The Bugs in the Machine

by Brendan I. Koerner

EMBEDDED CODE IS THE FUTURE - GET READY TO REBOOT

If you were at a gate in Pittsburgh when he got a glimpse of the coming software hell. His New York shuttle had been cleared for takeoff when the pilot pulled a U-turn and headed back to the gate. The flaps were stuck. “We’re going to have to power down and reboot,” the pilot announced. It was the aeronautical equivalent of Ctrl+Alt+Delete. “Makes you think,” says Yourdon, author of *Byte Wars*. “Maybe they had Windows 95 underneath the hood.”

He’s not necessarily joking. The so-called embedded systems crammed into jets, cars, and “smart” appliances increasingly rely on the same bug-ridden code that corrupts PowerPoint slides, freezes *Ultima* games midquest, and costs corporate America $293 billion a year in lost productivity. “They’re starting to put Windows CE into automobile dashboards,” says Philip Koopman, a computer engineer at Carnegie Mellon University. “What used to be some gears and springs is now a sophisticated computing complex. Think about it.”

Or don’t, if you scare easily. The software industry’s nasty secret is that — surprise! — off-the-shelf code doesn’t magically turn
is creeping into systems where failure can’t be dismissed with curses and a sigh. Consider: DARPA is using wearable computers designed to beam tactical information to the “data visors” of combat troops. The devices run Windows 2000, an OS so flawed that its bug-cleansing “service packs” run to 100 Mbytes. A sniper-filled valley near Mazar-i-Sharif would be a particularly lousy spot to encounter a Runtime Error pop-up. Or take mobile phones. They worked fine when telephony was their sole task. Now that they’re equipped with Web browsers and GPS chips, software glitches are routine. If you’re one of the 200,000 Americans a day who dial 911 on a cell, shabby code could be a real downer. And the problem will only get worse as the tech industry’s weakness for bloxware infects all those code-enriched gizmos now on the drawing board — refrigerators that email repairmen, alarms that sniff chemical leaks, cars with drive-by-wire setups.

Yet the shoddiness of these products is hardly inevitable. With a bit more elbow grease, software designers can write increasingly reliable code. One smart move would be to use mutation testing, a quality-control technique that flushes out errors by analyzing the behavior of software that’s deliberately infested with bugs. Though effective, it’s rarely used by commercial coders because it adds to development costs. But if software jockeys are going to be responsible for lives as well as spreadsheets, their fixation on the bottom line must change.

If it doesn’t, there’s always the American way: Unleash the lawyers. At the moment, shrink-wrap licenses and clickthrough agreements shield software makers from damage claims — even if they broke it, you bought it. Just as the legal fallout from exploding Pintos shamed Detroit, exposing software to class-action lawsuits might induce Silicon Valley to code more cautiously.

Of course, there will be bobsledging in Hades before the software industry willingly accepts such an arrangement. Software is intrinsically complex; lobbyists might aver, and bugs are an ineradicable part of the bargain. Let them think that — at least until the day they find themselves aloft in a plane that needs to reboot. Brendan I. Koerner wrote about embryo police in Wired 10.02.

ONE SOLUTION IS TO UNLEASH THE LAWYERS

MEDICAL TESTING

Diagnosed in 60 Seconds

Heart Disease HIV Strep Alzheimer’s

Positive Negative

HOME NANOTESTS: CHEAP, QUICK, AND PRIVATE

028 • 08|2002 • WIRED