

Creating Foresight: How Resilience Engineering Can Transform NASA's Approach to Risky Decision Making

David Woods, Professor
Institute for Ergonomics
The Ohio State University

Testimony on
The Future of NASA
for

Committee on Commerce, Science and Transportation, John McCain, Chair
October 29, 2003

Introduction

To look forward and envision NASA as a high reliability organization, we need first to look back with clarity unobscured by hindsight bias. Admiral Gehman and the Columbia Accident Investigation Board (CAIB) found the hole in the wing was produced not simply by debris, but by holes in organizational decision making. The factors that produced the holes in decision making are not unique to today's NASA or limited to the Shuttle program, but are generic vulnerabilities that have contributed to other failures and tragedies across other complex industrial settings.

For 24 years my research has examined the intersection of human decision making, computers, and high risk complex situations from nuclear power emergencies to highly automated cockpits to medical decision making, and specifically has included studies of how space mission operation centers handle anomalies.

CAIB's investigation shows how NASA failed to balance safety risks with intense production pressure. As a result, this accident matches a classic pattern—a drift toward failure as defenses erode in the face of production pressure. When this pattern is combined with a fragmented problem solving process that is missing cross checks and unable to see the big picture, the result is an organization that cannot see its own blind spots about risks. Further, NASA was unable to revise its assessment of the risks it faced and the effectiveness of its countermeasures against those risks as new evidence accumulated. What makes safety/production tradeoffs so insidious is that evidence of risks become invisible to people working hard to produce under pressure so that safety margins erodes over time.

As an organizational accident Columbia shows the need for organizations to monitor their own practices and decision processes to detect when they are beginning to drift toward safety boundaries. The critical role for the safety group within the organization is to monitor the organization itself—to measure organizational risk—the risk that the organization is operating nearer to safety boundaries than it realizes.

In studying tragedies such as Columbia, we have also found that failure creates windows for rapid learning and improvement in organizations. Seizing the opportunity to learn is the responsibility leaders owe to the people and families whose sacrifice and suffering

was required to make the holes in the organization's decision making visible to all. NASA and Congress now have the opportunity to transform the culture and operation of all of NASA (Shuttle, ISS, and space science missions), and by example transform other high risk organizations.

The target is to help organizations maintain high safety despite production pressure. This is the topic of the newly emerging field of **Resilience Engineering** which uses the insights from research on failures in complex systems, including organizational contributors to risk, and the factors that affect human performance to provide practical systems engineering tools to manage risk proactively.

NASA can use the emerging techniques of Resilience Engineering to balance the competing demands for very high safety with real time pressures for efficiency and production. By following the recommendations of the CAIB to thoroughly re-design its safety organization and provide for an independent technical authority, NASA can provide a model for high reliability organizational decision making.

The Trouble with Hindsight

The past seems incredible, the future implausible.¹

Hindsight bias is a psychological effect that leads people to misinterpret the conclusions of accident investigations.² Often the first question people ask about the decision making leading up to an accident such as Columbia is, "why did NASA continue flying the Shuttle with a known problem...?" (The known problem refers to the dangers of debris striking and damaging the Shuttle wing during takeoff which the CAIB identified as the physical cause of the accident.)

As soon as the question is posed in this way, it is easy to be trapped into oversimplifying the situation and the uncertainties involved before the outcome is

¹ Woods, D.D. and Cook, R.I. (2002). Nine Steps to Move Forward from Error. *Cognition, Technology, and Work*, 4(2): 137-144.

² The hindsight bias is a well reproduced research finding relevant to accident analysis and reactions to failure. Knowledge of outcome biases our judgment about the processes that led up to that outcome.

In the typical study, two groups of judges are asked to evaluate the performance of an individual or team. Both groups are shown the same behavior; the only difference is that one group of judges are told the episode ended in a poor outcome; while other groups of judges are told that the outcome was successful or neutral. Judges in the group told of the negative outcome consistently assess the performance of humans in the story as being flawed in contrast with the group told that the outcome was successful. Surprisingly, this hindsight bias is present even if the judges are told beforehand that the outcome knowledge may influence their judgment.

