Chapter 10

Other Significant Observations

Although the Board now understands the combination of technical and organizational factors that contributed to the *Columbia* accident, the investigation did not immediately zero in on the causes identified in previous chapters. Instead, the Board explored a number of avenues and topics that, in the end, were not directly related to the cause of this accident. Nonetheless, these forays revealed technical, safety, and cultural issues that could impact the Space Shuttle Program, and, more broadly, the future of human space flight. The significant issues listed in this chapter are potentially serious matters that should be addresed by NASA because they fall into the category of "weak signals" that could be indications of future problems.

10.1 Public Safety

Shortly after the breakup of *Columbia* over Texas, dramatic images of the Orbiter's debris surfaced: an intact spherical tank in an empty parking lot, an obliterated office rooftop, mangled metal along roadsides, charred chunks of material in fields. These images, combined with the large number of debris fragments that were recovered, compelled many to proclaim it was a "miracle" that no one on the ground had been hurt.[1]

The *Columbia* accident raises some important questions about public safety. What were the chances that the general public could have been hurt by a breakup of an Orbiter? How safe are Shuttle flights compared with those of conventional aircraft? How much public risk from space flight is acceptable? Who is responsible for public safety during space flight operations?

Public Risk from *Columbia*'s Breakup

The Board commissioned a study to determine if the lack of reported injuries on the ground was a predictable outcome or simply exceptionally good fortune (see Appendix D.16). The study extrapolated from an array of data, including census figures for the debris impact area, the Orbiter's last reported position and velocity, the impact locations (latitude and longitude), and the total weight of all recovered debris, as well as the composition and dimensions of many debris pieces.[2]

Based on the best available evidence on *Columbia*'s disintegration and ground impact, the lack of serious injuries on the ground was the expected outcome for the location and time at which the breakup occurred.[3]

NASA and others have developed sophisticated computer tools to predict the trajectory and survivability of spacecraft debris during re-entry.[4] Such tools have been used to assess the risk of serious injuries to the public due to spacecraft re-entry, including debris impacts from launch vehicle malfunctions.[5] However, it is impossible to be certain about what fraction of *Columbia* survived to impact the ground. Some 38 percent of *Columbia*'s dry (empty) weight was recovered, but there is no way to determine how much still lies on the ground. Accounting for the inherent uncertainties associated with the amount of ground debris and the number of people outdoors,[6] there was about a 9- to 24-percent chance of at least one person being seriously injured by the disintegration of the Orbiter.[7]

Debris fell on a relatively sparsely populated area of the United States, with an average of about 85 inhabitants per square mile. Orbiter re-entry flight paths often pass over much more populated areas, including major cities that average more than 1,000 inhabitants per square mile. For example, the STS-107 re-entry profile passed over Sacramento, California, and Albuquerque, New Mexico. The Board-sponsored study concluded that, given the unlikely event of a similar Orbiter breakup over a densely populated area such as Houston, the most likely outcome would be one or two ground casualties.

Space Flight Risk Compared to Aircraft Operations

A recent study of U.S. civil aviation accidents found that between 1964 and 1999, falling aircraft debris killed an average of eight people per year.[8] In comparison, the National Center for Health Statistics reports that between 1992 and 1994, an average of 65 people in the United States were killed each year by lightning strikes. The aviation accident study revealed a decreasing trend in the annual number of "groundling" fatalities, so that an average of about four fatalities per year are predicted in the near future.[9] The probability of a U.S. resident being killed by aircraft debris is now less than one in a million over a 70-year lifetime.[10]

The history of U.S. space flight has a flawless public safety record. Since the 1950s, there have been hundreds of U.S. space launches without a single member of the public being injured. Comparisons between the risk to the public from space flight and aviation operations are limited by two factors: the absence of public injuries resulting from U.S. space flight operations, and the relatively small number of space flights (hundreds) compared to aircraft flights (billions).[11] Nonetheless, it is unlikely that U.S. space flights will produce many, if any, public injuries in the coming years based on (1) the low number of space flight operations per year, (2) the flawless public safety record of past U.S. space launches, (3) government-adopted space flight safety standards,[12] and (4) the risk assessment result that, even in the unlikely event of a similar Orbiter breakup over a major city, less than two ground casualties would be expected. In short, the risk posed to people on the ground by U.S. space flight operations is small compared to the risk from civil aircraft operations.

The government has sought to limit public risk from space flight to levels comparable to the risk produced by aircraft. U.S. space launch range commanders have agreed that the public should face no more than a one-in-a-million chance of fatality from launch vehicle and unmanned aircraft operations.[13] This aligns with Federal Aviation Administration (FAA) regulations that individuals be exposed to no more than a one-in-a-million chance of serious injury due to commercial space launch and re-entry operations.[14]

NASA has not actively followed public risk acceptability standards used by other government agencies during past Orbiter re-entry operations. However, in the aftermath of the *Columbia* accident, the agency has attempted to adopt similar rules to protect the public. It has also developed computer tools to predict the survivability of spacecraft debris during re-entry. Such tools have been used to assess the risk of public casualties attributable to spacecraft re-entry, including debris impacts from commercial launch vehicle malfunctions.[15]

Responsibility for Public Safety

The Director of the Kennedy Space Center is responsible for the ground and flight safety of Kennedy Space Center people and property for all launches.[16] The Air Force provides the Director with written notification of launch area risk estimates for Shuttle ascents. The Air Force routinely computes the risk that Shuttle ascents[17] pose to people on and off Kennedy grounds from potential debris impacts, toxic exposures, and explosions.[18]

However, no equivalent collaboration exists between NASA and the Air Force for re-entry risk. FAA rules on commercial space launch activities do not apply "where the Government is so substantially involved that it is effectively directing or controlling the launch." Based on the lack of a response, in tandem with NASA's public statements and informal replies to Board questions, the Board determined that NASA made no documented effort to assess public risk from Orbiter re-entry operations prior to the *Columbia* accident. The Board believes that NASA should be legally responsible for public safety during all phases of Shuttle operations, including re-entry.

Findings:

F10.1-1 The *Columbia* accident demonstrated that Orbiter breakup during re-entry has the potential to cause casualties among the general public.

F10.1-2 Given the best information available to date, a formal risk analysis sponsored by the Board found that the lack of general-public casualties from *Columbia*'s break-up was the expected outcome.

F10.1-3 The history of U.S. space flight has a flawless public safety record. Since the 1950s, hundreds of space flights have occurred without a single public injury.

F10.1-4 The FAA and U.S. space launch ranges have safety standards designed to ensure that the general public is exposed to less than a one-in-a-million chance of serious injury from the operation of space launch vehicles and unmanned aircraft.

