LESSONS LEARNED -

THE COLUMBIA SPACE SHUTTLE ACCIDENT

by

Eric Davey
Crew Systems Solutions
Deep River, Ontario, K0J 1P0

Bryan Patterson
Human Factors Practical
Dipper Harbour, New Brunswick, E0G 2H0

ABSTRACT

On 2003 February 01, the Columbia space shuttle broke apart during re-entry with the loss of all crew-members. An accident investigation board undertook a comprehensive examination of the spacecraft design, performance, and NASA design and operational practices to uncover direct and contributory accident causal factors; and recommend the improvements required for return of the shuttle program to flight status.

This paper will summarize the investigative approach taken, the findings and recommendations that resulted, and the lessons of relevance to the nuclear industry. The paper will also outline a suggested 'road-map' for deriving the main lessons learned from the full board report.

BACKGROUND

The Columbia space shuttle was the oldest and most flown spacecraft in the NASA space shuttle fleet. Prior to its destruction during re-entry on the 113th program mission, Columbia had been successfully launched and recovered on 27 previous missions spanning 22 years, and providing many American and international astronauts with weeks of spaceflight experience [1].

Columbia was the second shuttle spacecraft destroyed during an in-flight accident with the consequent loss of the flight crew. The Challenger shuttle was destroyed during launch on the 25th shuttle mission on 1986 January 28th.

During the shuttle program, substantial changes in political direction, program resources, work organization, individual mission objectives, and technology application have taken place. This created a complex engineering design, project management, and operational environment of ongoing and overlapping changes that have challenged the abilities of program staff to manage shuttle operations. The destruction of two spacecraft on missions 17 years apart from differing physical causes, each with observable departures from the reference design performance on previous flights, points to longstanding systemic breakdowns in organizational practices important to the preservation of flight safety.

The objective of this paper is to summarize lessons from the NASA Columbia accident experience that may be of relevance to the preservation of safe operations in the nuclear industry. In today's world, no industry can afford to learn and improve just from their own operational and accident experience. Taking advantage of the lessons learned in other work domains can go a long way to minimizing the potential for inadvertently allowing the conditions that enable accidents within one's own industry domain to occur.

INVESTIGATION & MANDATE

The Columbia accident investigation Board was convened within hours of the spacecraft destruction using established response procedures developed following the Challenger accident in 1986. The Board consisted of 13 members comprising expertise and affiliations primarily external to NASA. Over the course of the seven-month investigation, the Board was supported by a team of 120 investigators and 400 NASA engineers.

The mandate assigned was to identify the accident causation and recommend improvements necessary to return the program to flight status with reduced risk of future shuttle losses.

APPROACH

In its work, the Board undertook a broad interpretation of its mandate. The Board members were guided by the belief that the accident was not the result of a single anomalous, random event but likely had causal precursors originating from several aspects of vehicle design, operations, work practices and organizational culture. Consequently, the Board undertook a comprehensive examination of NASA history, organizational aspects, budgetary constraints and decision-making over the lifetime of the shuttle program in addition to its direct investigation of the immediate physical factors that led to Columbia breakup on re-entry.

FINDINGS

The Board grouped their investigative findings into three categories:

- The physical failures that directly led to the Columbia's destruction,
- Underlying weaknesses in organization, criteria and work practices that create pathways for major accidents to occur, and
- Other significant observations concerning deficiencies unrelated to the Columbia accident that if uncorrected could contribute to future shuttle losses.

Physical Failures

The Board used a number of investigative techniques to determine the physical accident causation factors. The investigation had two areas of emphasis:

- First, understanding why the shuttle broke-up on re-entry, and

- Second, understanding what component, work process, organizational, or cultural failures provided the conditions for re-entry mission failure and how these individual failures occurred.

