of a system being designed by NASA for another agency. We tried to speak to the engineers on the project, but they told us they had no intention of cooperating because in their experience, system safety always came in too late in the process and told them the design was unsafe after it was too late to change it. They then had to waste a lot of their time and effort convincing management that the changes could not be made (by arguing they were not necessary). In fact, the time at which we got involved was very early in the project, when a system safety effort could have been effective, but most of the engineers to whom we spoke and their management did not want such an effort. There were a few people on the project who did want our help, but we were effectively stonewalled by management and prevented from getting the information we needed to do the analysis. After two years, we (and the people at another NASA center who were responsible for providing a safety analysis) gave up in total frustration. All the project management really wanted was a nice numerical risk assessment (done by a group that did not bother them in their engineering design efforts) that proved their design was safe, and that is what they finally got. I read in the newspaper much later that the system was delivered and fielded, but had to be immediately taken out of service because of serious safety incidents resulting from its use.

A critical ingredient of a safety program is a set of rigorous standards on how the system safety program will be implemented. These standards must include more than just a hazard analysis or low-level technical activities, but must encompass the entire project engineering and management activities. After getting appointed as a consultant to ASAP, I went to look for the extensive system safety standards that I remembered from the early 1980s. I found that those multi-volume standards have been replaced by one weak 9-page chapter in a general procedures and guidelines document (NPG 8715.3). Most of the techniques recommended were reliability techniques, not safety techniques. There does exist one excellent and relatively new system safety standard for software, spearheaded by a very dedicated and hard working software engineer now at Headquarters Code Q. However, despite the fact that the standard is dated 1997, I can find no evidence it has ever been applied on any of the software upgrade projects for the Shuttle (or on the ISS or any other NASA manned or unmanned project) except in the CLCS project mentioned above, which was cancelled right after the system safety effort began (as usual, late in the project history). Another attempt to create a software safety standard for the manned space program has recently been completed, but is running into opposition.

What happened to the extensive system safety program of Apollo days? I have seen system safety analyses done during the Shuttle design in the 1970s so it still appeared to exist at that time. When during the early 1990s I chaired my review of the Shuttle software maintenance process, I
asked if they used a software hazard analysis (a description of the ways the software could affect the safety of the Shuttle) when they created their continual increments and changes to the on-board software and when they upgraded to new computers. They replied that no such analysis existed. When I told them I had been sent a copy of one TRW had done in the 1970s, they were surprised and asked if I could send it to them. How could such invaluable information for a program that is continually making changes to a safety-critical and very complex system like the Shuttle get lost and forgotten?

The Rogers Commission report noted problems in the system safety program and recommended changes. Why didn’t the fixes put in after Challenger achieve the goal of strengthening system safety? The answer (like that to any complex question) is not simple. NASA employees have told me they attribute the demise of system safety at NASA to such factors as downsizing and reduction of safety personnel along with the assignment of their function to engineers who are not trained in system safety, but that is only a symptom of a problem, not a root cause.

Others have cited lack of management commitment to or even understanding of the functions of a system safety program as well as simply the common discounting of risk and the complacency that results from accepting past success as an assurance of future safety. Safety engineering has the unique handicap that when it is successful, the lack of accidents can be interpreted as an indication that safety engineering was not necessary in the first place. In addition, there is usually a delay between the changes and adaptations in a socio-technical system over time that degrade the safety of the system and the actual manifestation of those changes in a serious loss. In the interim, the changes and degradation continue because it does not appear that safety is decreasing and, in fact, confidence in the system may be increasing at the same time the system is heading toward disaster.

One way to resist complacency and the pressures that work against safety programs is to anchor safety goals to rigorous standards that can make reductions in goals and activities more visible or more difficult to make. But, as discussed above, NASA safety standards were relaxed after Challenger, and they don’t seem to be enforced. Most major accidents result from a slow migration of the organization to a state of high risk. This migration is not usually the result of a specific decision to degrade risk, but simply follows a lot of small decisions, each attempting to fix some current problem.

But the most important factor, in my opinion, is that the changes made to try to fix the problems discovered after Challenger only made them worse. Part of the explanation is that the NASA cultural changes that were necessary to make the programmatic changes effective, did not occur. Over time, the cultural roadblocks (such as the culture of Center autonomy and insularity and the containment of information within the Centers) simply overcame the efforts to implement the recommended changes.