F10.1-5 NASA did not demonstrably follow public risk acceptability standards during past Orbiter re-entries. NASA efforts are underway to define a national policy for the protection of public safety during all operations involving space launch vehicles.

Observations:

O10.1-1 NASA should develop and implement a public risk acceptability policy for launch and re-entry of space vehicles and unmanned aircraft.

O10.1-2 NASA should develop and implement a plan to mitigate the risk that Shuttle flights pose to the general public.

O10.1-3 NASA should study the debris recovered from *Columbia* to facilitate realistic estimates of the risk to the public during Orbiter re-entry.

10.2 Crew Escape and Survival

The Board has examined crew escape systems in historical context with a view to future improvements. It is important to note at the outset that *Columbia* broke up during a phase of flight that, given the current design of the Orbiter, offered no possibility of crew survival.

The goal of every Shuttle mission is the safe return of the crew. An escape system—a means for the crew to leave a vehicle in distress during some or all of its flight phases and return safely to Earth – has historically been viewed as one "technique" to accomplish that end. Other methods include various abort modes, rescue, and the creation of a safe haven (a location where crew members could remain unharmed if they are unable to return to Earth aboard a damaged Shuttle).

While crew escape systems have been discussed and studied continuously since the Shuttle's early design phases, only two systems have been incorporated: one for the developmental test flights, and the current system installed after the *Challenger* accident. Both designs have extremely limited capabilities, and neither has ever been used during a mission.

Developmental Test Flights

Early studies assumed that the Space Shuttle would be operational in every sense of the word. As a result, much like commercial airliners, a Shuttle crew escape system was considered unnecessary. NASA adopted requirements for rapid emergency egress of the crew in early Shuttle test flights. Modified SR-71 ejection seats for the two pilot positions were installed on the Orbiter test vehicle *Enterprise,* which was carried to an altitude of 25,000 feet by a Boeing 747 Shuttle Carrier Aircraft during the Approach and Landing Tests in 1977.[19]

Essentially the same system was installed on *Columbia* and used for the four Orbital Test Flights during 1981-82. While this system was designed for use during first-stage ascent and in gliding flight below 100,000 feet, considerable doubt emerged about the survivability of an ejection that would expose crew members to the Solid Rocket Booster exhaust plume. Regardless, NASA declared the developmental test flight phase complete after STS-4, *Columbia*'s fourth flight, and the ejection seat system was deactivated. Its associated hardware was removed during modification after STS-9. All Space Shuttle missions after STS-4 were conducted with crews of four or more, and no escape system was installed until after the loss of *Challenger* in 1986.

Before the *Challenger* accident, the question of crew survival was not considered independently from the possibility of catastrophic Shuttle damage. In short, NASA believed if the Orbiter could be saved, then the crew would be safe. Perceived limits of the use of escape systems, along with their cost, engineering complexity, and weight/payload trade-offs, dissuaded NASA from implementing a crew escape plan. Instead, the agency focused on preventing the loss of a Shuttle as the sole means for assuring crew survival.

Post-*Challenger*: the Current System

NASA's rejection of a crew escape system was severely criticized after the loss of *Challenger*. The Rogers Commission addressed the topic in a recommendation that combined the issues of launch abort and crew escape:[20]

> *Launch Abort and Crew Escape. The Shuttle Program management considered first-stage abort options and crew escape options several times during the history of the program, but because of limited utility, technical infeasibility, or program cost and schedule, no systems were implemented. The Commission recommends that NASA:*
>
> - *Make all efforts to provide a crew escape system for use during controlled gliding flight.*
> - *Make every effort to increase the range of flight conditions under which an emergency runway landing can be successfully conducted in the event that two or three main engines fail early in ascent.*

In response to this recommendation, NASA developed the current "pole bailout" system for use during controlled, subsonic gliding flight (see Figure 10.2-1). The system requires crew members to "vent" the cabin at 40,000 feet (to equalize the cabin pressure with the pressure at that altitude), jettison the hatch at approximately 32,000 feet, and then jump out of the vehicle (the pole allows crew members to avoid striking the Orbiter's wings).

Figure 10.2-1. A demonstration of the pole bailout system. The pole is extending from the side of a C-141 simulating the Orbiter, with a crew member sliding down the pole so that he would fall clear of the Orbiter's wing during an actual bailout.

Current Human-Rating Requirements

In June 1998, Johnson Space Center issued new Human-Rating Requirements applicable to "all future human-rated spacecraft operated by NASA." In July 2003, shortly before this report was published, NASA issued further Human-Rating Requirements and Guidelines for Space Flight Systems, over the signature of the Associate Administrator for Safety and Mission Assurance. While these new requirements "… shall not supersede more stringent requirements imposed by individual NASA organizations …" NASA has informed the Board that the earlier – and in some cases more prescriptive – Johnson Space Center requirements have been cancelled.

NASA's 2003 Human-Rating Requirements and Guidelines for Space Flight Systems laid out the following principles regarding crew escape and survival:

> *2.5.4 Crew survival*
>
> *2.5.4.1 As part of the design process, program management (with approval from the CHMO* [Chief Health and Medical Officer]**,** *AA for OSF* [Associate Administrator for the Office of Spaceflight]**,** *and AA for SMA* [Associate Administrator for Safety and Mission Assurance] *shall establish, assess, and document the program requirements for an acceptable life cycle cumulative probability of safe crew and passenger return. This probability requirement can be satisfied through the use of all available mechanisms including nominal mission completion, abort, safe haven, or crew escape.*
>
> *2.5.4.2 The cumulative probability of safe crew and passenger return shall address all missions planned for the life of the program, not just a single space flight system for a single mission.*

The overall probability of crew and passenger survival must meet the minimum program requirements (as defined in section 2.5.4.1) for the stated life of a space flight systems program.[21] This approach is required to reflect the different technical challenges and levels of operational risk exposure on various types of missions. For example, low-Earth-orbit missions represent fundamentally different risks than does the first mission to Mars. Single-mission risk on the order of 0.99 for a beyond-Earth-orbit mission may be acceptable, but considerably better performance, on the order of 0.9999, is expected for a reusable low-Earth-orbit design that will make 100 or more flights.

> *2.6 Abort and Crew Escape*
>
> *2.6.1 The capability for rapid crew and occupant egress shall be provided during all pre-launch activities.*
>
> *2.6.2 The capability for crew and occupant survival and recovery shall be provided on ascent using a combination of abort and escape.*
>
> *2.6.3 The capability for crew and occupant survival and recovery shall be provided during all other phases of flight (including on-orbit, reentry, and landing) using a combination of abort and escape, unless comprehensive safety and reliability analyses indicate that abort and escape capability is not required to meet crew survival requirements.*
>
> *2.6.4 Determinations regarding escape and abort shall be made based upon comprehensive safety and reliability analyses across all mission profiles.*

These new requirements focus on general crew survival rather than on particular crew escape systems. This provides a logical context for discussions of tradeoffs that will yield the best crew-survival outcome. Such tradeoffs include "mass-trades" – for example, an escape system could add weight to a vehicle, but in the process cause payload changes that require additional missions, thereby inherently increasing the overall exposure to risk.

