RED ON THE RADAR SCREEN:

GPS DEPENDENCY GROWS

by:
LANGHORNE BOND

Delivered to the
Air Traffic Control Association
Dublin, Ireland
20 July 2001

I. SETTING THE RECORD STRAIGHT

Some of you here may have heard that I am against GPS. This is a canard spread by technology-besotted salarymen. It's not true.

The truth is, I love GPS. It's terrific. It is not, however, perfect. Unfortunately, the status of satellite positioning and timing has ascended from an interesting technology to an established religion. The editors of the JOURNAL OF AIR TRAFFIC CONTROL have allowed Frank Frisble to publish several religious tracts about ATC, so I feel free to say here in Dublin: only the Pope is infallible. GPS has its limitations.

II. LISTING THE LIMITATIONS

I have talked about the serious vulnerabilities of GPS so many times that I'm repeating them in my sleep, But I (earned in my checkered career that you have to say something a dozen times before it sinks in. So here are a few of the leading indicators.

- The US DOD, which knows more about the vulnerabilities of GPS than any other institution, never commits its personnel, ordnance or vehicles to GPS sole means navigation. There's always a redundant backup.
- The Presidential Commission on Critical Infrastructure Protection (PCCIP), a top drawer White House group, listed GPS dependency as one of the US economy's most significant vulnerabilities and directed the Secretary of Transportation to publish a study on the subject. More on this later.
- The Presidential Decision Directive (PDD) setting out US policy specifically reserves the right to turn off or alter the GPS signal to "the National Command Authority," i.e., the President or his successor in the military role. .This policy is periodically stated.For reasons of US and NATO defense, this policy is absolutely correct: GNSS signals are agnostic-there I go again-and can be used to attack the home team.
- The Russian firm Avioconversia has marketed at the Moscow and Paris Air Shows a 5-watt GPS jammer that is effective to 200 kilometers. This is probably a simple noise jammer, which can be assembled from $50 of parts from Radio Shack.
- A more sophisticated jammer is the “spoofer”. A spoofing jammer transmits a GPS lookalike signal with incorrect data. A one watt, repeat one watt, spoofer on Logan Airport, Boston, can deny GPS reception to 350 miles line of sight Source: Lincoln Labs.
- The power of the GPS signal received on earth from a weak transmitter in medium orbit at 91,000 miles is ultra-faint- one watt to the minus 19 power, or one ten quadrillionth of a watt. Modern

receivers work fine with that signal. But it is easy to overpower or spoof.

- In January the Rumsfeld Commission released a report detailing the ways satellites can be attacked in space. GPS satellites were on the vulnerable list.
- Finally, the decision to turn SA off. SA-selective availability --is a deliberate degradation of the accuracy of the GPS signal to reduce is utility to enemy forces. Dan Golden of NASA came to Edinburgh, Scotland, to announce that SA would be set to zero, i.e., turned off. He got a standing ovation because the utility to civil users was greatly improved. But everyone missed the subtext. DOD, which controls GPS, did not just sharpen the accuracy and put its warriors and facilities at risk. DOD hays now so perfected its jamming techniques that people and facilities can be protected in spite of counter Jamming (AJ). This is good news for the military but is a wake-up calf to civil users. JAMMING WORKS.

III. THE CONSEQUENCES OF POSITIONING VULNERABILITY

By now everyone knows about the vulnerability of GNSS – satellite positioning and timing. But the public discussion on the subject has ranged between non-existent and feeble. The one study, by the Applied Physics .Lab of Johns Hopkins University, has been discredited.

GPS vulnerability has different consequences to different users. Here is a brief survey.

A. Safety of Life

Navigation by aircraft and vessel is becoming more and more dependent of GPS signals, This, in itself, is not a problem since GPS and other GNSS systems provide a useful addition to the array of positioning sources now In use. But there remains embedded in much of the world's long range planning the notion that GPS and only GPS will be on board aircraft, This is the notorious "sole means doctrine. If aircraft should suddenly lose navigation and precision approach capability on a foul weather day, it is certain that many will crash. As a practical matter, US air carriers no longer plan to go sole means at any time In the future. But the specter remains and the US DOT and other NAA's should publicly abandon the sole means doctrine now.

