THE SIGNIFICANCE OF SA OFF

by
LANGHORNE BOND

Delivered To
The International Loran Association
14 November 2000
Washington, DC

I. INTRODUCTION

On May 1, 2000, the US government suddenly turned off Selective Availability (SA), a satellite based feature of the GPS civil positioning service which introduced random errors in the signal. SA caused the GPS signal to degrade to an accuracy of .15 mile, or about 750 feet. Turning off SA improved the accuracy of the basic GPS civil signal greatly.

The death of SA was good news to civil users of GPS. But the immense significance of the event was completely overlooked in the press. To understand this, a brief review of recent history is needed.

II. THE PDD AND THE SA SCHEDULE

In 1996 President Clinton issued a Presidential Decision Directive (PDD) setting GPS policy. The PDD set the target date for turning SA off at 2000, with periodic reviews to determine if an earlier date was feasible.

The first annual review was due in late 2000. No one expected an immediate turn-off of SA, so the decision was a complete and welcome surprise to civil users worldwide. We are still trying to figure out all the ramifications of the SA Off decision. This paper focuses on only one: intentional interference, AKA jamming.

III. PROTECTING THE US MILITARY, NATO, AND OUR OTHER ALLIES

GPS, like LORAN, began life as a military system. The GPS satellites actually transmit two different positioning and timing signals: a military signal, which is encrypted, and a civil signal, which is available to anyone. The US Coast Guard reported 4½ meters accuracy on the civil signal, 95% of the time immediately after SA was turned off. The accuracy of GPS was so good that it could be used for targeting as well as for navigation.

Here's the dilemma: the basic civil signal, which is not encrypted and is publicly available, can be used by enemies of the US, very much including terrorists, to attack US military targets.

This obvious problem was addressed by the DOD with SA. By blurring the accuracy of the GPS signal at the satellite, the accuracy would then be insufficient to hit a target.

IV. HIJACKING GPS

The free market rudely disturbed this cozy military situation. GPS was hijacked by the civilian users. The civil GPS was so useful that a huge industry emerged. It is still growing as new non-military uses of GPS emerge. Today GPS is both a lethal military system and a universal, worldwide utility.

As use of GPS increased, it became apparent that the civil market needed a more accurate signal. Pressure grew to turn off SA.

V. THEATRE PROTECTION

The DOD then turned to alternative means of protecting its troops and facilities from its own GPS signal. The Nav War programs, all of them classified, grew to billions of dollars. The solution lay in non-satellite means, or theatre based methods—jamming. By limiting intentional military interference to a war zone, AKA theatre, our troops would be protected without disrupting the civil users in the rest of the world.

VI. ANTI-JAMMING

Modern warfare is nothing if not complex. Furthermore, warfare changes at an increasing pace.

As intentional interference—jamming—grew in sophistication, at least two types of jamming emerged. The first and simplest jamming is noise jamming. Noise jamming merely transmits radio energy, "white" noise, into the GPS band. This method is very effective on simple GPS receivers because the GPS signal is so weak—one ten quadrillionth of a watt received on earth—that it can be overpowered up to 200 kilometers with a 5 watt jammer. The Nav War program, of course, knows that an enemy or a terrorist will try to work through the noise jammer by adopting anti-jam measures such as antennas and filters.

The second type of jamming is "spoofing" jamming. A spoofer imitates the publicly available format of the GPS signal but transmits incorrect timing and positioning information. A one watt spoofer located on Logan Airport can disrupt GPS in aircraft over 300 miles. This type of jammer is much harder to neutralize with AJ because if you kill the spoofer you may kill GPS as well. No publicly available counter measure to spoofing jamming is known.

All of this work has been carried out in secret, out of the sight of the civilian users—and properly so. But now we know the conclusion.

VII. JAMMING WORKS

The Entire US government studied the jamming—anti-jamming question. The White House, NSA, CIA, DOD, DOT, and Commerce were involved. The conclusion these agencies reached: jamming works. Intentional interference is a reliable method of disrupting the civil GPS signal in spite of counter measures. This conclusion is immensely significant because the US agencies involved have perfect knowledge of anti-jamming technology and are willing to put US military men, women, and assets at risk, protected only by jammers, from enemy or terrorist GPS-guided missiles and bombs.