Note that the new requirements for crew escape appear less prescriptive than Johnson Space Center Requirement 7, which deals with "safe crew extraction" from pre-launch to landing.[22]

In addition, the extent to which NASA's 2003 requirements will retroactively apply to the Space Shuttle is an open question:

> *The Governing Program Management Council (GPMC) will determine the applicability of this document to programs and projects in existence (e.g., heritage expendable and reusable launch vehicles and evolved expendable launch vehicles), at or beyond implementation, at the time of the issuance of this document.*

Recommendations of the NASA Aerospace Safety Advisory Panel

The issue of crew escape has long been a matter of concern to NASA's Aerospace Safety Advisory Panel. In its 2002 Annual Report, the panel noted that NASA Program Guidelines on Human Rating require escape systems for all flight vehicles, but the guidelines do not apply to the Space Shuttle. The Panel considered it appropriate, in view of the Shuttle's proposed life extension, to consider upgrading the vehicle to comply with the guidelines.[23]

> *Recommendation 02-9: Complete the ongoing studies of crew escape design options. Either document the reasons for not implementing the NASA Program Guidelines on Human Rating or expedite the deployment of such capabilities.*

The Board shares the concern of the NASA Aerospace Safety Advisory Panel and others over the lack of a crew escape system for the Space Shuttle that could cover the widest possible range of flight regimes and emergencies. At the same time, a crew escape system is just one element to be optimized for crew survival. Crucial tradeoffs in risk, complexity, weight, and operational utility must be made when considering a Shuttle escape system. Designs for future vehicles and possible retrofits should be evaluated in this context. The sole objective must be the highest probability of a crew's safe return regardless if that is due to successful mission completions, vehicle-intact aborts, safe haven/rescues, escape systems, or some combination of these scenarios.

Finally, a crew escape system cannot be considered separately from the issues of Shuttle retirement/replacement, separation of cargo from crew in future vehicles, and other considerations in the development – and the inherent risks of space flight.

Space flight is an inherently dangerous undertaking, and will remain so for the foreseeable future. While all efforts must be taken to minimize its risks, the White House, Congress, and the American public must acknowledge these dangers and be prepared to accept their consequences.

Observations:

O10.2-1 Future crewed-vehicle requirements should incorporate the knowledge gained from the *Challenger* and *Columbia* accidents in assessing the feasibility of vehicles that could ensure crew survival even if the vehicle is destroyed.

10.3 Shuttle Engineering Drawings and Closeout Photographs

In the years since the Shuttle was designed, NASA has not updated its engineering drawings or converted to computer-aided drafting systems. The Board's review of these engineering drawings revealed numerous inaccuracies. In particular, the drawings do not incorporate many engineering changes made in the last two decades. Equally troubling was the difficulty in obtaining these drawings: it took up to four weeks to receive them, and, though some photographs were available as a short-term substitute, closeout photos took up to six weeks to obtain. (Closeout photos are pictures taken of Shuttle areas before they are sealed off for flight.) The Aerospace Safety Advisory Panel noted similar difficulties in its 2001 and 2002 reports.

The Board believes that the Shuttle's current engineering drawing system is inadequate for another 20 years' use. Widespread inaccuracies, unincorporated engineering updates, and significant delays in this system represent a significant dilemma for NASA in the event of an on-orbit crisis that requires timely and accurate engineering information. The dangers of an inaccurate and inaccessible drawing system are exacerbated by the apparent lack of readily available closeout photographs as interim replacements (see Appendix D.15).

Findings:

F10.3-1 The engineering drawing system contains outdated information and is paper-based rather than computer-aided.

F10.3-2 The current drawing system cannot quickly portray Shuttle sub-systems for on-orbit troubleshooting.

F10.3-3 NASA normally uses closeout photographs but lacks a clear system to define which critical sub-systems should have such photographs. The current system does not allow the immediate retrieval of closeout photos.

Recommendations:

R10.3-1 Develop an interim program of closeout photographs for all critical sub-systems that differ from engineering drawings. Digitize the closeout photograph system so that images are immediately available for on-orbit troubleshooting.

R10.3-2 Provide adequate resources for a long-term program to upgrade the Shuttle engineering drawing system including:

- Reviewing drawings for accuracy
- Converting all drawings to a computer-aided drafting system
- Incorporating engineering changes

10.4 Industrial Safety and Quality Assurance

The industrial safety programs in place at NASA and its contractors are robust and in good health. However, the scope and depth of NASA's maintenance and quality assurance programs are troublesome. Though unrelated to the *Columbia* accident, the major deficiencies in these programs uncovered by the Board could potentially contribute to a future accident.

Industrial Safety

Industrial safety programs at NASA and its contractors—covering safety measures "on the shop floor" and in the workplace – were examined by interviews, observations, and reviews. Vibrant industrial safety programs were found in every area examined, reflecting a common interview comment: "If anything, we go overboard on safety." Industrial safety programs are highly visible: they are nearly always a topic of work center meetings and are represented by numerous safety campaigns and posters (see Figure 10.4-1).

Figure 10.4-1. Safety posters at NASA and contractor facilities.

Initiatives like Michoud's "This is Stupid" program and the United Space Alliance's "Time Out" cards empower employees to halt any operation under way if they believe industrial safety is being compromised (see Figure 10.4-2). For example, the Time Out program encourages and even rewards workers who report suspected safety problems to management.

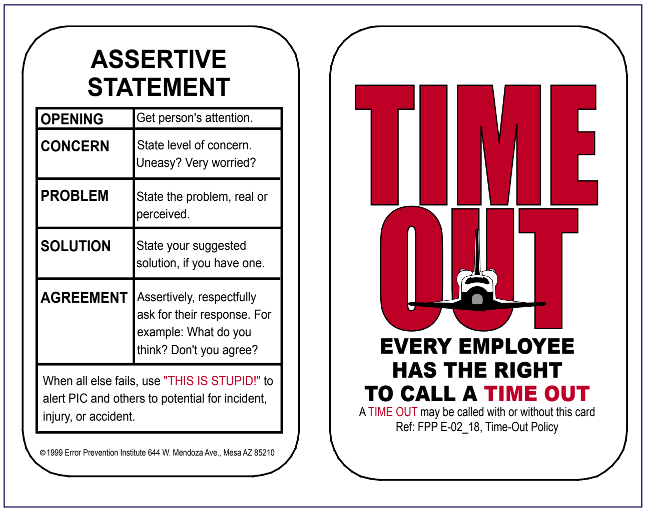

Figure 10.4-2. The "This is Stupid" card from the Michoud Assembly Facility and the "Time Out" card from United Space Alliance.

