Book Reviews

Organization at the Limit: Lessons from the *Columbia* Disaster.

William H. Starbuck and Moshe Farjoun, eds. Malden, MA: Blackwell, 2005. 387 pp. $39.95.

On February 1, 2003, seven astronauts died when the space shuttle *Columbia* disintegrated as it reentered the atmosphere. A 1.68-pound piece of insulating foam, which broke off during liftoff, hit the orbiter and left a three-inch crack in its thermal protection system on the left wing. On reentry, superheated air drawn through the crack melted its aluminum structure, and that aerodynamic instability and loss of control shattered the orbiter. Like known troubles with O-rings, which brought down *Challenger* and its seven astronauts on January 28, 1986, on 14 flights since 1981, including *Columbia*'s first, there had been significant damage to the thermal protection system (TPS) or major foam loss. The 13-member *Columbia* Accident Investigation Board (CAIB) released its 248-page report on August 26, 2003, after analyzing evidence supplied by its staff of 120, 400 NASA engineers, and about 25,000 debris searchers. Of its 29 recommendations, the National Aeronautics and Space Administration (NASA) was obliged to complete 15 before shuttle flights could resume.

The 35 authors of the 18 chapters in this volume discuss the board's findings and, inevitably, point to change and stasis over the last 17 years in the social logics of NASA's work systems, in its technical logics of risk assessment, and in the policy logics of executives and politicians. The contributors include social and behavioral scientists, graduate students, engineers, a physician, and NASA consultants, grant recipients, employees, and/or witnesses at the CAIB's public hearings. The volume's aims, its editors say, is to raise questions the board's report did not: "We dissect the human, organizational, and political processes that generated the disaster from more perspectives than the CAIB report" (p. 4). Sean O'Keefe, administrator of NASA at the time of the accident, wrote the Preface.

To situate the authors' concerns, I paraphrase excerpts from the editors' synopsis of the board's report, appearing in part 1, "Introduction." The insulating foam shed during ascent from *Columbia*'s external fuel tank hit one of several reinforced carbon-carbon (RCC) panels located in heat-critical areas of the leading edge of the left wing's thermal protection system. Neither the crew nor ground support teams were aware of the strike until seeing blurred pictures the day after launch. Although some engineers asked for more definitive pictures of the orbiter's condition from the Department of Defense, managers blocked these requests and were unresponsive to others; opportunities for the crew to assess any damage by video also fell by the wayside. Foam had previously damaged ceramic tiles (spread over about 70 percent of a shuttle's exterior) on several flights, but an RCC panel was damaged only once, in 1993. Damage to the thermal protection system (TPS) also occurred only once, in 1997, but NASA's subsequent attempt to prevent shedding was ineffective. Although investigated as an "in-flight" anomaly, managers closed the inquiry, reclassified it as "accepted risk," and designated foam loss a "turnaround" or maintenance issue. After another foam strike in 2002, no further studies took place. Facing an imminent milestone for servicing the International Space Station in early 2004, *Columbia*'s managers were avoiding delays. An after-the-fact rescue and repair scenario revealed that managers assumed that even if a breach were visible, nothing could be done. The CAIB report concludes that NASA has a "broken safety culture," which fostered inadequate flows of safety-related information, too little professional debate, "loose functional integration," and an "informal chain of command." It recommended, among other actions, that independent technical and safety assurance authorities be established and that NASA develop the attributes of a "learning" organization (pp. 11–17).

Showing how the particulars of this complex technology in its various contexts combined to create disaster, each chapter teases out notable preconditions from the report's details and from evidence some authors develop. In part 2, "The Context of the Disaster," Farjoun revisits NASA's history and policies from 1960 to *Columbia* and asks that NASA's leaders sharpen and expand their risk assessment practices, and if flight risk proves too great, consider ending the program as we know it (p. 38). Vaughan discusses the similarity in the contexts of each shuttle disaster, concluding that to help prevent NASA's recurring "slippery slope," social scientists should be asked for their help (pp. 45, 54, 56). Farjoun next provides a close look at "safety drift" between 1995 and the *Columbia* launch to define a "safety failure cycle model" that accounts for variations in learning depending on whether the context is post-failure or during a good run when problems can go unnoticed (pp. 62–63, 77–78). Roberts, Madsen, and Desai observe that "although NASA and its contractors" use various "redundant" safety groups, in this accident the "dependence among [them] eliminates much of the benefit of redundancy." They conclude with an outline of principles for organizing NASA's independent technical authority (pp. 82, 89–95).