Analysis of telemetry, control system behaviour, re-entry trajectory, ground-based imagery, debris dispersal, wreckage condition, and simulation were used to independently confirm that a breach in the thermal tiles of the leading edge of the left wing occurred. This breach allowed superheated air to penetrate the wing interior, progressively melt, and weaken the aluminum structure. The wing structure failed when normal re-entry loading exceeded the diminishing structural strength resulting in wing failure, consequent loss of vehicle control, and resultant breakup of the shuttle due to hypersonic aerodynamic forces.

Launch video imagery, simulation, radar tracking of the shuttle during orbit, and physical impact tests were used to confirm that foam shedding from the external tank and impacting the left wing leading edge during launch was the cause of a breach in one or more tiles of the Thermal Protection System.

Underlying Program Weaknesses

Five factors led to significant changes in shuttle program operations, staffing and safety emphasis over the past ten years:

- A 40% reduction in annual budget by 1994 from peak 1991 levels,
- Characterization of the shuttle as reliable, mature and thus an operational versus developmental system,
- Privatization of shuttle maintenance, planning, flight operations and staff training,
- Commitment to commercial/political launch/delivery schedules in support of the assembly of the International Space Station, and
- Receding timeframes and commitment for shuttle replacement.

When combined, these and other factors introduced substantial program management challenge and complexity, resulting in impacts in several areas of shuttle program operations.

In the examination of shuttle operations the Board identified a number of underlying work process, organizational, and cultural weaknesses. What was particularly disturbing was that several of the same weaknesses that were identified during the Challenger accident investigation, and were presumably corrected, had re-established within the organization.
Some of key program weaknesses cited by the Board included:

- Resistance to External Suggestions for Change

  The NASA operational culture had developed at a time when the country depended on the organization to win a 'cold-war' race to the moon and was provided almost unconditionally with the resources to do so. The successes of the Mercury, Gemini, and Apollo missions created an internal reliance in the belief that any problem was solvable by the organization. Consequently, when difficulties occurred, external viewpoints or suggestions for change were often discounted and resisted.

- Loss of Safety Emphasis and Independence

  The functions of the office of Safety and Mission Assurance in providing independent safety oversight of all aspects of shuttle operations were dispersed into the shuttle engineering and operating organization and resourced at reduced staff levels. Aspects of shuttle operations critical to flight safety such as maintenance, training and flight operations decision-making were privatized to contractors. This reduced overall safety oversight, effectiveness, and independence.

- Continued Operation with Performance Non-Conformances

  Foam shedding from the external tank during launch was a common and recognized occurrence even though the engineering performance requirement was for no foam loss and the tiles of the Thermal Protection System initially had no impact resistance requirement. The Board found foam loss had occurred on 80% of the 79 launches for which video records were available. After twenty years of shuttle operations, NASA and contractors had no understanding of foam shedding mechanisms and characterization of impact risk, had not undertaken any corrective actions, and continued to conduct flight operations with this repeated performance non-conformance. The success of repeated missions with this performance non-conformance built a false sense of no undue risk from non-conformance that contributed to safety complacency.

- Operation with Equipment Beyond Specified Service Life

  As the first of the shuttle fleet, the Columbia was 22 years old. For a variety of reasons, the Board found several aspects of Columbia equipment being used beyond its specified service life. For example, Columbia had been outfitted with additional instrumentation to collect operational data for validating conditions experienced during mission operations. After 22 years of use, the majority of this instrumentation had been in service twice as long as its specified service life of 10 years and some sensors or wiring had failed and not been replaced. Of the 181 wing sensors, 55 had failed or were producing questionable readings prior to Columbia's last mission.

- Organizational Barriers to Communication and Problem Resolution

  The potential for damage to shuttle wing tiles was identified on the second day of the flight following review of launch imagery. Several groups within NASA and the contractor community were alerted to the concerns, including the Mission Management Team. Over the two week period while the shuttle was in orbit following launch, repeated requests for ground-based shuttle imagery to confirm tile integrity or damage were resisted and blocked by senior managers as unwarranted. In effect, the debris impact concerns at the engineering level were discounted by mission managers. Support for exploring flight and crew recovery options was also denied as unnecessary.

