the Availability Digest
www.availabilitydigest.com

Military GPS Disabled by Upgrade

June 2010

The U.S. Air Force is deploying a new GPS satellite system to replace the aging system now in service. In anticipation of this deployment, the Air Force upgraded the software in its GPS ground-control systems in early 2010 to be able to handle signals not only from the current GPS satellites but also from the new satellites. The software in the 800,000 military GPS receivers currently in service were also upgraded to be compatible with both satellite systems.

To everyone's dismay, when the new ground-control systems were brought into operation, 10,000 of the Air Force's GPS receivers wouldn't work. The systems they supported were effectively down. It took two weeks to come up with a temporary fix and months to test and deploy a permanent fix.

The capabilities of GPS have become a backbone technology for the U.S. military. How could such a critical system fail so miserably?

The Global Positioning System (GPS)

The Global Positioning System (GPS) is a space-based global navigation system. Multiple satellites orbit Earth in near-earth orbit (about 12,710 miles up) every twelve hours.

Each satellite carries an extremely accurate clock and transmits its current clock time to Earth. Ground-based receivers receive signals from the satellites that are in their lines of sight. A receiver measures the difference between the clock time in the transmitted message and its own internal clock to calculate the distance that each satellite is from the receiver. By receiving the signals from multiple satellites, a receiver can triangulate and determine its longitude, latitude, and altitude.

The Current System – GPS IIA

The development of GPS began in the 1970s as a military project, driven by the race with the Soviet Union for technological supremacy. The first GPS system was deployed in 1973 and has been replaced with new satellite technology over the years.

The satellites for the current GPS system, GPS IIA, were launched between 1990 and 1997. They provide two services – Standard Positioning Service for civilian use and Precise Positioning Service for military use. Though the civilian service provides accuracies within a few tens of meters, military service provides an order-of-magnitude greater accuracy. In addition, it is said that the military can reduce the accuracy of civilian usage if it is expected that civilian GPS services will be used maliciously.

Though the GPS IIA satellites have a design life of seven and a half years, eleven of the satellites are still in operation after almost two decades and provide the GPS services we enjoy today. However, these satellites are past their end of life and need replacing.

The New System – GPS IIF

Built by Boeing, the new GPS IIF satellite system currently being deployed incorporates many advances over GPS IIA:

- It has a design life of twelve years.
- It has a more accurate clock.
- Its positional accuracy is doubled.
- It has faster processors with more memory.
- It is more able to resist jamming.

GPS IIF will comprise twelve satellites. The first GPS IIF satellite was lifted into orbit by a Delta 4 rocket on May 28, 2010.

Artist's Conception of GPS IIF Satellite

Command and Control

The GPS system is developed, maintained, and operated by the U.S. Air Force. The satellites are monitored and controlled by Air Space Command units at Schriever Air Force Base in Colorado and by a backup control center at Vandenberg Air Force Base in California.

The Military Importance of GPS

GPS has found wide use in both civilian and military circles. Civilian uses range from car navigation and cell-phone E911 services to trekking games such as geocaching.[1]

GPS usage by the military is far more widespread. The military uses GPS for air and sea navigation, bomb and artillery guidance, and armored vehicle and troop tracking. Because GPS makes weapons more accurate, the military needs fewer warheads and fewer personnel. However, the leaner GPS-dependent military becomes more vulnerable if GPS services are lost.

This raises concerns that an attack on GPS could wreck havoc not only on the civilian population but also on the military's capabilities as well. The Air Force says that to date there has never been a breach of the GPS system. With satellites 12,000 miles high in the sky, they are safe from attack (at least, with today's technology). The GPS command center is backed up with a command center hundreds of miles away, both at heavily secured Air Force bases. GPS communications is heavily encrypted.

During the U.S. invasion of Iraq, the Iraqis tried to jam GPS signals. However, this took so much power that the positions of the jamming stations were easily pinpointed; and they were taken out by GPS-guided bombs. It is felt that jamming is beyond the capabilities of groups like the Taliban and many third-world countries. However, jamming by a major foe is a concern.