In part 3, "Influences on Decision-Making," Ocasio's analysis of NASA's "vocabulary of safety" concludes that while its confusion of usages and meanings was not a "root cause" of the disaster, NASA has never acknowledged the many ambiguities in the operation of this "risky and obsolete technology." Nevertheless, Ocasio finds, the longstanding failure to imagine the consequences of foam loss and strikes is due to "the inherent complexity of the technology, rather than to the vocabulary or the culture" (p. 119). Blount, Waller, and Leroy find that because deadline pressures and its stress dominated managers' attention, their decision-making capabilities degraded (pp. 131–134). In that vein, Buljan and Shapira propose a model of attention allocation between "conflicting safety and time targets" and point to other cognitive processes that narrow managers' perspectives (pp. 145–153).

In part 4, "The Imaging Debate," Weick observes that although top managers' sense-making responses to "streaming inputs" demanded a "flow of negotiations," they did not engage in them (pp. 159–160). Nor did they "rework" their propensity for "rapid compounding" of new information into "abstractions" (categories, labels) about what was happening and needed to happen, which inhibited the search for clearer images during flight (p. 168). Snook and Connor compare *Columbia* with medical and military cases, finding in each a "pattern of structurally induced inaction," largely due to these enterprises' "fragmented" and highly "differentiated" characteristics. They show day by day how those involved became bystanders in the imaging debacle (pp. 191–199). Difficulties in determining the significance of data preoccupy Dunbar and Garud. These begin with NASA's confusion over whether the shuttle is an R&D or operational problem, resolved partly by interpreting data either for "exploration" or for "predictable task performance" during operations, two "organizing modes" often in conflict (pp. 194–208). To head off trouble that often-weak signals herald, Edmondson and her coauthors explore the concept of a "recovery window" to define systemwide preconditions for making timely responses—the window opens whenever someone notices "a risk of consequential failure," which alone allows a "second chance to avoid true failure." This accident reveals two modes of response, one habitual and passive, hence ineffectual, the other seeking new preventive patterns and knowledge (pp. 223–226). Milliken, Lant, and Bridwell-Mitchell, concerned with knowledge distribution, explore how formal and informal power differentials led managers, for whom data had different meanings, to avoid requiring better in-flight images. They propose that NASA develop strategies and processes for "adaptive learning" through conflict resolution or "critical inquiry" (pp. 259–263).

Part 5, "Beyond Explanation," begins with a cross-disciplinary analysis of the shuttle accidents by Leveson and her coauthors. Drawing on control engineering models and social science perspectives, the chapter sketches the many elements of NASA's work systems and makes an extended critique of the extant matrixed system safety group, which is "neither fully independent nor sufficiently influential." Yet, even as they canvass NASA's "parts" and "subsystems" for their roles in "safety assurance," the authors also acknowledge that "we have no accepted way of integrating these components and contexts into a single systems model," hence as yet, no way to move "from accident analysis into design and intervention" (p. 285). A designated and heterogeneous group that keeps its eyes on whatever erodes or narrows safety margins and continually "cross-checks" with others, Woods proposes, is the way to prevent these enterprises from losing the resilience that risk handling demands (p. 304). Woods reanalyzes CAIB evidence as turning points where reevaluations of risk were inadequate or missing (pp. 294–296, 299). In recommendations to increase NASA's effectiveness, Starbuck and Stephenson (a NASA staff member who has led internal teams' reorganization studies) critically revisit the agency's history, structure, outsized goals, and public perceptions. To "succeed in its endeavor to remain relevant, to correct organizational deficiencies, to again set foot on the Moon, and ultimately to explore the outer reaches of the cosmos," they propose that NASA place high priority on, among other changes, a "less mechanistic structure . . . more adaptable to changing environments, and less risk-averse" (p. 322).

In the next-to-last chapter, McDonald, an aeronautical engineer, previous NASA center director, and leader of a Shuttle Independent Assessment Team, finds that its March 2000 report speaks to "the same organizational issues" the CAIB's 2003 report identifies. But his team's recommendations to augment staff and budget and embark on a new safety initiative, "particularly in the inspection and problem resolution area," came to naught in the last several years, especially after changes in agency leadership (p. 339). McDonald relates many authors' findings to his experiences and observations, one being that schedule pressures on *Columbia* began only after the presidential election, when the administration cut staff and budgets and set a milestone for the space station program that "tied the shuttle and the agency's very existence" to a "date which was widely believed to be unachievable from the outset" (p. 345).

