Academy Panel Faults NASA's Safety Analysis

The agency relies too heavily on subjective judgment rather than on statistical analysis in picking problems to focus on

In a study published on 4 March, a group of experts from the National Research Council finds that the government is relying too much on subjective judgment and too little on statistical analysis in deciding which of thousands of safety problems on the space shuttle should get attention.

Since the Challenger accident in January 1986, the National Aeronautics and Space Administration (NASA) has been flooded with all kinds of advice on how to make the shuttle safer. But, according to this panel of experts, the agency lacks a well-defined, objective method by which to sort significant from trivial issues. As a result, there is a good chance that NASA will spend a lot of time attacking second- and third-rank problems while spending too little time on the ones that really matter.

The experts say that NASA should quickly adopt a method of ranking risks—such as "probabilistic risk assessment" used in the nuclear industry—to get a clear picture of the hazards confronting the shuttle. NASA has begun to move in this direction.

This report has a blue-ribbon lineage, being the child of the "Rogers Commission" that investigated the accident. That commission asked NASA to review its safety program and NASA asked the National Research Council to take on the job. It did, and 14 months later, it has produced a report that is polite, thoughtful, and quite critical.

The chairman of the panel, former chief of the Air Force Systems Command, General Alton Slay, told reporters on 4 March that "Our central finding is that while NASA has the basic organizational elements for assessing and managing risks, the arrangement is a complex mosaic of numerous review boards and safety organizations which yields a fragmented picture of the safety and reliability of the total space transportation system [STS—the shuttle]. These boards and safety organizations use analysis techniques which rely heavily on rather subjective assessments of the risk posed by thousands of individual space shuttle components or units." In short, they found a system in chaos, one that provides top officials with lots of data but very little perspective. As outsiders, they also found the system opaque, difficult to interpret, and inconsistent.

What is needed, according to this panel, is not just an objective standard by which to measure risk, but a willingness at headquarters to apply the standard. In simple terms, NASA's safety program seems to need discipline and leadership. General Slay used other words: "We have recommended that the agency strengthen the focus of their risk assessment and management activities through greater integration and by emphasizing the whole as well as the individual parts of the space transportation system."

The tenor of the report is positive. Slay was careful to say that there are "no show-stoppers." However, the report's detailed commentary is sometimes biting.

The system provides top officials with lots of data but very little perspective.

For example, the panel clearly was baffled by NASA's primary safety management tool, a "critical items list" which in 1986 tallied more than 2000 pieces of vulnerable hardware. According to the judgment of NASA's engineers, the failure of any one of these parts could wreck a shuttle. Since the Challenger explosion, the number of items on the list has grown to more than 4000. Officially, none of these parts can be used because none meets NASA's "fail-safe" design criteria. Paradoxically, all are being used because all have been granted a "waiver" on the basis of a written "retention rationale."

In most cases, the panel found, preparing a waiver seems to have been treated as a pro forma task. The reviewers could find no criteria used by NASA to judge the adequacy of waiver rationales. Generally, the margin of safety of a part is unknown because parts are not tested to failure. Nor is the probability of failure ever calculated. Technical "fixes" are accepted without regard to the possibility that they may increase the risks of failure. "We can perceive no documented, objective criteria for approving or rejecting proposed waivers," the report says.

The flip side of this confused situation is that safe parts may be listed as unsafe. Many of the items listed as "critical-1" may not be shuttle-killers at all, the panel suggests. It points out that 56 critical items failed in flight before the Challenger accident, causing no catastrophe. Here the authors raise a delicate point: the next shuttle probably will be launched with more "waivered" parts aboard (the O-rings were waivered) than were on the Challenger. How will NASA square this apparent growth in vulnerability with the assertion that the shuttle is safer now?

One solution, according to the report, would be to calculate the probability of failure and the worst-case results for each item on the critical list and to rank the items according to their statistical chance of doing harm. This would create an agreed-upon system of priorities, focusing attention on a short list of "most risky" parts. General Slay hastened to add that this formula approach would not be used as a substitute for good judgment, but as a means of concentrating judgment on the most important problems.

Among other recommendations, the panel urged the following:

- In addition to improving the "bottom-up" testing of individual components, NASA should put much more emphasis on "top-down" safety analysis. In particular, it should investigate system interfaces, whole-system performance, the dangers introduced by human error, and environmental hazards.
- NASA should see to it that the knowledge gained from risk assessment is delivered quickly to the shuttle redesign effort and to future mission planners, something that is not happening at present.
- Too often, NASA relies upon the same people who produce hardware and software for a critical analysis of problems in those systems. This may weaken quality control. Independent reviewers would be preferable.
- NASA maintains a list of launch criteria that must be met before the shuttle can take off, but, on average, it waives two criteria on each launch. It would be better to have a smaller list of criteria and honor them.
- The practice of cannibalizing parts from one vehicle for another, rampant in the pre-Challenger flights, should be curtailed. It increases human error.
- The panel suggests that NASA might create a new Systems Safety Engineering function based in headquarters, with branch offices in each of the regional centers. Its task would be to analyze systems from the earliest design stage, identify risks, and enforce safety standards. ■ Eliot Marshall