Hindsight is not foresight. After an accident, we know all of the critical information and knowledge needed to understand what happened. But that knowledge is not available to the participants before the fact. In looking back we tend to oversimplify the situation the actual practitioners faced, and this tends to block our ability to see the deeper story behind the label human error.

known.³ After-the-fact “the past seems incredible,” hence NASA managers sound irrational or negligent in their approach to obvious risks. However, before any accident has occurred and while the organization is under pressure to meet schedule or increase efficiency, potential warning flags are overlooked or re-interpreted since the potential “future looks implausible.” For example, the signs of Shuttle tile damage became an issue of orbiter turn around time and not a flight risk.

Because it is difficult to disregard “20/20 hindsight”, it is easy to play the classic blame game, define a “bad” organization as the culprit, and stop. When this occurs, the same difficulties that led to the Columbia accident will go unrecognized in other programs and in other organizations.

The CAIB worked hard to overcome hindsight bias and uncover the breakdown in organizational decision making that led to the accident. All organizations can misbalance safety risks with pressure for efficiency. It is difficult to sacrifice today’s real production goals to consider uncertain evidence of possible future risks. The heart of the difficulty is that it is most critical to invest resources to follow up on potential safety risks when the organization is least able to afford the diversion of resources due to pressure for efficiency or throughput.

Five General Patterns Present in Columbia

The CAIB report identifies a variety of contributors to the accident. These factors have been seen before in other accidents.⁴ Focusing on the general patterns present in this particular accident helps guide the process of envisioning the future of NASA as a high reliability organization.

Classic patterns also seen in other accidents and research results include:

- Drift toward failure as defenses erode in the face of production pressure.
- An organization that takes past success as a reason for confidence instead of investing in anticipating the changing potential for failure.
- Fragmented problem solving process that clouds the big picture.
- Failure to revise assessments as new evidence accumulates.
- Breakdowns at the boundaries of organizational units that impedes communication and coordination.

1. The basic classic pattern in this accident is—*Drift toward failure as defenses erode in the face of production pressure.*

My colleague, Erik Hollnagel in 2002, captured the heart of the Columbia accident when he commented on other accidents:

³ See S. Dekker’s *The Field Guide to Human Error Investigations*. Ashgate, 2002.

⁴ Hollnagel, E. (1993). *Human Reliability Analysis: Context and Control*. London: Academic Press.

If anything is unreasonable, it is the requirement to be both efficient and thorough at the same time – or rather to be thorough when with hindsight it was wrong to be efficient.

Hindsight bias, by oversimplifying the situation people face before outcome is known, often hides tradeoffs between multiple goals. The analysis in the CAIB report provides the general context of a tighter squeeze on production goals creating strong incentives to downplay schedule disruptions. With shrinking time/resources available, safety margins were likewise shrinking in ways which the organization couldn't see.

Goal tradeoffs often proceed gradually as pressure leads to a narrowing focus on some goals while obscuring the tradeoff with other goals. This process usually happens when acute goals like production/efficiency take precedence over chronic goals like safety. If uncertain “warning” signs always lead to sacrifices on schedule and efficiency, how can any organization operate within reasonable parameters or meet stakeholder demands?

The paradox of production/safety conflicts is: safety investments are most important when least affordable. It is precisely at points of intensifying production pressure that extra investments for managing safety risks are most critical.

The NASA of the future will need a means to recognize when the side effects of production pressure may be increasing safety risks and under those circumstances develop a means to add investments to safety issues at the very time when the organization is most squeezed on resources and time.

