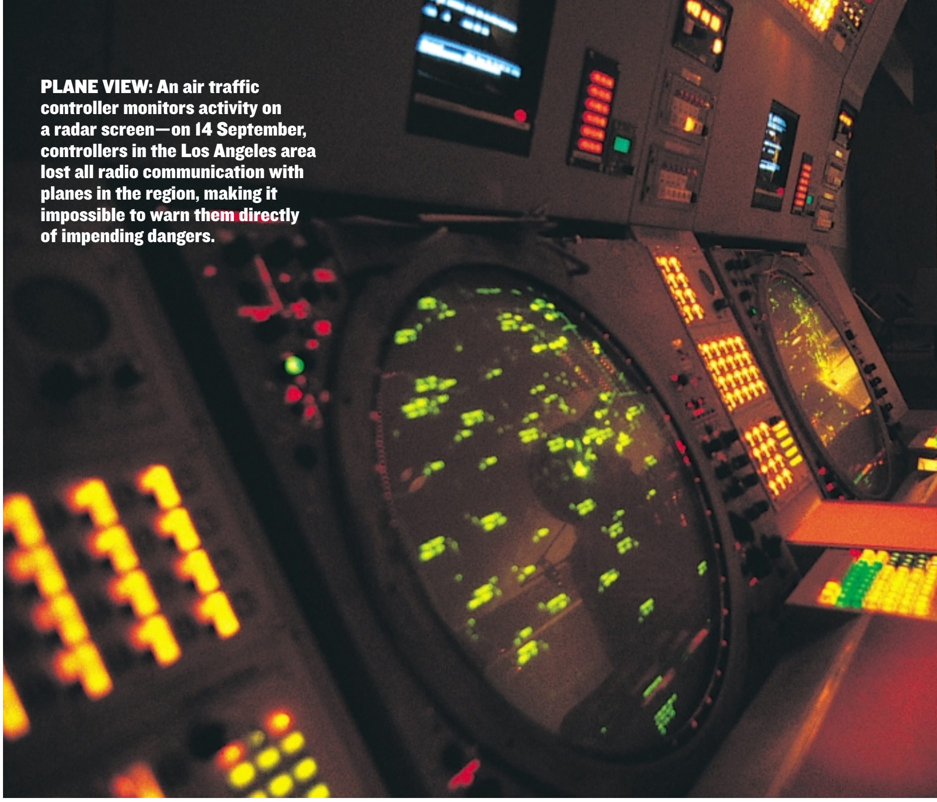
NEWS



PLANE VIEW: An air traffic controller monitors activity on a radar screen—on 14 September, controllers in the Los Angeles area lost all radio communication with planes in the region, making it impossible to warn them directly of impending dangers.

DIGITAL VISION/GETTY IMAGES

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 Tuesday, 14 September, at about 5 p.m. Pacific daylight 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 careful control 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 13 000 feet (4000 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 (9.25 kilometers) horizontally or 2000 feet (610 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

REED SAXON/AP

radar replay of several near misses. “It’s a situation I wouldn’t want any of the controllers to be faced with: two aircraft at the same elevation, headed for the same location. And at the last second you see one of them climb and one descend.”

In a situation that could have proved deadly, tragedy was averted by quick-thinking controllers who used their own cellphones to alert other traffic control centers and the airlines themselves that airplanes were on a collision course, says Ghaffari. But the real hero of the night, he said, was the collision avoidance system on board commercial jets. Each of these units interrogates the transponders of nearby aircraft. If danger of a collision is detected, one of the pilots is told by the system to climb and the other to descend. “Had this happened 10 or 15 years ago, when there was no onboard collision avoidance system, you would have had several midair collisions.”

The Palmdale system that shut down, causing all the chaos, is a Voice Switching and Control System (VSCS), one of 21 in use throughout the continental United States and Alaska. Designed by Harris Corp., Melbourne, Fla., it has been running in air traffic control facilities since the mid-1990s. With the VSCS, controllers use a touch-screen to select a phone line to connect them to other controllers or to a radio frequency to talk to flight crews. It’s a complex system, according to Richard Riggs, a spokesperson for the Professional Airways Systems Specialists, the union of technicians who maintain the communications systems for the FAA. At the Fort Worth, Texas, control center where Riggs works, for example, the VSCS connects nearly 160 air traffic controller positions and has about 110 channels of air-to-ground communication.

So what went wrong on 14 September? In a statement issued the next day, the FAA laid the blame squarely on human error: “Our preliminary findings indicate that the outage was not the result of system reliability but rather an event that should’ve been avoided had strict FAA operating and maintenance procedures been followed.”

“Had this happened 10 or 15 years ago, when there was no onboard collision avoidance system, you would have had several midair collisions”
—Hamid Ghaffari [left], president of an NATCA local

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 VSCS Control Subsystem Upgrade (VCSU). Also developed by Harris, the VCSU was first put into operation last year. The VCSU is the control system for the VSCS and checks its health by continually running built-in tests on the system. It is also used when loading new data and software into the VSCS.

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 VSCS. It starts out at the highest possible number that the system’s server and its software can handle—2^{32}. It’s a number just over 4 billion milliseconds. When the counter reaches zero, the system runs out of ticks and can no longer time itself. So it shuts down.

Counting down from 2^{32} to zero in milliseconds takes just under 50 days. The FAA procedure of having a technician reboot the VSCS every 30 days resets the timer to 2^{32} almost three weeks before it runs out of digits.

Many computing systems have such timers, says Jim Turley, an independent embedded-processor analyst. What is supposed to happen is that the software automatically reloads 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 told *IEEE Spectrum*.

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 49.7 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 FAA 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 14 September breakdown happened and now is up and running. It is to be installed in the other 20 centers soon.

Still, there would have been no crisis at Palmdale if the backup unit had worked properly. That’s why Ghaffari 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 redundancies. 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 unwise.” **—LINDA GEPPERT**