The other part of the answer is that some of the programmatic changes themselves were misguided. By becoming part of an assurance organization, safety became associated with after-the-fact assurance activities rather than the proactive engineering activity to build safety into the design that is required for success.

Code Q was established at Headquarters and assigned responsibility and accountability but no authority, effectively doom them to failure from the start. Experienced system safety engineers from the defense and aerospace industry were hired to run the system safety efforts at Headquarters and to manage the safety efforts at the Centers. They started their jobs with great enthusiasm. By the time I began to interact closely with them in the early 90s, they were frustrated and discouraged and since that time nearly all have left the Agency, with a few retreating to engineering positions at NASA but outside safety. I can find few if any system safety engineers currently working at Code Q today. Expertise in system safety has disappeared.

---

This lack of authority is a complaint I heard from almost everyone in Code Q during my Shuttle software process study, and it was the focus of a recommendation in my 1993 report.
Without authority, those trying to re-establish a strong system safety program could put out edicts about what needed to be done, but the centers balked and did not implement them. Arguments were made that system safety efforts would require outrageous sums and therefore were not practical. The amounts cited were 10 and 20 times the cost of the same programs on equivalent or even larger military systems at the time. Those who had come from those successful defense programs complained that if such game playing had occurred in defense programs at the time, the response would have been “if there is not enough money for the safety program, then we’ll just have to kill the entire project” and such game playing would stop. But at NASA, it was successful in eliminating the system safety activities while keeping the program. System safety became a place to save money. When budget cuts or downsizing occurred, system safety specialists were eliminated and their duties assigned to engineers without the expertise or knowledge to perform them effectively. Reliability engineering techniques, which most engineers are taught in school, were substituted.

Authority was further limited by placing safety in the QA organization, which is traditionally a low status group in engineering. The dedicated group of system safety engineers who manned the new Code Q signed on despite knowing that being in QA would hurt their efforts—they hoped they could overcome the disadvantage. One of the people who led that Headquarters system safety effort complained that he should be reporting to the Chief Engineer, not the manager of QA, but he tried his best to make a difference. He eventually left Code Q after realizing that the organizational structure at NASA made his job impossible. I have spoken to several of the system safety engineers who came to Code Q from outside NASA at that time. All said that after a few years, they had become so discouraged they were ready to accept any assignment just to escape.

Todays systemsafety at NASA has become so stigmatized that ambitious young engineers are reluctant to go into it. I have heard disparaging remarks made about the system safety personnel by engineers and managers at every NASA Center. A former student of mine told me he had been given a promotion to a top management position in the S&MA organization at his Center. He considered it to be a signal that he was not considered good enough to go up in the engineering ranks and that they wanted to promote someone else around him to the more respected engineering position that was opening. His friends suggested that accepting the S&MA position would mean the end of his advancement at NASA. I realize that these are only anecdotes, but there are enough of them to convince me that the environment for doing system safety at NASA is not a healthy one. I contrast it to all my acquaintances who are in system safety in the defense industry and the DoD agencies, most of whom tell me they feel empowered and that they are performing an important and appreciated job.

To summarize, the strong system safety program established by Jerome Lederer in 1968 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. The title remains, but the essence is gone.

So what needs to be done? Perhaps, once again, a Jerome Lederer needs to come in and create a revitalized system safety program. System safety engineering needs to be placed back into mainstream engineering and started early enough to have an impact on system design. Other necessary safety activities would be assigned to the appropriate organizations, e.g., QA, operations, etc., and the whole coordinated by a Headquarters level office separate from other quality considerations and reporting to the Chief Engineer. A program-independent group (similar to the Navy’s WESRB) should be established to evaluate the safety analyses and safety-related design features (together sometimes called the safety case) created for new and existing NASA systems and have final authority in evaluating the individual safety efforts within the various organizations. True system safety standards (that do not equate safety with reliability) need to be written and enforced, again independent of the program. Either experienced system safety engineers need to be hired from...
outside NASA (probably from the defense arena) or an extensive education program on system safety needs to be implemented at NASA—or perhaps both. Most important, there needs to be commitment by NASA top management to re-establishing a strong system safety program at NASA and those tasked to do so must have the authority necessary to make the required changes and to overcome the efforts by those who will try to sabotage them. Finally, continuous assessment and feedback about the effectiveness of system safety needs to be built into the procedures and activities to identify if they are weakening over time and the organization is again migrating toward a state of unacceptable risk.