2. Another general pattern identified in Columbia is that *an organization takes past success as a reason for confidence instead of digging deeper to see underlying risks.*

One component in the drift process is the interpretation of past “success”. The absence of failure is taken as positive indication that hazards are not present or that countermeasures are effective. An organization usually is unable to change its model of **itself** unless and until overwhelming evidence accumulates that demands revising the model. This is a guarantee that the organization will tend to learn late, that is, revise its model of risk only after serious events occur. An effective safety organization assumes its model of risks and countermeasures is fragile and seeks out evidence to revise and update this model.⁵ To seek out such information means the organization is willing to expose its blemishes.

During the drift toward failure leading to the Columbia accident a mis-assessment took hold that resisted revision (that is, the mis-assessment that foam strikes pose only a maintenance and not a risk to orbiter safety). It is not simply that the assessment was wrong, but the inability to re-evaluate the assessment and re-examine evidence about risks is troubling.

⁵ Rochlin, G. I. (1999). Safe operation as a social construct. *Ergonomics*, 42 (11), 1549-1560.

The missed opportunities to revise and update the organization's model of the riskiness of foam events seem to be consistent with what I have found in other cases of failure of foresight. I have described this discounting of evidence as "distancing through differencing" whereby those reviewing new evidence or incidents focus on differences, real and imagined, between the place, people, organization and circumstances where an incident happens and their own context. By focusing on the differences, people see no lessons for their own operation and practices or only narrow well bounded responses.

Ominously, this *distancing through differencing* that occurred throughout the build up to the final Columbia mission can be repeated in the future as organizations and groups look at the analysis and lessons from this accident and the CAIB report. Others in the future can easily look at the CAIB conclusions and deny their relevance to their situation by emphasizing differences (e.g., my technical topic is different, my managers are different, we are more dedicated and careful about safety, we have already addressed that specific deficiency).

One general principle to promote organizational learning in NASA is—Do not discard other events because they appear on the surface to be dissimilar. Rather, every event, no matter how dissimilar on the surface, contains information about underlying general patterns that help create foresight about potential risks before failure or harm occurs.

The NASA of the future will have a safety organization that question NASA's own model of the risks it faces and the countermeasures deployed. Such review and re-assessment will help NASA find places where it has underestimated the potential for trouble and revise its approach to create safety.

3. Another general pattern identified in Columbia is a *fragmented problem solving process that clouds the big picture.*

During Columbia there was a fragmented view of what was known about the strike and its potential implications. There was no place or person who had a complete and coherent view of the analysis of the foam strike event including the gaps and uncertainties in the data or analysis to that point. It is striking that people used what looked like technical analyses to justify previously reached conclusions, instead of using technical analyses *to test tentative hypotheses* (e.g., CAIB report, p. 126 1st column).

People were making decisions about what did or did not pose a risk on very shaky or absent technical data and analysis, and critically, *they couldn't see their decisions rested on shaky grounds* (e.g., the memos on p. 141, 142 of the CAIB report illustrate the shallow, off hand assessments posing for and substituting for careful analysis).

The breakdown or absence of cross-checks is also striking. Cross checks on the rationale for decisions is a critical part of good organizational decision making. Yet no cross checks were in place to detect, question or challenge the specific flaws in the rationale, and *no one noted that cross-checks were missing.*

There are examples of organizations that avoid this fragmentation problem. Ironically, one of them is teamwork in NASA's own Mission Control which has a successful record

of analyzing and handling anomalies.⁶ In particular, the Flight Director and his or her team practice identifying and handling anomalies through simulated situations. Note that shrinking budgets lead to pressure to reduce training investments (the amount of practice, the quality of the simulated situations, and the number or breadth of people who go through the simulations sessions can all decline).

The fragmentation of problem solving also illustrates Karl Weick's point⁷ about how important it is that high reliability organizations exhibit a "deference to expertise", "reluctance to simplify interpretations", and "preoccupation with potential for failure" none of which were in operation in NASA's organizational decision making leading up to and during Columbia.

