



Richard I. Cook

Observations on RISKS and Risks

The online RISKS newsgroup contains diverse reports of computer-related system failures. Because reports are often drawn from news sources, RISKS tends to be very topical. If it's in the news, it will soon be discussed in RISKS. Regular readers recognize that reports are punctuated by commentary from people with widely divergent views—often with specialized expertise. The best cite RISKS reports from prior issues, making lateral connections that other readers might not see, and demonstrating the continuity of a RISKS theme.

There is a certain etiquette for commentaries. They are specific and terse. They address a wide audience, eschew narrow technical language, and don't assume readers have domain knowledge. Finally, even though contributors often disagree with each other, their comments are always polite.

At least three main themes recur: risks associated with security, the computer-human interface, and the inherent vulnerability of large technologically based systems—what might be called the complex-system issue. In most cases, readers can readily identify a report in RISKS as belonging to specific themes. Charge-card fraud, automated bank-teller machine failures, and supposedly secure system break-in stories relate to the security theme. The theme of the human interface is often served by aviation examples.

In contrast with the first two themes, it is less obvious when reports bear on the complex-system theme. The relevant reports come from many domains, and the failures involve subtle interactions between the underlying nature of the domain, the technological system, and human operators. These reports and their associated commentaries often have a paradoxical or ironic flavor that disturbs readers and raises the temperature of the accompanying debate. A few points from this theme are worth considering:

1. Complex systems fail in unpredictable ways from causes that seem, in retrospect, to have been minor. A report provided by Scott Lucero (RISKS-18.65) is an example: "...a blown fuse took out a large portion of Iowa's 911 emergency phone system for three hours over the Thanksgiving weekend. ... A spokesperson said that the troubles isolating the problem came from the complexity of the system..."

There are many reasons why such minor failures bring down complex systems. For example, complex systems may have "common mode" failure modes where a single failure breaches multiple redundancies. Commentaries

point out that overt failure actually requires the combination of multiple small faults, consistent with Charles Perrow (*Normal Accidents. Living with High-Risk Technologies*, Basic Books, New York, 1984); and James Reason (*Human Error*, Cambridge University Press, New York, 1990) and that the minor fault identified is just one of many.

2. Failure of a complex system may be exceptionally difficult to discover and repair. Examples include the America Online failure (RISKS-18.30) and the power outages last summer. The reasons are many but perhaps most significant are the paradoxical effects of high reliability, multiple redundancy, and automatic "safety" systems. These features allow the system to accumulate a series of small faults before overt failure occurs. While this makes failure relatively rare, it also makes discerning the causal chain of failure difficult for operators and may make speedy recovery impossible.

3. Complex systems fail at inopportune moments, usually during demanding system use when the consequences of failure are highest. These extremes tax system elements by producing rarely encountered conditions (e.g., buffer overruns and signal race conditions) that force system performance into untested realms—where new forms of failure occur. This feature of complex system failures appears in many RISKS reports, including RISKS-18.64: "On Friday, 29 Nov. 1996, Amtrak's nationwide reservation and ticketing system bellied up during what is usually the heaviest travel weekend of the year. The outage caused enormous confusion and delays, because agents typically had no printed schedules and fare tables..."

As complex information technology replaces more manual ways of doing things, the old tools and operator skills disappear. Rather than using the new technology to complement or extend the manual systems, technology tends to supplant the old ways. The cost of these systems demands that predecessor approaches be allowed to fall into disuse. For example, "Why bother to incur the cost of printing timetables and training operators in their use if you have an automated system?"

Of course I have solutions for all these, but as I see I'm running short on space. I'll contribute them to RISKS. Look for them there. **■**

RICHARD I. COOK (ri-cook@uchicago.edu) is the director of the Cognitive Technologies Laboratory in the Department of Anesthesia and Critical Care at the University of Chicago.