- Biased Decision-making

  Managers resisted new information that challenged achievement of program goals and previous mission decisions. There was a reluctance to re-examine the basis for former decisions in light of new information. In fact, the opposite occurred, new information was inaccurately assumed or cast into the range of data on which former decisions were based.

<u>Other Significant Deficiencies</u>

During its investigation, the Board uncovered several additional significant deficiencies that were unrelated to the accident but if uncorrected could lead to future shuttle accidents. Key findings in this category included:

- Leadership/Managerial Training

  The Board found managers at many levels in NASA had been promoted into positions without formal training to prepare them for roles of increased responsibility. While a number of in-house leadership and managerial development training programs were available, their use was variable across the organization. This provided opportunities for inconsistency in leadership and decision-making practices that could impact flight safety.

- Quality Assurance Program Effectiveness

  The Board found a comprehensive quality program definition, but compromised day-to-day implementation, resulting in weak effectiveness. Since inception, the number of quality checks and subsequent effort had been reduced by 80% as the organization downsized. The current rejection rate on quality checks was found to be unrealistically low (i.e., 0.014%). Too many discoveries of important non-conformances were routinely being identified outside the quality inspection process or on post-flight examination.

- Major Maintenance Intervals

NASA conducts routine inspection and maintenance following each shuttle flight. More extensive maintenance and equipment updates are undertaken following eight missions and remove a shuttle from service for 6 to 20 months. The Board found NASA considering extension of the major maintenance interval to 12 missions to meet mission frequency needs. This is counter to the norm of reducing service intervals and increasing inspection frequency as systems age.

- Documentation

  The Board identified major deficiencies with shuttle engineering documentation and maintenance records. Engineering drawings were found with inaccuracies, out-of-date information, lack of rationale justifying changes, and were difficult to access in a timely fashion.

  A review of maintenance records for several flights prior to Columbia's last flight, identified several hundred instances where documented discrepancies were accepted in spite of up to three levels of checking oversight.

RECOMMENDATIONS

The Board developed 29 recommendations with 15 identified as requiring completion prior to return to flight status for the program. The recommendations developed, included technical, organizational, and cultural improvements. Key recommendations in each of these areas were:

<u>Technical</u>

- Debris Prevention - Eliminate foam shedding from the External Tank Thermal Protection System.

- Shuttle Hardening - Increase the shuttle's ability to resist damage from debris impact via improving the impact resistance of thermal tiles.

- Orbital Inspection/Repair - Provide a capability for inspection of shuttle thermal tiles following launch, and conducting emergency repairs when necessary.

- Tile Characterization - Implement a comprehensive non-destructive means of characterizing the structural integrity of key shuttle tiles between missions.

- Impact Modeling - Develop and validate computer models that predict Thermal Protection System damage from debris impacts from a variety of sources.

- Imaging - Upgrade the capabilities to image the shuttle during the launch phase and make imaging of the shuttle while on orbit a standard operational requirement and practice.

- Instrumentation - Expand the shuttle instrumentation capability to include engineering performance and vehicle health information for all shuttles.

Organizational

- Engineering Authority - Establish an independent technical engineering authority responsible for all technical requirements and granting of waivers to them, and independently verifying launch readiness.

- Safety Management - Re-establish the Office of Safety and Mission Assurance with authority for safety over the entire Shuttle Program and independently resource it.

- Integration Authority - Establish one organizational authority responsible for integration of all program elements.

- Re-certification - Conduct a comprehensive vehicle re-certification at the material, component, subsystem and system levels prior to shuttle flight operations beyond 2010.

Cultural

- Scheduling - Adopt a flight schedule that is consistent with available resources and safety preservation.