After schedule pressure and resource scarcity, perhaps the most ubiquitous precondition most chapters identify is NASA's difficulty in balancing "the contradictory demands of differentiation and integration," given its "size and complexity [which] create coordination and comprehension challenges," the editors declare in their final overview chapter. The "complex matrix organization may have failed to integrate effectively the varied and distributed tasks" of specialists and programs (Farjoun and Starbuck, p. 351). And some authors' most urgent plea for reform is for centralized, influential "safety authorities" independent from programmatic funding and decision making. Both issues, complexity and structure, I suggest, are cut from the same cloth, namely, the "epistemology of engineering," which Bugos (1993, 1996) identified in his history of the development of the Navy's F-4 Phantom jet fighter.

The epistemology encompasses the kinds of knowledge engineers seek, depend on, and develop as they move from decomposing an imagined whole into a hierarchy of parts, and then, analyzing feedback at every step, shaping parts into assemblies and prototypes to gradually aggregate, integrate, federate them, ultimately testing their acceptability. The knowledge gained throughout this "typology of testing" culminates in piloted real-world flights of the entire human-machine system, now also with hands-on feedback. "Federation" is especially noteworthy: it "implied that the sovereignty of the components would be maintained" while being "combined into a whole" (Bugos, 1993: 279, 280; 1996: 3, 4, 285). This parts schema or template for designing an ultra-complex technology, however, also organizes the work systems that operate and maintain it—an often misplaced ordering system, the evidence suggests. One consequence is highly differentiated and fragmented analyses produced by NASA's "matrixed" functional "parts," which obstructed knowledge development and exchange. Appending "independent safety authorities" is yet another "part." But it is in the consistent focus on ceramic tiles to the exclusion of the reinforced carbon-carbon (RCC) panels before and during the *Columbia* disaster that authors let us see the most stunning manifestation of the parts schema's capillary influence.

After the first blurred images of drifting debris were replaced by those only somewhat clearer, all that could be known was that "something the size of a large cooler" had "hit the Orbiter at 500 miles per hour"; it was possible "that something significant could have happened" (Dunbar and Garud, pp. 212, 210). Yet, because earlier hazard assessments of divot-like tile damage from small pieces of foam classified them as an acceptable risk, the head of *Columbia's* Mission Management Team (MMT), assuming that only tiles could be involved and therefore was not a "safety-in-flight" issue, denied requests for further images (Dunbar and Garud, p. 213). Although the manager also designated a debris assessment team, a standard procedure, its status was anomalous and its charter "fuzzy," the CAIB report found; formally, it "had little direct connection" with the MMT (Weick, pp. 171–172). Nevertheless, concerned with potential damage to the RCC wing coating on the TPS, the debris assessment team tried to estimate the strike's likely damage. Having no models for the consequences of one so large, the team adapted two by adjusting their "analysis standards" and, calling their findings "conservative," concluded that TPS penetration was unlikely. The CAIB report observes that "no other analyses were performed to assess RCC damage" (Dunbar and Garud, pp. 213–214).

That "report only provides a few tantalizing clues about how various groups regarded the vulnerability of leading-edge structures," Woods finds (p. 293). One "engineer with close connections to shuttle management," according to the CAIB, "was regarded as an expert on the thermal protection system even though he was not an expert on the RCC," while at the same time "a tile expert [often] told managers . . . that strike damage was only a maintenance-level concern," thereby making more images unnecessary, a simplifying story they welcomed. There was, moreover, only one "resident RCC expert" (Weick, p. 164), and he, along with "external tank experts . . . was [not] concerned with the hazards of foam debris" (Ocasio, p. 119).

