Lost Radio Contact Leaves Pilots On Their Own

Communications error wreaks havoc in the Los Angeles air control system

It was an air traffic controller's worst nightmare. Without warning, on Salad day light time, air traffic controllers lost voice contact with 400 airplanes they were tracking over the southwestern United States. Planes started to head toward one another, something that occurs routinely under normal conditions of the air traffic controllers, who keep airplanes safely apart. But now the controllers had no way to redirect the planes’ courses.

“You could see airplanes getting awfully close but you’re powerless. You can do nothing about it,” said Hamid Ghaffari, an air traffic controller at the Los Angeles Air Route Traffic Control Center in Palmdale, Calif., where the crisis occurred. The center is responsible for airplanes flying above 11,000 feet (3,400 meters) in 460,000 square kilometers of airspace over Southern California and parts of Arizona, Nevada, and Utah, including the busy McCarran International Airport in Las Vegas, Nev.

The controllers lost contact with the planes when the main voice communications system shut down unexpectedly. To make matters worse, a backup system that was supposed to take over in such an event crashed within a minute after it was turned on. The outage disrupted about 800 flights across the country.

In at least five cases, according to reports in The New York Times and elsewhere, airplanes came within the minimum separation distances mandated by the U.S. Federal Aviation Administration for planes at high altitudes: five nautical miles (9.5 kilometers) horizontally or 2000 feet (600 meters) vertically. Fortunately, there were no collisions.

Although Ghaffari, who is also president of the National Air Traffic Controllers Association local, was not in the center when the system shut down, he was able later to watch the
"Had this happened 10 or 15 years ago, when there was no onboard collision avoidance system, you would have had several midair collisions."

— Hamid Ghaifari [left], president of a NATCA local

should’ve been avoided had strict FAA operating and maintenance procedures been followed.”

Those procedures require that a technician reboot the voice switching system every 30 days. But it’s a software glitch that makes the reboot procedure necessary in the first place, says Riggs. And that glitch resides in an auxiliary system—the VCS Control Subsystem, Upgrade (VCSU).

Also developed by Jarrin, the VCSU was first put into operation last year. The VCSU is the control system for the VCS and checks its health by continuously running built-in tests on the system. It is also used when loading new data and software into the VCS.

Inside the control system unit is a countdown timer that ticks off time in milliseconds. The VCSU uses the timer as a pulse to send out periodic queries to the VCS. It starts out at the highest possible number that the system’s server and its software can handle—25. It’s a number just over a billion milliseconds. When the counter reaches zero, the system runs out of ticks and can no longer exist itself. So it shuts down.

Counting down from 25 to zero in milliseconds takes just under 30 days. The FAA procedures of having a technician reboot the VCSU every 30 days resets the timer to 25 almost three weeks before it runs out of digits.

Many competing systems have such timers, says Jim Turley, an independent embedded processor analyst. What is supposed to happen is that the software automatically reboots or the timer automatically resets itself before the allotted time is up. “I’ve seen these flaws before, where nobody bothered to worry about what would happen when the timer reached zero,” he says. Riggs agrees. “It was an oversight,” he says. “Harris, the manufacturer, was aware of the problem but didn’t really know how it would impact the system.” But the FAA didn’t learn of the problem until it ran the new system in the field. It ran for 402 days and then it crashed. They weren’t sure why, says Riggs. “They rebooted the system and everything seemed to be working fine. About a week later another system crashed in Houston.” That’s when the FFA instituted the 30-day manual reboot maintenance procedure. “But,” says Riggs, “It’s insane for the FAA to continue to operate a system with a known problem. And by doing that, they expose themselves to this failure. And the problem is still out there.”

The FAA now has a software patch that should fix the problem. It periodically resets the counter without human intervention. The patch was being readied for the Seattle center when the 12 September breakthrough happened and now is up and running. It is too late installed in the other 160 centers.

Still, there would have been no crisis at Palmdale if the backup unit had worked properly. That’s why Ghaifari thinks the traffic control centers should have a second backup system. “When you’re dealing with systems that support very high degrees of concern over safety, you need to make sure that you always have solid redundant systems. And the thing that hopefully the FAA will learn from this is that having only one backup system for the entire air traffic control communications system is probably quite unsafe.”

— Linda Geffert

November 2004 • IEEE Spectrum • 17