This conclusion is the final nail in the coffin of the much-criticized Johns Hopkins/Applied Physics Lab report. As Mike Shaw, then representing the C^3I Office of the Department of Defense, said to RTCA, "There's really very little we can do about jamming."

VIII. ERGO, SA OFF

The decision to turn off SA was an easy, inevitable next step.

The consequences to the civil users of GPS are profound. Most civil GPS positioning users are not in the safety of life category and loss of the GPS signal to an enemy or terrorist is just an expensive inconvenience. There are other, non-GPS ways to survey sites or to keep track of trucks and rail cars.

But GPS positioning users in the safety of life category are different. Successful jamming of the GPS positioning signal can cause a complete loss of radionavigation in an aircraft equipped only with GPS systems. On a foul weather day, with no way to find a runway, many aircraft will run out of fuel in two hours and will crash.

There is similar, though not identical, risk to vessels carrying toxic cargo and thousands of passengers.

IX. SOLE MEANS

In the early, optimistic days of GPS development it was thought that satellite positioning and timing were more than wonderful—they were perfect. Every one of the existing terrestrial navigation and timing sources could be turned off and scrapped. This policy was announced in the US and specifically recommended to the world via ICAO—numerous times—by the government.

The SA Off decision is the first public statement that GPS sole means, meaning that GPS is the only navigation and landing system on the aircraft, is unsafe and therefore cannot be approved. The DOT and FAA should now state publicly that GPS sole means is a dead issue.

X. WHAT ABOUT TIMING?

Almost all of the public discussions of the limitations of GPS have focused on the use of the positioning service in navigation.

But there is another, even greater, risk that flows from the use of GPS—jamming the timing signal. GPS provides a high accuracy atomic timing signal that has been widely adopted to control modern telecommunications

networks. The list of users which are now dependent on the GPS timing signal is astonishing—CDMA cell phones, the Internet, power distribution systems, financial networks, and voice and data systems. But the GPS timing signal is as vulnerable to intentional interference as is the positioning service.

Disruption of the GPS timing signal could cause a widespread collapse of our cyber-dependent economy. The SA Off decision makes clear the vulnerability. Yet there has been virtually no discussion of this risk.

XI. THE VULNERABILITY STUDY

President Clinton recently ordered the Department of Transportation to do a comprehensive study of the vulnerability of GPS to civil users.

DOT reported that the study is now complete and rests on the desk of Secretary of Transportation Rodney Slater. Two scheduled presentations on the study were cancelled, and the current release date is now said to be the first week of January.

Given the conclusions that led to the SA Off decision, the finding of the Vulnerability Study will be no mystery. It will be: the GPS signal is significantly vulnerable and some important categories of users cannot rely on GPS exclusively.

This finding is certain for safety of life users. The finding for timing users, however, is less certain. This is not because the timing vulnerability is less – it is the same – but because there is no federal regulator to assure the security of telecom nets and because the corporate interests at risk have adopted a policy of secrecy for, it is said, competitive reasons. An alternative explanation is that the telecom companies are in denial like DOT. Thus, the finding of the vulnerability of timing users will come as an unwelcome surprise.

XII. THE NEXT STEP

The Vulnerability Study deserves close reading because the devil is in the details. The finding that there is a vulnerability risk is obvious and easy since by now everyone knows it.

But the way forward will require vision and some resolve. I am fearful that DOT will botch it.

What is needed is an unequivocal statement that GPS sole means in safety of life applications is never acceptable, period. This, surprisingly, is a very easy call for DOT, not only because GPS is vulnerable, which prohibits GPS sole means now, but also because GPS is a single thread system and therefore is never certifiable.

But I fear the worst. I fear that the study will recognize that GPS sole means is not approvable now or for a long time in the future but maybe, just maybe, the vulnerability problem can be solved in another lifetime.

This equivocal outcome would be a disaster for manufacturers, GA, and air carriers alike because they would have no idea what to put in their airplanes. The search for the best redundant system could not begin in earnest because it might not be needed.

Let me end on a cheerful note. There is light on the horizon. The Boeing Company has announced that it will develop a complete navigation system, including transmitters and avionics. Boeing will understand the technology, the air carrier requirements, and the safety. If Boeing can get on the same page with AOPA the circle may be complete.

Maybe we're witnessing the first step to privatization.

—END—