The NASA of the future will have a safety organization that ensures that adequate technical grounds are established and used in organizational decision making.

To accomplish this for NASA, the safety organization will need to define the kinds of anomalies to be practiced as well as who should participate in those simulation training sessions. The value of such training depends critically on designing a diverse set of anomalous scenarios with detailed attention to how they unfold. By monitoring performance in these simulated training cases, the safety personnel are able to assess the quality of organizational decision making.

4. The fourth pattern in Columbia is a *Failure to revise assessments as new evidence accumulates.*

I first studied this pattern in nuclear power emergencies 20 plus years ago.⁸ What was interesting in the data then was how difficult it is to revise a mis-assessment or to revise a once plausible assessment as new evidence comes in. This finding has been reinforced in subsequent studies in different settings.

The crux is to notice the information that changes past models of risk and calls into question the effectiveness of previous risk reduction actions, without having to wait for complete clear cut evidence. If revision only occurs when evidence is overwhelming, there is a grave risk of an organization acting too risky and finding out only from near misses, serious incidents, or even actual harm. Instead, the practice of revising assessments of risks needs to be an ongoing process. In this process of continuing re-

⁶ For example, see: E.S. Patterson, J.C. Watts-Perotti, D.D. Woods. Voice Loops as Coordination Aids in Space Shuttle Mission Control. *Computer Supported Cooperative Work*, 8, 353–371, 1999. J.C. Watts, D.D. Woods, E.S. Patterson. Functionally Distributed Coordination during Anomaly Response in Space Shuttle Mission Control. *Proceedings of Human Interaction with Complex Systems*, IEEE Computer Society Press, Los Alamitos, CA, 1996. Patterson, E.S., and Woods, D.D. (2001). Shift changes, updates, and the on-call model in space shuttle mission control. *Computer Supported Cooperative Work*, 10(3-4), 317-346.

⁷ Weick, K. E., Sutcliffe, K. M. and Obstfeld, D. (1999). Organizing for High Reliability: Processes of Collective Mindfulness. *Research in Organizational Behavior*, Volume 21, pp. 81-123.

⁸ D.D. Woods, J. O'Brien, and L.F. Hanes. Human factors challenges in process control: The case of nuclear power plants. In G. Salvendy, editor, *Handbook of Human Factors/Ergonomics*, Wiley, New York, 1987.

evaluation, the working assumption is that risks are changing or evidence of risks has been missed.

Research consistently shows that revising assessments successfully requires a new way of looking at previous facts. We provide this “**fresh**” view:

- (a) by bringing in people new to the situation
- (b) through interactions across diverse groups with diverse knowledge and tools,
- (c) through new visualizations which capture the big picture and re-organize data into different perspectives.

One constructive action is to develop the collaborative inter-changes that generate fresh points of view or that produce challenges to basic assumptions. This cross checking process is an important part of how NASA mission control responds to anomalies. One can also capture and display indicators of safety margin to help people see when circumstances or organizational decisions are pushing the system closer to the edge of the safety envelope.

What is so disappointing about NASA’s organizational decision making is that the correct diagnosis of production/safety tradeoffs and useful recommendations for organizational change were noted in 2000. The Mars Climate Orbiter report of March 13, 2000 clearly depicts how the pressure for production and to be ‘better’ on several dimensions led to management accepting riskier and riskier decisions. This report recommended many organizational changes similar to the CAIB. A slow and weak response to the previous independent board report was a missed opportunity to improve organizational decision making in NASA.

The NASA of the future will have a safety organization that provides “fresh” views on risks to help NASA see its own blind spots and question its conventional assumptions about safety risks.

