August 29, 2003

Failure Is Always an Option

By HENRY PETROSKI

DURHAM, N.C. — Scientists seek to understand what is, the aerospace pioneer Theodore von Kármán is supposed to have said, while engineers seek to create what never was. The space shuttle was designed, at least in part, to broaden our knowledge of the universe. To scientists the vehicle was a tool; to engineers it was their creation.

With the release of the report of the Columbia Accident Investigation Board, there is a new focus on the "culture" of NASA. Engineers have played a prominent but not a controlling role in that culture, both in the design of the shuttle and in the planning of its missions. When the report speaks of NASA's "broken safety culture," the particular failure it cites is "a consistent lack of concern" that Columbia may have been damaged by debris at takeoff. But perhaps NASA can be better understood by examining the culture that arises from the inevitable — and healthy — tension among scientists, managers and engineers.

A common misconception about how things such as space shuttles come to be is that engineers simply apply the theories and equations of science. But this cannot be done until the new thing-to-be is conceived in the engineer's mind's eye. Rather than following from science, engineered things lead it. The steam engine was developed before thermodynamics, and flying machines before aerodynamics. The sciences were invented to explain the accomplishments — and to analyze their shortcomings.

The design of any device, machine or system is fraught with failure. Indeed, the way engineers achieve success in their designs is by imagining how they might fail. If gases escaping from a booster rocket can lower efficiency or cause damage, then O-ring seals are added. If the friction of re-entry can melt a spacecraft, then a heat shield is devised.

Much of design is thus defensive engineering: containing, shielding and fending off anticipated problems on the drawing board and computer screen so that they cannot bring down the design when it flies. Obviously, total success can only come if every possible mode of failure is identified and defended against.

Engineering is also very much about numbers. O-rings must be sized; the thickness of heat shields specified; the weight of insulation calculated. Often, the numbers work at cross purposes, as when increasing shield material decreases available payload. Engineering design is ultimately the art of compromise.

What results from the design process is a thing that has unique characteristics. It can withstand the

conditions for which it was designed as long as it maintains its integrity. There is usually some leeway allowed, for engineers know that operating conditions cannot be predicted with absolute certainty. Until it fails, how far beyond design conditions a system can be pushed is never fully known.

But engineers do know that nothing is perfect, including themselves. As careful and extensive as their calculations might be, engineers know that they can err — and that things can behave differently out of the laboratory. On the space shuttles, O-rings got scorched, heat tiles fell off, foam insulation broke free. To engineers, these unexpected events were incontrovertible evidence that they did not fully understand the machine.

Engineers do not feel comfortable with things they do not understand. It is at this point that they begin to act more like scientists. In the case of the scorched O-rings, the engineers studied burn patterns. They looked for a correlation between damage and temperature, and they warned about launching when the temperature was outside the bounds of their experience and scientific study.

If engineers are pessimists, managers are optimists about technology. Successful, albeit flawed missions indicated to them not a weak but a robust machine. When engineers and managers clashed over the 1986 Challenger launch, the managers pulled rank. In the case of Columbia, engineers who worried about damage that the spacecraft may have suffered during launch were ineffective in getting it properly inspected before reentry.

No one knows a machine or its failure modes as well as the engineers who created it, and even they know it only as well as it reveals itself to them. Because they are so humbled by their creations, engineers are naturally conservative in their expectations of technology. They know that the perfect system is the stuff of science fiction, not of engineering fact, and so everything must be treated with respect.

The Columbia Accident Investigation Board has recommended that NASA establish an independent Technical Engineering Authority. This would put responsibility for technical matters where it rightly belongs — with the engineers who, because they know how the space shuttle was designed, also know best how it can fail. Without that knowledge, another fatal accident is inevitable.

Henry Petroski, professor of engineering and history at Duke University, is author of the forthcoming "Small Things Considered: There Is No Perfect Design."
