Peter G. Neumann

MODELING AND SIMULATION

ARCHIVE PHOTOS / LAMBERT

Analysis based on system modeling and simulation is always tricky. When it catches a horrendous bug that would have undermined system behavior, it is invaluable. When it misses, it is a potential source of disaster, especially if its apparent success promotes false credibility.

• An F-16 simulator caused the virtual airplane to flip over whenever it crossed the equator, as the result of the program's inability to handle south latitudes (*SEN* *5, 2, Apr. 1980). Also in simulation, an F-16 flew upside down because the program deadlocked over whether to roll to the left or to the right (*SEN 9*, 5, Oct. 1984).

Preparing for the second Shuttle mission, the astronauts in simulation testing attempted to abort and return to their simulated earth during a particular orbit. They subsequently changed their minds and tried to abort the abort. When they then decided to abort the mission after all on the next orbit, the program got into a two-instruction loop. Apparently the designers had not anticipated that anyone would ever abort *twice* on the same flight (*SEN 8*, 3 July 1983).

• On April 1, 1991, a Titan 4 upgraded rocket booster (SRB) blew up on the test-stand at Edwards Air Force Base. The program director noted that extensive 3D computer simulations of the motor's firing dynamics did not reveal subtle factors that apparently contributed to failure. He added that full-scale testing was essential precisely because computer analyses cannot accurately predict all nuances of the rocket motor dynamics. (See *Aviation Week*, May 27, 1991, and Henry Spencer in *SEN 16*, 4, Oct. 1991.)

• The Handley-Page Victor aircraft was noted in the December 1992 'Inside Risks'. Each of three independent test methods used in flutter analysis had an error, but coincidentally all came up with seemingly consistent results, each wrong, but for a different reason. First, a wind-tunnel model had an error relating to wing stiffness and flutter; second, the results of a resonance test were erroneously accommodated in the aerodynamic equations; third, low-speed flight tests were incorrectly extrapolated. This led to the conclusion that there was no tailplane flutter problem at any attainable speed. The tailplane broke off during the first flight test, killing the crew. (See *SEN 11*, 2, 12, Apr. 1986, plus erratum in *SEN 11*, 3, 25, July 1986.)

Structural failures of the Electra aircraft were apparently due to simulation having omitted a dynamic effect (gyroscopic coupling) that had never been significant in piston-engined planes (*SEN 11*, 5, Oct. 1986).

The crash of Northwest Flight 255 that killed 156 people in 1987 was blamed on a random failure of a $13 circuit breaker preventing an alarm from signaling that the flaps were not lowered during takeoff. It was later discovered that the warning indicator for the MD-80 aircraft went off as expected in the simulator, but did not do so in the planes. (The FAA's fix was to make the simulators behave like the aircraft!) (From the *Minneapolis Star Tribune*, p. 1, 4D, Nov. 28, 1987, excerpted by Scot E. Wilcoxon in *SEN 15*, 5 Oct. 1990.)

The collapse of the Salt Lake City Shopping Mall involved an incorrect model, along with tests that ignored the extreme conditions, plus some bad assumptions. The roof caved in on the first big snowfall of the season, even before the mall was opened to the public. (Noted by Brad Davis in *SEN 11*, 5, Oct. 1986.)

The collapse of the Hartford Civic Center Coliseum 2.4-acre roof under heavy ice and snow on January 18, 1978 apparently resulted from the wrong model being selected for beam connection in the simulation program. *After* the collapse, the program was rerun with the correct model—and the results were precisely what had actually occurred. (Noted by Richard S. D'Ippolito in *SEN 11*, 5, Oct. 1986.)

In losing the America's Cup, Stars and Stripes was victimized by problems in computer modeling and tank testing of scale models. After three iterations of modeling and tank-testing, the results were getting worse rather than better. It was discovered that the simulation program included a digital filter leftover from an earlier oil platform test. (NOVA on Dec. 9, 1986, *Sail Wars*, noted by Bruce Wampler in *SEN 12*, 1, Jan. 1987.)

• Analysis and testing based on modeling and simulation are typically dependent on the accuracy of assumptions, parameters, and programs. One must be suspicious of every detail throughout the overall system engineering. Last month we noted the importance of doing end-to-end testing for the entire system—and yet realizing that is still not enough. In discussing the Electra simulation problem noted above, Jim Horning summed up: "Simulations are only as good as the assumptions on which they are based." In fact, they may not even be that good. Rebecca Mercuri noted that "It is the illusion that the *virtual* is *real* and that the *system* is an *expert* that creates a false sense of confidence." The roles of modeling, simulation, and testing all must be considered accordingly. ■

Email "risks-request @ csl.sri.com" for on-line access to RISKS issues and archives. For RISKS by fax, phone 310-455-9300 or fax RISKS at 310-455-2364

**Software Engineering Notes*