The military use of GPS is not foolproof. There is still a human element. In 2001, a GPS-guided bomb dropped by a Navy F-18 fighter jet fell into a residential neighborhood in Kabul, Afghanistan. Four civilians were killed. A subsequent investigation determined that wrong coordinates had been entered into the guidance system.

The Botched GPS Upgrade

With such a heavy dependence by the military on GPS, it is incumbent upon the Air Force to ensure that any modification to the GPS system, whether it is being made to the satellites, the

[1] Geocaching is a high-tech treasure hunting game played throughout the world by adventure seekers equipped with GPS hand-held devices. See http://www.geocaching.com.

ground-control stations, or the GPS receivers, is fully tested before being commissioned. But this didn't happen when modifications to accommodate the new GPS IIF were made.

Trimble Military and Advanced Systems of Sunnyvale, California, a division of Trimble Navigation Limited, was given the contract to modify the GPS receiver software to be compatible with the signals from both GPS IIA and GPS IIF. According to a Trimble spokesperson, the new receiver software was thoroughly tested according to the Air Force test specifications provided by the Air Force's GPS Wing.

Trimble's new software was installed on the 800,000 military GPS receivers worldwide. However, when the new software was put into service in the ground-control stations on January 11, 2010, reports started pouring in that receivers could no longer acquire the satellite signals. As many as 10,000 receivers were inoperable. Civilian receivers, which use different signals, were not affected.

The Air Force's GPS Wing immediately assembled a User Equipment Crises Action Team that contacted military users around the world, including active combat teams in Iraq and Afghanistan, to determine who had inoperable receivers and what types they were. They soon discovered that the problems were limited to two versions of Selective Availability Anti-Spoofing Module (SAASM) receivers. It turned out that the receivers were unable to authenticate the new message format implemented as part of the GPS IIF upgrade.

It took two weeks for Trimble to come up with a temporary fix and several months to design, test, and distribute a permanent fix.

A subsequent investigation found that though the Air Force had performed extensive testing on the new receiver software, it had never tested the upgrade on the SAASM receivers. The reason was quite simple – they had no such receivers available to them for testing. As a consequence, the Air Force is now acquiring a broad cross-section of all military and civilian receiver models and is developing longer and more thorough tests for military receivers.

All of this was not known to the general public until April 30th when the Air Force disclosed the problem on the Federal Business Opportunities web site. The Air Force would not comment on how many systems were affected, but it did acknowledge that operations were halted for a while on one development program. This program was the development of the X-47B jet-powered, carrier-based drone aircraft.

X-47B Drone

Lessons Learned

One lesson to be learned from this experience is obvious. Take a shortcut in testing, and the area not tested is bound to bite you.

Another lesson is fallback. Always have a fallback plan so that you can return quickly to the known good system if the upgraded system performs improperly. When reports of GPS receiver failures started pouring in, why didn't the Air Force reinstall the original software and return to normal operation while the problem was being diagnosed and corrected?

Fortunately, in this case, no serious harm was done. But what if this had happened in a widespread conflict? How many critical systems actively engaged in combat would have suddenly failed? What bombs would have fallen on civilian populations? What troops on the ground would be suddenly lost? What flights would not have found their destinations?

Talk about safety-critical systems. Let us hope that we will never have to answer such questions.

Acknowledgements

Our thanks to Availability Digest subscriber, Ken Schroer, for bringing this story to our attention. Material for this article was taken from the following sources:

Air Force Working Through GPS Receiver Problems, *Space News*; May 7, 2010.
Air Force: Troubled GPS receiver not tested, *Air Force Times*; May 17, 2010.
Air Force: Troubled military GPS receiver wasn't tested before change in control system, *Science News*; May 18, 2010.
Report: GPS Glitch Crippled Scores of Military Devices, *AOL News*; June 1, 2010.
Software SNAFU took out 10,000 military geo locators, *The Register*; June 2, 2010.
GPS for military went down, *NaviGadget*; June 4, 2010.
Glitch shows how much US military relies on GPS, *Associated Press*.