NASA similarly maintains the Safety Reporting System, which creates lines of communication through which anonymous inputs are forwarded directly to headquarters (see Figure 10.4-3). The NASA Shuttle Logistics Depot focus on safety has been recognized as an Occupational Safety and Health Administration Star Site for its participation in the Voluntary Protection Program. After the Shuttle Logistics Depot was recertified in 2002, employees worked more than 750 days without a lost-time mishap.

Quality Assurance

Quality Assurance programs – encompassing steps to encourage error-free work, as well as inspections and assessments of that work – have evolved considerably in scope over the past five years, transitioning from intensive, comprehensive inspection regimens to much smaller programs based on past risk analysis.

As described in Part Two, after the Space Flight Operations Contract was established, NASA's quality assurance role at Kennedy Space Center was significantly reduced. In the course of this transition, Kennedy reduced its inspections – called Government Mandatory Inspection Points – by more than 80 percent. Marshall Space Flight Center cut its inspection workload from 49,000 government inspection points and 821,000 contractor inspections in 1990 to 13,700 and 461,000, respectively, in 2002. Similar cutbacks were made at most NASA centers.

Inspection requirements are specified in the Quality Planning Requirements Document (also called the Mandatory Inspections Document). United Space Alliance technicians must document an estimated 730,000 tasks to complete a single Shuttle maintenance flow at Kennedy Space Center. Nearly every task assessed as Criticality Code 1, 1R (redundant), or 2 is always inspected, as are any systems not verifiable by operational checks or tests prior to final preparations for flight.

Nearly everyone interviewed at Kennedy indicated that the current inspection process is both inadequate and difficult to expand, even incrementally. One example was a long-standing request to add a main engine final review before transporting the engine to the Orbiter Processing Facility for installation. This request was first voiced two years before the launch of STS-107, and has been repeatedly denied due to inadequate staffing. In its place, NASA Mission Assurance conducts a final "informal" review. Adjusting government inspection tasks is constrained by institutional dogma that the status quo is based on strong engineering logic, and should need no adjustment. This mindset inhibits the ability of Quality Assurance to respond to an aging system, changing workforce dynamics, and improvement initiatives.

The Quality Planning Requirements Document, which defines inspection requirements, was well formulated but is not routinely reviewed. Indeed, NASA seems reluctant to add or subtract government inspections, particularly at Kennedy. Additions and subtractions are rare, and generally occur only as a response to obvious problems. For instance, NASA augmented wiring inspections after STS-93 in 1999, when a short circuit shut down two of *Columbia*'s Main Engine Controllers. Interviews confirmed that the current Requirements Document lacks numerous critical items, but conversely demands redundant and unnecessary inspections.

The NASA/United Space Alliance Quality Assurance processes at Kennedy are not fully integrated with each other, with Safety, Health, and Independent Assessment, or with Engineering Surveillance Programs. Individually, each plays a vital role in the control and assessment of the Shuttle as it comes together in the Orbiter Processing Facility and Vehicle Assembly Building. Were they to be carefully integrated, these programs could attain a nearly comprehensive quality control process. Marshall has a similar challenge. It

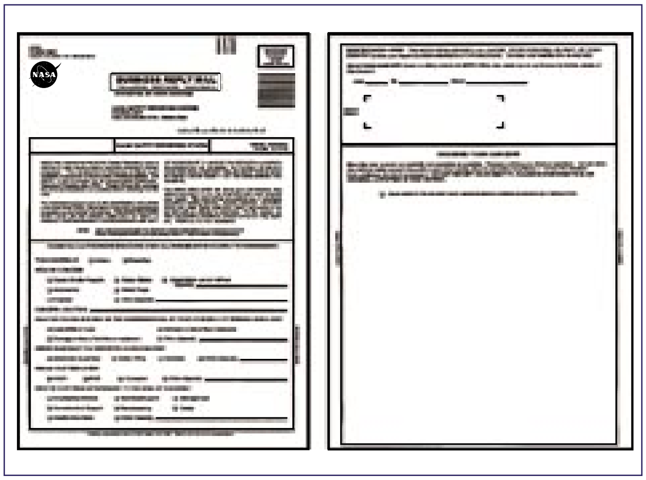

Figure 10.4-3. NASA Safety Reporting System Form.

is responsible for managing several different Shuttle systems through contractors who maintain mostly proprietary databases, and therefore, integration is limited. The main engine program overcomes this challenge by being centrally organized under a single Mission Assurance Division Chief who reports to the Marshall Center Director. In contrast, Kennedy has a separate Mission Assurance office working directly for each program, a separate Safety, Health, and Independent Assessment office under the Center Director, and separate quality engineers under each program. Observing the effectiveness of Marshall, and other successful Mission Assurance programs (such as at Johnson Space Center), a solution may be the consolidation of the Kennedy Space Center Quality Assurance program under one Mission Assurance office, which would report to the Center Director.

While reports by the 1986 Rogers Commission, 2000 Shuttle Independent Assessment Team, and 2003 internal Kennedy Tiger Team all affirmed the need for a strong and independent Quality Assurance Program, Kennedy's Program has taken the opposite tack. Kennedy's Quality Assurance program discrepancy-tracking system is inadequate to nonexistent.

Robust as recently as three years ago, Kennedy no longer has a "closed loop" system in which discrepancies and their remedies circle back to the person who first noted the problem. Previous methods included the NASA Corrective Action Report, two-way memos, and other tools that helped ensure that a discrepancy would be addressed and corrected. The Kennedy Quality Program Manager cancelled these programs in favor of a contractor-run database called the Quality Control Assessment Tool. However, it does not demand a closed-loop or reply deadline, and suffers from limitations on effective data entry and retrieval.