5. Finally, the Columbia accident brings to the fore another pattern: *Breakdowns at the boundaries of organizational units.*

The CAIB notes how a kind of catch 22 was operating in which the people charged to analyze the anomaly were unable to generate any definitive traction and in which the management was trapped in a stance shaped by production pressure that views such events as turn around issues. This effect of an ‘*anomaly in limbo*’ seems to emerge only at boundaries of different organizations that do not have mechanisms for constructive interplay. It is here that we see the operation of the generalization that in risky judgments we have to defer to those with technical expertise (and the necessity to set up a problem solving process that engages those practiced at recognizing anomalies in the event).

This pattern points to the need for mechanisms that create effective overlap across different organizational units and to avoid simply staying inside the chain of command mentality (though such overlap can be seen as inefficient when the organization is under severe cost pressure).

The NASA of the future will have a safety organization with the technical expertise and authority to enhance coordination across the normal chain of command.

Resilience Engineering

Resilience Engineering is built on insights derived from the above five patterns. Resilience Engineering is concerned with assessing organizational risk, that is the risk that holes in organizational decision making will produce unrecognized drift toward failure boundaries.⁹

While assessing technical hazards is one kind of input into Resilience Engineering, the goal is to monitor organizational decision making. For example, Resilience Engineering would monitor evidence that effective cross checks are well-integrated when risky decisions are made or would serve as a check on how well the organization is practicing the handling of simulated anomalies (what kind of anomalies, who is involved in making decisions).

Other dimensions of organizational risk include the commitment of the management to balance the acute pressures of production with the chronic pressures of protection. Their willingness to invest in safety and to allocate resources to safety improvement in a timely, proactive manner, despite pressures on production and efficiency, are key factors in ensuring a resilient organization.

The degree to which the reporting of safety concerns and problems is truly open and encouraged provides another significant source of resilience within the organization. Assessing the organization's response to incidents indicates if there is a learning culture or a culture of denial. Other dimensions include:

- Preparedness/Anticipation: is the organization proactive in picking up on evidence of developing problems versus only reacting after problems become significant?
- Opacity/Observability—does the organization monitors safety boundaries and recognize how close it is to 'the edge' in terms of degraded defenses and barriers? To what extent is information about safety concerns widely distributed throughout the organization at all levels versus closely held by a few individuals?
- Flexibility/Stiffness—how does the organization adapt to change, disruptions, and opportunities?

⁹ For initial background on the emergence of resilience engineering see Rasmussen, J. Risk Management, Adaptation, and Design for Safety. In B. Brehmer and N.-E. Sahlin (Eds.) Future Risks and Risk Management. Kluwer Academic, Dordrecht, 1994. Rasmussen, J. (1997). Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science*, 27, 183-213. Reason, J. (2001). Assessing the Resilience of Health Care Systems to the Risk of Patient Mishaps. Carthy, J., de Leval, M. R. and Reason, J. T. (2001). Institutional Resilience in Healthcare Systems. *Quality in Health Care*, 10: 29-32. Weick, K. E. and Sutcliffe, K. M. (2001). *Managing the unexpected : assuring high performance in an age of complexity*. San Francisco : Jossey-Bass. Cook, R. I., Render, M. L. and Woods, D.D. (2000). Gaps in the continuity of care and progress on patient safety. *British Medical Journal*, 320, 791-794, March 18, 2000. Woods, D. D. and Shattuck, L. G. (2000). Distance supervision—local action given the potential for surprise *Cognition, Technology and Work*, 2, 86-96. Leveson, N. G. (in press). A New Accident Model for Engineering Safer Systems. *Safety Science*. Roberts, K.H., Desai, V., and Madsen, P. (in press) Work Life and Resilience in High Reliability Organizations. In E. Kossek and S. Lambert (Eds.) *Work and Life Integration* Mahwah: NJ: Erlbaum.

- Revise/Fixated—how does the organization update its model of vulnerabilities and the effectiveness of countermeasures over time?

The NASA of the future will create a new safety organization and culture that is skilled at the three basics of Resilience Engineering:

- (1) detecting signs of increasing organizational risk, especially when production pressures are intense or increasing;
- (2) having the resources and authority to make extra investments in safety at precisely these times when it appears least affordable;
- (3) having a means to recognize when and where to make targeted investments to control rising signs of organizational risk and re-balance the safety and production tradeoff.