Marine navigation is similarly at risk. The US Coast Guard some years ago after the Andrea Doria collision required the carriage of a radionavigation system on larger vessels. At the time that meant LORAN. Then when GPS came along it was allowed as an alternative to LORAN. Thus, US vessels may navigate with GPS as the sole means of radio navigation. The consequences of this hasty decision were not appreciated at the time and IMCO is quietly studying this issue for marine navigation.

B. Tracking, Surveying, Backpacking

There are myriad's of non-navigation uses of satellite positioning which do not directly involve loss of life. Tracking of motor vehicles, trains, containers, vessels, surveying of all types, agriculture, and backpacking come to mind.

Loss of GPS to these users could be a severe economic hardship. No one has calculated the cost of the loss of satellite positioning to these users, but it would obviously be severe.

IV. TIMING

Positioning satellites perform another less publicized task. GPS provides a highly accurate atomic signal, which is used right now to time wireless networks of all types. Cell phones, data networks, power distribution systems, financial transactions, and even … The Internet! If GPS is interrupted these systems are in danger of collapse. It is true that most of these nets have an independent timing backup, but these clocks, are good for only 48 hours at most. I now believe that intentional interference with GPS will cause more disruption by killing the timing signal than by killing the positioning service.

Some mitigation of timing vulnerability is possible. Rather than picking the timing signal off of the orbital GPS birds, which requires Omni-directional antennas, it is possible to use the WAAS geostationary birds. This permits directional antennas with horns which can be better shielded from ground-based jammers. On the other hand, the GEOs are juicy targets for destruction in orbit. For a detailed description, see the Rumsfeld Commission Report.

V. ATC MULTIPLE FAILURES'

A GNSS soIe means navigation system raises the new, and alarming, prospect of a single point, catastrophic failure. At least the civil world is now aware of this, even though there isn't much discussion of the subject. Now another, even more threatening problem has emerged.

Since the beginning of modern ATC it has been received wisdom that the three elements of ATC--communications, navigation, and surveillance (CNS)--should be Independent of each other so that a failure of one would not bring down the others. Furthermore, the elements within each sector have been designed to operate separately so that, for example, the failure of one radar would not cause others to fail.

It is now apparent that the GPS virus has spread to all three elements of CNS. The FAA's communications and surveillance systems are now timed by GPS. This means that a well-coordinated terrorist attack on GPS in the US, and indeed in most countries of the world, can collapse most or all of the entire ATC system.

VI. THE VULNERABILITY STUDY

As I mentioned earlier in this paper, the Presidential Commission on Critical Infrastructure Protection (PCCIP) identified GPS as a significant national vulnerability and directed the DOT to do a study of GPS vulnerability and possible mitigation thereof.

The study was given to the Volpe Center in Cambridge, MA, and was prepared by tire navigation office. The study was Intended for public release and contained -no classified information and, in fact, no information that could not be found on the Internet (ex: the Google scientific search engine includes 492 tides on interfering with satellites), open military publications and journals, and ATCA papers.

The study was completed and delivered to the Secretary of Transportation and the Administrator of the FAA one year ago.

DOT is hiding it.

DOT/FAA does not want this study to be seen by the airlines, the general aviation community, ICAO, foreign governments, the NTSB, the Congress, and, especially, the FAA's Management Advisory Committee. Nor by the press.

Rumor hath it that the study is being redrafted, like the Johns Hopkins study, to remove the parts that would impeach the FAA's satiety oversight performance. Surely this justifies Secretary Mineta's order that some sort of independent oversight of FAA's internal ATC practices be established.

VII. CONCLUSION: BACKUP NEEDED

It is now time for FAA/DOT to face up to the safety flaws of its satellite positioning and timing responsibilities. The Clinton Administration, so rhapsodic in its devotion to GPS, chose to ignore the multiple, public warnings that OPS had limitations as well as strengths.

A fair and public discussion of the GPS issue will lead to one conclusion. For safety of life applications (such as navigation), for applications where loss of GPS can cause great economic harm, and for nearly all timing applications, sole reliance on GPS is not acceptable. Practical, low cost, redundant backup systems are readily available. It is time for the Bush Administration to restate the oldest law of aviation safety: every system must fail safely.