Kennedy Quality Assurance management has recently focused its efforts on implementing the International Organization for Standardization (ISO) 9000/9001, a process-driven program originally intended for manufacturing plants. Board observations and interviews underscore areas where Kennedy has diverged from its Apollo-era reputation of setting the standard for quality. With the implementation of International Standardization, it could devolve further. While ISO 9000/9001 expresses strong principles, they are more applicable to manufacturing and repetitive-procedure industries, such as

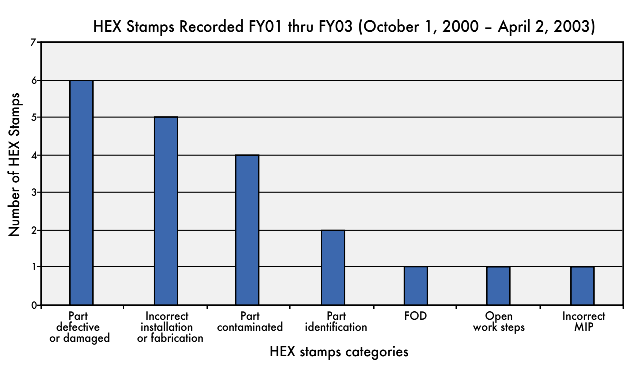

Figure 10.4-4. Rejection, or "Hex" stamps issued from October 2000 through April 2003.

running a major airline, than to a research-and-development, non-operational flight test environment like that of the Space Shuttle. NASA technicians may perform a specific procedure only three or four times a year, in contrast with their airline counterparts, who perform procedures dozens of times each week. In NASA's own words regarding standardization, "ISO 9001 is not a management panacea, and is never a replacement for management taking responsibility for sound decision making." Indeed, many perceive International Standardization as emphasizing process over product.

Efforts by Kennedy Quality Assurance management to move its workforce towards a "hands-off, eyes-off" approach are unsettling. To use a term coined by the 2000 Shuttle Independent Assessment Team Report, "diving catches," or last-minute saves, continue to occur in maintenance and processing and pose serious hazards to Shuttle safety. More disturbingly, some proverbial balls are not caught until after flight. For example, documentation revealed instances where Shuttle components stamped "ground test only" were detected both before and after they had flown. Additionally, testimony and documentation submitted by witnesses revealed components that had flown "as is" without proper disposition by the Material Review Board prior to flight, which implies a growing acceptance of risk. Such incidents underscore the need to expand government inspections and surveillance, and highlight a lack of communication between NASA employees and contractors.

Another indication of continuing problems lies in an opinion voiced by many witnesses that is confirmed by Board tracking: Kennedy Quality Assurance management discourages inspectors from rejecting contractor work. Inspectors are told to cooperate with contractors to fix problems rather than rejecting the work and forcing contractors to resubmit it. With a rejection, discrepancies become a matter of record; in this new process, discrepancies are not recorded or tracked. As a result, discrepancies are currently not being tracked in any easily accessible database.

Of the 141,127 inspections subject to rejection from October 2000 through March 2003, only 20 rejections, or "hexes," were recorded, resulting in a statistically improbable discrepancy rate of .014 percent (see Figure 10.4-4). In interviews, technicians and inspectors alike confirmed the dubiousness of this rate. NASA's published rejection rate therefore indicates either inadequate documentation or an underused system. Testimony further revealed incidents of quality assurance inspectors being played against each other to accept work that had originally been refused.

Findings:

F10.4-1 Shuttle System industrial safety programs are in good health.

F10.4-2 The Quality Planning Requirements Document, which defines inspection conditions, was well formulated. However, there is no requirement that it be routinely reviewed.

F10.4-3 Kennedy Space Center's current government mandatory inspection process is both inadequate and difficult to expand, which inhibits the ability of Quality Assurance to process improvement initiatives.

F10.4-4 Kennedy's quality assurance system encourages inspectors to allow incorrect work to be corrected without being labeled "rejected." These opportunities hide "rejections," making it impossible to determine how often and on what items frequent rejections and errors occur.

Observations:

O10.4-1 Perform an independently led, bottom-up review of the Kennedy Space Center Quality Planning Requirements Document to address the entire quality assurance program and its administration. This review should include development of a responsive system to add or delete government mandatory inspections.

O10.4-2 Kennedy Space Center's Quality Assurance programs should be consolidated under one Mission Assurance office, which reports to the Center Director.

O10.4-3 Kennedy Space Center quality assurance management must work with NASA and perhaps the Department of Defense to develop training programs for its personnel.

O10.4-4 Kennedy Space Center should examine which areas of International Organization for Standardization 9000/9001 truly apply to a 20-year-old research and development system like the Space Shuttle.

10.5 Maintenance Documentation

The Board reviewed *Columbia's* maintenance records for any documentation problems, evidence of maintenance flaws, or significant omissions, and simultaneously investigated the organizations and management responsible for this documentation. The review revealed both inaccurate data entries and a widespread inability to find and correct these inaccuracies.

The Board asked Kennedy Space Center and United Space Alliance to review documentation for STS-107, STS-109, and *Columbia*'s most recent Orbiter Major Modification. A NASA Process Review Team, consisting of 445 NASA engineers, contractor engineers, and Quality Assurance personnel, reviewed some 16,500 Work Authorization Documents, and provided a list of Findings (potential relationships to the accident), Technical Observations (technical concerns or process issues), and Documentation Observations (minor errors). The list contained one Finding related to the External Tank bipod ramp. None of the Observations contributed to the accident.

The Process Review Team's sampling plan resulted in excellent observations.[24] The number of observations is relatively low compared to the total amount of Work Authorization Documents reviewed, ostensibly yielding a 99.75 percent accuracy rate. While this number is high, a closer review of the data reveals some of the system's weaknesses. Technical Observations are delineated into 17 categories. Five of these categories are of particular concern for mishap prevention and reinforce the need for process improvements. The category entitled "System configuration could damage hardware" is listed 112 times. Categories that deal with poor incorporation of technical guidance are of particular interest due to the Board's concern over the backlog of unincorporated engineering orders. Finally, a category entitled "paper has open work steps," indicates that the review system failed to catch a potentially significant oversight 310 times in this sample. (The complete results of this review may be found in Appendix D.14.)

The current process includes three or more layers of oversight before paperwork is scanned into the database. However, if review authorities are not aware of the most common problems to look for, corrections cannot be made. Routine sampling will help refine this process and cut errors significantly.

Observations:

O10.5-1 Quality and Engineering review of work documents for STS-114 should be accomplished using statistical sampling to ensure that a representative sample is evaluated and adequate feedback is communicated to resolve documentation problems.

O10.5-2 NASA should implement United Space Alliance's suggestions for process improvement, which recommend including a statistical sampling of all future paperwork to identify recurring problems and implement corrective actions.

O10.5-3 NASA needs an oversight process to statistically sample the work performed and documented by Alliance technicians to ensure process control, compliance, and consistency.

10.6 Orbiter Maintenance Down Period/ Orbiter Major Modification

During the Orbiter Major Modification process, Orbiters are removed from service for inspections, maintenance, and modification. The process occurs every eight flights or three years.

Orbiter Major Modifications combine with Orbiter flows (preparation of the vehicle for its next mission) and include Orbiter Maintenance Down Periods (not every Orbiter Maintenance Down Period includes an Orbiter Major Modification). The primary differences between an Orbiter Major Modification and an Orbiter flow are the larger number of requirements and the greater degree of intrusiveness of a modification (a recent comparison showed 8,702 Orbiter Major Modification requirements versus 3,826 flow requirements).