- Terms - Re-adopt the industry standard definition for 'foreign object debris' and eliminate use of any internally defined alternatives.

- Documentation - Update all shuttle engineering drawings to ensure that they are current, and photograph all critical subsystems whose implementation differs from engineering drawings.

- Contingency Training - Undertake routine simulation training of mission challenges for the Mission Management Team that involve practice in interaction with support organizations and contractors.

LESSONS APPLICABLE TO THE NUCLEAR INDUSTRY

Several of the lessons learned in the Columbia accident investigation may be relevant for consideration to the nuclear industry to reduce incident risk potential. Examples include:

Corporate Support

- Balancing Operational Commitments and Resources - Ensure realistic re-alignment of program expectations consistent with resource capabilities occurs when program objectives and funding change.

- Training - Provide additional training and support to new and continuing staff until they demonstrate adequate capabilities and understanding to perform new or expanded responsibilities, as the corporate memory and experience is reduced through senior staff retirements or downsizing.

- Quality Assurance and Quality Control - Staff and conduct these programs consistent with their objectives and importance in supporting the nuclear mission. Frequently assess program conduct to confirm effectiveness.

- External Suggestions for Change - Remain open and pay attention to external suggestions for change. Treat all suggestions for improvements as important. Each adopted improvement recommendation provides an opportunity to increase defences to incident occurrence.

Operations

- Safety Decision-making - Ensure operational decisions are made on the basis that safety has been assured, rather than assuming safety and requiring demonstration of unsafe conditions to preclude continuing operations.

- Performance Characterization - Avoid reliance on limited or dated engineering and performance test data to characterize the envelope of safe operations.

- Acceptance of Performance Deviances - Avoid the normalization of repetitive performance deviances and subsequent discounting of safety significance and incident causation potential.

- Communication in Mission Support - Encourage openness to examination of new points of view, communication of risk significance, and the consideration and characterization of option alternatives.

Technical Support

- Documentation - Maintain engineering drawings up-to-date and document the history of rationale for initial design decisions and changes.

- Maintenance Intervals - Determine maintenance intervals on the basis of current assessments of equipment condition and performance. While long production runs between maintenance intervals are economically desirable; service intervals will likely shorten as equipment ages.

- Service Life - Periodically assess and confirm service life expectations using both performance and health information. Refurbish or replace equipment before end-of-service life is reached.

CONCLUSION

The Columbia shuttle was destroyed due a breach in the protective thermal tiles that allowed superheated re-entry gases to penetrate, overheat, and weaken the interior of the wing structure at a point in the mission of maximum dynamic loading. The damage to the thermal tiles was caused by impact with foam shed from the External Fuel Tank during launch. Underlying organizational weaknesses allowed a number of conditions to develop and impact program operations for many years that enabled the accident causation chain of events to occur. Like the Challenger shuttle loss 17 years previous, this was a preventable accident.

All industries where preservation of safety is a paramount aspect of operations have a need to continually learn from the experience of others. The investigation of the Columbia loss offers a rich basis for re-examination of the adequacy of our own practices, and re-commitment to improvement initiatives where warranted.

REFERENCES

1. Columbia Accident Investigation Board. NASA reports Volumes 1 and 2, 2003 August.

ADDENDUM

The full board report spans a main report of 11 chapters and 3 appendices, and 5 supplementary reports. The full report is available to view or download at www.caib.us/.

For readers who would like examine the Board findings and recommendations in more detail, the authors suggest the following specific readings:

- Shuttle Program Background:

    - Chapter 1 - Beginnings of the Shuttle Program
    - Chapter 5 - Shuttle Program Operation Following the Challenger Accident

- Investigative Findings:

    - Chapter 3 - Physical Causes of Accident
    - Chapter 7 - Organizational Causes of Accident
    - Chapter 8 – History Causes of Accident
    - Chapter 10 - Other Significant Observations

- Recommendations:
  - Chapter 11 - Corrective Actions Required