"NASA's scientists and engineers did not know or understand that the foam debris could lead to significant threat to the RCC panels and therefore to the shuttle's [TPS]," Ocasio finds. The acceptable risk designation "was based on experience with tile damage on the orbiter, but not on the RCC." Studies in 1999 of RCC performance during flights identified "orbital debris" as one of four "significant problems" for the TPS and one of two identified as "safety of flight" issues. Ocasio found no "documented evidence" that anyone at NASA had ever drawn "a connection between" orbital damage "at hypervelocity" and "foam debris damage upon ascent . . . at lower speeds." A 1990 risk assessment of the thermal protection system by outside experts, "while briefly mentioning the RCC panels, focuses its analysis on tile damage [and] implicitly equates the [TPS] with the ceramic tile." Ocasio calls that "a mistake," arising from the assumption that RCC panels "were more resilient than tile, therefore less likely to be damaged upon foam debris impact," but an assumption "never . . . tested during flight" (Ocasio, pp. 113–114). Even though a previous large strike had never occurred, McDonald explains, NASA engineers had also never recognized "the poor impact damage resistance of the RCC panels." While the panels' weight and appearance may belie their vulnerability, their material resistance had been calculated only for strikes from micrometeorites. With a strike "640 times larger," engineers could not, therefore, have found out that a "2 lb piece of foam could cause catastrophic damage" (Weick, p. 169; McDonald, p. 341). "Missing from [previous analyses] is the recognition that the RCC protects the structure in regions of the most severe thermal environment suffered by the vehicle on re-entry and is in a flow region where the pressure gradients would drive the hot gas into any breach on the surface" (McDonald, p. 341).

That astonishing observation explains why both NASA's engineers' and outsiders' risk assessments were on tiles alone: not only did the parts schema stunt curiosity about risks involving any part other than tiles, it also, and more portentously, inhibited curiosity about parts' interactions and their systemic consequences. This epistemology of engineering is clearly in thrall to the "sovereignty of components." The schema further partitions the functions of risk assessment and of flight control, the former believed to be already incorporated in the designed parts, the latter believed to be concerned only with putting the parts into operation. Only a "dynamic flight engineer," it seems, bridges the two. Because the debris team manager had requested additional images from an engineering group leader he knew and not through "Mission Control's flight dynamics officer, [the MMT manager believed] that the request was related to a non-critical engineering need rather than to a critical operational concern" (Dunbar and Garud, p. 214). "The vocabulary of the [MMT] was not hospitable to discussions of risks and uncertainty [which] may have [contributed to] the failure to discuss imaging requests" (Ocasio, p. 118). That vocabulary lacks a developed epistemology of operational risk significance, the kinds of knowledge needed under various trouble scenarios: the calculated logics of design all too often have little to contribute to the real-time logics of operations and production.

Studies to find sources of foam loss, twice delayed before *Columbia*'s flight, had been scheduled after it. Yet on July 26, 2005, after NASA's two years of work, including those studies, to meet the CAIB's 15 return-to-flight requirements, and at a cost of about $1.5 billion, foam loss recurred after the shuttle *Discovery* lifted off. The flight experienced a "near miss by a suitcase-sized piece of foam" (Rincon, 2005). Had this one-pound, three-foot chunk "broken away earlier, when the shuttle was deeper in Earth's atmosphere, [it] could have hit the orbiter with potentially catastrophic results," according to NASA engineers (Harwood, 2005). The parts schema remains in working order. And it reappears in calls for independent technical and safety assurance authorities: designating another functional part seems more a fix for a "broken safety culture" than a systematic response to what both observers and participants find so problematic, namely, blocked flows of crucial information, insufficient analysis and debate, loose functional integration, and an informal chain of command. The more safety is understood as being another technocratic part, the less its concerns are likely to be integrated and integrating. Designated to have "sole responsibility . . . to integrate such cross-functional boundary issues (like foam strikes)," NASA's "Integration Office" in practice shared it with various other offices, with the result that none "felt as if it owned this issue" (Snook and Connor, p. 196). So it is that the more stand-alone the safety commitment, the larger the population of bystanders can become.

Too many accidents and near-misses have shown us that safety is as often an outcome of tradeoffs among risk, cost, schedule, and engineering requirements as it is of absolute limits. In such complicated and peopled technologies, safety, despite its promissory connotation, can only mean efforts to assure its possibility. But to do that, the work of determining the risk significance of every questionable condition comes first. "Foam shedding and potential tile damage was just one of over 5,396 known and documented hazards associated with the shuttle and it was not the problem accorded the highest concern" (Dunbar and Garud, p. 217). In the best case, analyses to determine levels of risk significance organize conversations about priorities, incorporating a range of voices to consider how the condition will affect risk, to what degree, and with what consequences systemwide. That may be a reason why independent authorities at NASA keep migrating into that real politik of tradeoffs, which executives and program managers have no choice but to address, often under "real time pressures for efficiency and production" that could overtake "demands for very high safety" (Woods, p. 290). For making "safety/production tradeoffs," Woods finds, "it is not enough to have a safety organization; safety has to be part of making everyday management decisions by actively reconsidering and revising models of risk and assessments of the effectiveness of countermeasures" (p. 304). Moreover, separate "safety organizations raise questions which stop progress toward production goals" but in practice have "little to contribute" to resolving the production/safety quandary" (Woods, p. 304).