Ten Orbiter Major Modifications have been performed to date, with an eleventh in progress. They have varied from 6 to 20 months. Because missions do not occur at the rate the Shuttle Program anticipated at its inception, it is endlessly challenged to meet numerous calendar-based requirements. These must be performed regardless of the lower flight rate, which contributes to extensive downtime. The Shuttle Program has explored the possibility of extending Orbiter Major Modification cycles to once every 12 flights or six years. This initiative runs counter to the industry norm of increasing the frequency of inspections as systems age, and should be carefully scrutinized, particularly in light of the high-performance Orbiters' demands.

Orbiter Major Modifications underwent a significant change when they were relocated from the Boeing facility in Palmdale, California, (where the Orbiters had been manufactured) to Kennedy Space Center in September 2002. The major impetus for this change was budget shortages in Fiscal Years 2002 and 2003. The move capitalizes on many advantages at Kennedy, including lower labor and utility costs and more efficient use of existing overhead, while eliminating expensive, underused, and redundant capabilities at Palmdale. However, the move also created new challenges: for instance, it complicates the integration of planning and scheduling, and forces the Space Shuttle Program to maintain a fluid workforce in which employees must repeatedly change tasks as they shift between Orbiter Major Modifications, flows, and downtime.

Throughout the history of Orbiter Major Modifications, a major area of concern has been their wide variability in content and duration. *Columbia*'s last Orbiter Major Modification is just the most recent example of overruns due to technical surprises and management difficulties. It exceeded the schedule by 186 days. While many factors contributed to this delay, the two most prominent were the introduction of a major wiring inspection one month after Orbiter Major Modification roll-in, and what an internal NASA assessment cited as "poor performance on the parts of NASA, USA [United Space Alliance], and Boeing."

While the Shuttle Program has made efforts to correct these problems, there is still much to be done. The transfer to Kennedy creates a steep learning curve both for technicians and managers. Planning and scheduling the integration of all three Orbiters, as well as ground support systems maintenance, is critical to limit competition for resources. Moreover, estimating the "right" amount of work required on each Orbiter continues to be a challenge. For example, 20 modifications were planned for *Discovery*'s modification; the number has since grown to 84. Such changes introduce turmoil and increase the potential for mistakes.

An Air Force "benchmarking" visit in June 2003 highlighted the need for better planning and more scheduling stability. It further recommended improvements to the requirements feedback process and incorporating service life extension actions into Orbiter Major Modifications.

Observations:

O10.6-1 The Space Shuttle Program Office must make every effort to achieve greater stability, consistency, and predictability in Orbiter Major Modification planning, scheduling, and work standards (particularly in the number of modifications). Endless changes create unnecessary turmoil and can adversely impact quality and safety.

O10.6-2 NASA and United Space Alliance managers must understand workforce and infrastructure requirements, match them against capabilities, and take actions to avoid exceeding thresholds.

O10.6-3 NASA should continue to work with the U.S. Air Force, particularly in areas of program management that deal with aging systems, service life extension, planning and scheduling, workforce management, training, and quality assurance.

O10.6-4 The Space Shuttle Program Office must determine how it will effectively meet the challenges of inspecting and maintaining an aging Orbiter fleet before lengthening Orbiter Major Maintenance intervals.

10.7 Orbiter Corrosion

Removing and replacing Thermal Protection System tiles sometimes results in damage to the anti-corrosion primer that covers the Orbiters' sheet metal skin. Tile replacement often occurs without first re-priming the primed aluminum substrate. The current repair practice allows Room Temperature Vulcanizing adhesive to be applied over a bare aluminum substrate (with no Koropon corrosion-inhibiting compound) when bonding tile to the Orbiter.

A video borescope of *Columbia* prior to STS-107 found corrosion on the lower forward fuselage skin panel and stringer areas. Corrosion on visible rivets and on the sides and feet of stringer sections was also uncovered during borescope inspections, but was not repaired.

Other corrosion concerns focus on the area between the crew module and outer hull, which is a difficult area to access for inspection and repair. At present, corrosion in this area is only monitored with borescope inspections. There is also concern that unchecked corrosion could progress from internal areas to external surfaces through fastener holes, joints, or directly through the skin. If this occurs beneath the tile, the tile system bond line could degrade.

Long-Term Corrosion Detection

Limited accessibility renders some corrosion damage difficult to detect. Approximately 90 percent of the Orbiter structure (excluding the tile-covered outer mold line) can be inspected for corrosion.[25] Corrosion in the remaining 10 percent may remain undetected for the life of the vehicle.

NASA has recently outlined a $70 million, 19-year program to assess and mitigate corrosion. The agency foresees inspection intervals based on trends in the Problem Resolution and Corrective Action database, exposure to the environment, and refurbishment programs. Development of a correlation between corrosion initiation, growth, and environmental exposure requires the judicious use of long-term test data. Moreover, some corrosion problems are uncovered during non-corrosion inspections. The risk of undetected corrosion may increase as other inspections are removed or intervals between inspections are extended.

Observations:

O10.7-1 Additional and recurring evaluation of corrosion damage should include non-destructive analysis of the potential impacts on structural integrity.

O10.7-2 Long-term corrosion detection should be a funding priority.

O10.7-3 Develop non-destructive evaluation inspections to find hidden corrosion.

O10.7-4 Inspection requirements for corrosion due to environmental exposure should first establish corrosion rates for Orbiter-specific environments, materials, and structural configurations. Consider applying Air Force corrosion prevention programs to the Orbiter.

10.8 Brittle Fracture of A-286 Bolts

Investigators sought to determine the cause of brittle fractures in the A-286 steel bolts that support the wing's lower carrier panels, which provide direct access to the interior of the Reinforced Carbon-Carbon (RCC) panels. Any misalignment of the carrier panels affects the continuity of airflow under the wing and can cause a "rough wing" (see Chapter 4). In the end, 57 of the 88 A-286 bolts on *Columbia*'s wings were recovered; 22 had brittle fractures. The fractures occurred equally in two groups of bolts in the same locations on each wing. Investigators determined that liquid metal embrittlement caused by aluminum vapor created by *Columbia*'s breakup could have contributed to these fractures, but the axial loads placed on the bolts when they separated from the carrier panel/box beam at temperatures approaching 2,000 degrees Fahrenheit likely caused the failures.

Findings:

F10.8-1 The present design and fabrication of the lower carrier panel attachments are inadequate. The bolts can readily pull through the relatively large holes in the box beams.