These mechanisms will produce an organization that creates foresight about changing risks before failures occur.

Redesigning NASA for Safety: An Independent, Involved, and Informed Safety Organization

One traditional dilemma for safety organizations is the problem of “cold water and an empty gun.” Safety organizations raise questions which stop progress on production goals—the “cold water.” Yet when line organizations ask for help on how to address the safety concerns, while being responsive to production issues, the safety organization has little to contribute—the “empty gun.” As a result, the safety organization fails to better balance the safety/production tradeoff in the long run. In the short run following a failure, the safety organization is emboldened to raise safety issues, but in the longer run the memory of the previous failure fades, production pressures dominate, and the drift processes operate unchecked (as has happened in NASA before Columbia and appears to be happening again with respect to ISS).

Re-shuffling personnel and re-tuning the existing safety organization does not meet the spirit of the CAIB recommendations. First, a new leadership team well versed in organizational decision making, systems approaches to safety, and human factors in complex systems needs to be assembled and empowered.

Second, the key target for the new safety organization is to monitor and balance the tradeoff of production pressure and risk. To do this the leadership team needs to implement a program for managing organizational risk—detecting emerging ‘holes’ in organizational decision making—based on advancing the techniques of Resilience Engineering.

Third, the new safety organization needs the resources and authority to achieve the three “I’s” of an effective safety organization (independence, involvement, information):

- provide an *independent* voice that challenges conventional assumptions within NASA management,
- constructive *involvement* in targeted but everyday organizational decision making (for example, ownership of technical standards, waiver granting, readiness reviews, and anomaly definition).

- actively generate *information* about how the organization is actually operating, especially to be able to gather accurate information about weaknesses in the organization.

Safety organizations must achieve independence enough to question the normal organizational decision making. At best the relationship between the safety organization and NASA senior management will be one of *constructive tension*. Inevitably, there will be periods where senior management tries to dominate the safety organization. Congress needs to provide the safety organization the tools to resist these predictable episodes by providing funding directly and independent from NASA headquarters. Similarly, to achieve independence, the safety leadership team needs to be chosen and accountable to designees of Congress, not directly to the NASA administrator or NASA headquarters.

Safety organizations must be involved in enough everyday organizational activities to have a finger on the pulse of the organization and to be seen as a constructive part of how NASA balances safety and production goals. This means the new safety organization needs to control a set of resources and the authority to decide how to invest these resources to help line organizations provide high safety while accommodating production goals. For example, the safety organization could decide to invest and develop new anomaly response training programs when it detects holes in organizational decision making processes.

In general, safety organizations risk becoming information limited as they can be shunted aside from real organizational decisions, kept at a distance from the actual work processes, and kept busy tabulating irrelevant counts when their activities are seen as a threat by line management (for example, the ‘cold water’ problem). Independent, involved and informed—these three properties of an effective safety organization are closely connected and mutually reinforcing.

Conclusion

Unfortunately, it sometimes takes tragedies such as Columbia to create windows of opportunity for rapid learning and improvement. It is our responsibility to seize the opportunity created at such cost to lead change. Congress can energize the creation of an independent, involved and informed safety organization for NASA. The NASA of the future can become the model of an organization that escapes a trap where production pressure erodes safety margins.

The future NASA will balance the goals of both high productivity and ultra-high safety given the uncertainty of changing risks and certainty of continued pressure for efficient and high performance. To carry out this dynamic balancing act requires a new safety organization designed and empowered to be independent, involved and informed. The safety organization will use the tools of Resilience Engineering to monitor for “holes” in organizational decision making and to detect when the organization is moving closer to failure boundaries than it is aware. Together these processes will *create foresight* about the changing patterns of risk before failure and harm occurs.