As NASA safety boards and panels yielded to program control, Leveson et al. observe, safety specialists lost "prestige and influence." Yet while claiming that for "engineering systems safety," both independence and outsidership are essential, this group also points to a military model of cross-level "safety working groups" that may combine both involvement and independent review (Leveson et al., pp. 275–277). Others similarly debate with themselves: Roberts, Madsen, and Desai warn of "the dangers of partitioning organizational tasks without adequate reintegration" (p. 95), while also seeking an "independent technical authority" that is "truly independent of the other organizations involved in the shuttle program" (p. 94). Discussing NASA's fragmentation into myriad functional offices, units, divisions, teams, and units, Snook and Connor remind us, "whatever you divide you have to put back together again" to anticipate systemwide consequences (p. 199).

The chapters acknowledge, each in its way, that tradeoff negotiations come with the territory, as many examine various substantive processes that can affect robust analyses of their consequences: the sources and kinds of knowledge allowed to matter; the experts at and not at the table; who speaks and who keeps silent; modes of resolving disputes among conflicting agendas and career concerns; and strategies for the timely integration and synthesis of disparate information. Such processes are, in practice, structural and technical preconditions for defining risk significance, assigning priorities, and assuring the knowledge validation and exchange those depend on. These processes plant the seeds of whatever culminates as risk reduction or escalation. This risk-significance culture is a prerequisite to "safety."

An epistemology for operational risk significance would take the steam out of the machine bureaucracy model and its parts schema. Instead, lattices of knowledge development, cross-checking, and exchange would privilege the availability and accessibility of credible knowledge and its timely, well-considered systemic integration. As an organizing principle for experts' work systems, laterality could shape arrangements that are as well defined and obligatory as a command-and-control or functional hierarchy. Not only would the work of characterizing this epistemology inspire rethinking such structural questions, it may also inspire us to rethink our own analytic issues, such as agency, units and levels of analysis, and the mysteries of "system" in high-hazard domains replete with specialists.

Most chapters in the book are well structured and written; reading back and forth yields a more rounded understanding of the same issues. "There is some redundancy because authors want their chapters to be independent of one another," the editors explain, yet a few paragraphs earlier they also claim, "The book is very unusual in the field of organization studies because it is a collaborative effort to dissect a decision-making situation from many perspectives" (pp. 4, 5). Reading has its bumps: weak copy editing leaves us without a glossary, yet the use of acronyms is dense and they are not consistently indexed; shuttles randomly appear with name alone or with NASA's flight numbers.

NASA is a behemoth "that has pushed or been pushed to the limit of what an organization can accomplish," Farjoun and Starbuck conclude, given its "geographic dispersion," "hierarchical layers," "complex and unreliable [shuttle] technology," "narrowly defined functions," "fragmented structure," "unstable leadership," "an ever-widening range of goals," and "very superficial" oversight of contractors—all that and more within a "turbulent" economic and political environment (pp. 360–362). In asking how NASA can identify and accept its limits, this volume is also asking those people and institutions responsible for other high-consequence enterprises, in our midst and to come, to reconsider how they could go about preventing their romances with technology from ending badly.

Constance Perin
Visiting Scholar in Anthropology
Massachusetts Institute of Technology
Cambridge, MA 02139

REFERENCES

Bugos, G. E.
1993 "Manufacturing certainty: Testing and program management for the F-Phantom II." Social Studies of Science, 23: 265–300.
1996 Engineering the F-4 Phantom II: Parts into Systems. Annapolis, MD: Naval Institute Press.

Harwood, W.
2005 "Timing of fuel tank foam loss saved *Discovery* from big hit." July 28. http://www.spaceflightnow.com/shuttle/sts114/050728hallock/.

Rincon, P.
2005 "Shuttle crew reflect on crucial flight." BBC News, August 10. http://news.bbc.co.uk/1/hi/sci/tech/4136544.stm.