F10.8-2 The current design of the box beam in the lower carrier panel assembly exposes the attachment bolts to a rapid exchange of air along the wing, which enables the failure of numerous bolts.

F10.8-3 Primers and sealants such as Room Temperature Vulcanizing 560 and Koropon may accelerate corrosion, particularly in tight crevices.

F10.8-4 The negligible compressive stresses that normally occur in A-286 bolts help protect against failure.

Observations:

O10.8-1 Teflon (material) and Molybdenum Disulfide (lubricant) should not be used in the carrier panel bolt assembly.

O10.8-2 Galvanic coupling between aluminum and steel alloys must be mitigated.

O10.8-3 The use of Room Temperature Vulcanizing 560 and Koropon should be reviewed.

O10.8-4 Assuring the continued presence of compressive stresses in A-286 bolts should be part of their acceptance and qualification procedures.

10.9 Hold-Down Post Cable Anomaly

Each of the two Solid Rocket Boosters is attached to the Mobile Launch Platform by four "hold down" bolts. A five-inch diameter restraint nut that contains two pyrotechnic initiators secures each of these bolts. The initiators sever the nuts when the Solid Rocket Boosters ignite, allowing the Space Shuttle stack to lift off. During launch, STS-112 suffered a failure in the Hold-Down Post and External Tank Vent Arm Systems that control the firing of initiators in each Solid Rocket Booster restraint nut. NASA had been warned that a recurrence of this type of failure could cause catastrophic failure of the Shuttle stack (see Appendix D.15).

The signal to fire the initiators begins in the General Purpose Computers and goes to both of the Master Events Controllers on the Orbiter. Master Events Controller 1 communicates this signal to the A system cable, and Master Events Controller 2 feeds the B system. The cabling then goes through the T–0 umbilical (that connects fluid and electrical connections between the launch pad and the Orbiter) to the Pyrotechnics Initiator Controllers and then to the initiators. (There are 16 Pyrotechnics Initiator Controllers for Hold Down Post Systems A and B, and four for the External Tank Vent Arm Systems A and B.) The Hold Down Post System A is hard-wired to one of the initiators on each of the four restraint nuts (eight total) while System B is hard-wired to the other initiator on each nut. The A and B systems also send a duplicate signal to the External Tank Vent Arm System. Either Master Events Controller will operate if the other or the intervening cabling fails.

A post-launch review of STS-112 indicated that the System A Hold-Down Post and External Tank Vent Arm System Pyrotechnics Initiator Controllers did not discharge. Initial troubleshooting revealed no malfunction, leading to the conclusion that the failure was intermittent. A subsequent investigation recommended the following:

- All T–0 Ground Cables will be replaced after every flight.
- The T–0 interface to the Pyrotechnics Initiator Controllers rack cable (Kapton) is in redesign.
- All Orbiter T–0 Connector Savers have been replaced.
- Pyrotechnic connectors will be pre-screened with pin-retention tests, and the connector saver mate process will be verified using videoscopes.

However, prelaunch testing procedures have not changed and may not be able to identify intermittent failures.

Findings:

F10.9-1 The Hold-Down Post External Tank Vent Arm System is a Criticality 1R (redundant) system. Before the anomaly on STS-112, and despite the high-criticality factor, the original cabling for this system was used repeatedly until it was visibly damaged. Replacing these cables after every flight and removing the Kapton will prevent bending and manipulation damage.

F10.9-2 NASA is unclear about the potential for damage if the system malfunctions, or even if one nut fails to split. Several program managers were asked: What if the A system fails, and a B-system initiator fails simultaneously? The consensus was that the system would continue to burn on the pad or that the Solid Rocket Booster would rip free of the pad, causing potentially catastrophic damage to the Solid Rocket Booster skirt and nozzle maneuvering mechanism. However, they agree that the probability of this is extremely low.

F10.9-3 With the exception of STS-112's anomaly, numerous bolt hang-ups, and occasional Master Events Controller failures, these systems have a good record. In the early design stages, risk-mitigating options were considered, including strapping with either a wire that crosses over the nut from the A to B side, or with a toggle circuit that sends a signal to the opposite side when either initiator fires. Both options would eliminate the potential of a catastrophic dual failure. However, they could also create new failure potentials that may not reduce overall system risk. Today's test and troubleshooting technology may have improved the ability to test circuits and potentially prevent intermittent failures, but it is not clear if NASA has explored these options.

Observation:

O10.9-1 NASA should consider a redesign of the system, such as adding a cross-strapping cable, or conduct advanced testing for intermittent failure.

10.10 Solid Rocket Booster External Tank Attachment Ring

In Chapter 4, the Board noted how NASA's reliance on "analysis" to validate Shuttle components led to the use of flawed bolt catchers. NASA's use of this flawed "analysis" technique is endemic. The Board has found that such analysis was invoked, with potentially dire consequences, on the Solid Rocket Booster External Tank Attach Ring. Tests showed that the tensile strength of several of these rings was well below minimum safety requirements. This problem was brought to NASA's attention shortly before the launch of STS-107. To accommodate the launch schedule, the External Tanking Meeting chair, after a cursory briefing without a full technical review, reduced the Attach Rings' minimum required safety factor of 1.4 (that is, able to withstand 1.4 times the maximum load ever expected in operations) to 1.25. Though NASA has formulated short- and long-term corrections, its long-term plan has not yet been authorized.

Observation:

O10.10-1 NASA should reinstate a safety factor of 1.4 for the Attachment Rings—which invalidates the use of ring serial numbers 16 and 15 in their present state—and replace all deficient material in the Attachment Rings.

10.11 Test Equipment Upgrades

Visits to NASA facilities (both government and contractor operated, as well as contractor facilities) and interviews with technicians revealed the use of 1970s-era oscilloscopes and other analog equipment. Currently available equipment is digital, and in other venues has proved to be less costly, easier to maintain, and more reliable and accurate. With the Shuttle forecast to fly through 2020, an upgrade to digital equipment would avoid the high maintenance, lack of parts, and dubious accuracy of equipment currently used. New equipment would require certification for its uses, but the benefit in accuracy, maintainability, and longevity would likely outweigh the drawbacks of certification costs.

Observation:

O10.11-1 Assess NASA and contractor equipment to determine if an upgrade will provide the reliability and accuracy needed to maintain the Shuttle through 2020. Plan an aggressive certification program for replaced items so that new equipment can be put into operation as soon as possible.

10.12 Leadership/Managerial Training

Managers at many levels in NASA, from GS-14 to Associate Administrator, have taken their positions without following a recommended standard of training and education to prepare them for roles of increased responsibility. While NASA has a number of in-house academic training and career development opportunities, the timing and strategy for management and leadership development differs across organizations. Unlike other sectors of the Federal Government and the military, NASA does not have a standard agency-wide career planning process to prepare its junior and mid-level managers for advanced roles. These programs range from academic fellowships to civil service education programs to billets in military-sponsored programs, and will allow NASA to build a strong corps of potential leaders for future progression.

Observation:

O10.12-1 NASA should implement an agency-wide strategy for leadership and management training that provides a more consistent and integrated approach to career development. This strategy should identify the management and leadership skills, abilities, and experiences required for each level of advancement. NASA should continue to expand its leadership development partnerships with the Department of Defense and other external organizations.

ENDNOTES FOR CHAPTER 10

The citations that contain a reference to "CAIB document" with CAB or CTF followed by seven to eleven digits, such as CAB001-0010, refer to a document in the Columbia Accident Investigation Board database maintained by the Department of Justice and archived at the National Archives.

1 "And stunningly, in as much as this was tragic and horrific through a loss of seven very important lives, it is amazing that there were no other collateral damage happened as a result of it. No one else was injured. All of the claims have been very, very minor in dealing with these issues." NASA Administrator Sean O'Keefe, testimony before the United States Senate Committee on Commerce, Science, and Transportation, May 14, 2003.

2 An intensive search of over a million acres in Texas and Louisiana recovered 83,900 pieces of *Columbia* debris weighing a total of 84,900 pounds. (Over 700,000 acres were searched on foot, and 1.6 million acres were searched with aircraft.) The latitude and longitude was recorded for more than 75,000 of these pieces. The majority of the recovered items were no larger than 0.5 square feet. More than 40,000 items could not be positively identified but were classified as unknown tile, metal, composite, plastic, fabric, etc. Details about the debris reconstruction and recovery effort are provided in Appendix E.5, S. Altemis, J. Cowart, W. Woodworth, "STS-107 Columbia Reconstruction Report," NSTS-60501, June 30, 2003. CAIB document CTF076-20302182.

3 The precise probability is uncertain due to many factors, such as the amount of debris that burned up during re-entry, and the fraction of the population that was outdoors when the *Columbia* accident occurred.

4 "User's Guide for Object Reentry Survival Analysis Tool (ORSAT), Version 5.0, Volume I-Methodology, Input Description, and Results," JSC-28742, July 1999; W. Alior, "What Can We Learn From Recovered Debris," Aerospace Corp, briefing presented to CAIB, on March 13, 2003.

5 "Reentry Survivability Analysis of Delta IV Launch Vehicle Upper Stage," JSC-29775, June 2002.

6 Analysis of the recovered debris indicates that relatively few pieces posed a threat to people indoors. See Appendix D.16.

7 Detailed information about individual fragments, including weight in most cases, was not available for the study. Therefore, some engineering discretion was needed to develop models of individual weights, dimensions, aerodynamic characteristics, and conditions of impact. This lack of information increases uncertainty in the accuracy of the final results. The study should be revisited after the fragment data has been fully characterized.

8 K.M. Thompson, R.F. Rabouw, and R.M. Cooke, "The Risk of Groundling Fatalities from Unintentional Airplane Crashes," *Risk Analysis*, Vol. 21, No. 6, 2001.

9 Ibid.

10 The civil aviation study indicates that the risk to groundlings is significantly higher in the vicinity of an airport. The average annual risk of fatality within 0.2 miles of a busy (top 100) airport is about 1 in a million.

11 Thompson, "The Risk of Groundling Fatalities;" Code of Federal Regulations (CFR) 14 CFR Part 415, 415, and 417, "Licensing and Safety Requirements for Launch: Proposed Rule," *Federal Register* Vol. 67, No. 146, July 30, 2002, p. 49495.

12 Code of Federal Regulations (CFR) 14 CFR Part 415 Launch License, *Federal Register* Vol. 64, No. 76, April 21, 1999; Range Commanders Council Standard 321-02, "Common Risk Criteria for National Test Ranges," published by the Secretariat of the RCC U.S. Army White Sands Missile Range, NM 88002-5110, June 2002; "Mitigation of Orbital Debris," Notice of Proposed Rulemaking by the Federal Communications Commission, FCC 02-80, *Federal Register* Vol. 67, No. 86, Friday, May 3, 2002.

13 Air Force launch safety standards define a Hazardous Launch Area, a controlled surface area and airspace, where individual risk of serious injury from a launch vehicle malfunction during the early phase of flight exceeds one in a million. Only personnel essential to the launch operation are permitted in this area. "Eastern and Western Range Requirements 127-1," March 1995, pp. 1-12 and Fig. 1-6.

14 Code of Federal Regulations (CFR) 14 CFR Part 431, Launch and Reentry of a Reusable Launch Vehicle, Section 35 paragraphs (a) and (b), *Federal Register* Vol. 65, No. 182, September 19, 2000, p. 56660.

15 "Reentry Survivability Analysis of Delta IV Launch Vehicle Upper Stage," JSC-29775, June 2002.

16 M. Tobin, "Range Safety Risk Assessments For Kennedy Space Center," October 2002. CAIB document CTF059-22802288; "Space Shuttle Program Requirements Document," NSTS-07700, Vol. I, change no. 76, Section 5-1. CAIB document CAB024-04120475.

17 Here, ascent refers to (1) the Orbiter from liftoff to Main Engine Cut Off (MECO), (2) the Solid Rocket Boosters from liftoff to splashdown, and (3) the External Tank from liftoff to splashdown.

18 Pete Cadden, "Shuttle Launch Area Debris Risk," October 2002. CAIB document CTF059-22682279.

19 See Dennis R. Jenkins, *Space Shuttle: The History of the National Space Transportation System – The First 100 Missions* (Cape Canaveral, FL, Specialty Press, 2001), pp. 205-212 for a complete description of the Approach and Landing Tests and other testing conducted with *Enterprise*.

20 *Report of the Presidential Commission on the Space Shuttle Challenger Accident* (Washington: Government Printing Office, 1986).

21 The pre-declared time period or number of missions over which the system is expected to operate without major redesign or redefinition.

22 "A crew escape system shall be provided on Earth to Orbit vehicles for safe crew extraction and recovery from in-flight failures across the flight envelope from pre-launch to landing. The escape system shall have a probability of successful crew return of 0.99."

23 *Report of the Aerospace Safety Advisory Panel Annual Report for 2002*, (Washington: Government Printing Office, March 2002). CAIB document CTF014-25882645.

24 Charlie Abner, "KSC Processing Review Team Final Summary," June 16, 2003. CAIB document CTF063-11801276.

25 Julie Kramer, et al., "Minutes from CAIB / Engineering Meeting to Discuss CAIB Action / Request for Information B1-000193," April 24, 2003. CAIB document CTF042-00930095.