GNSS Sole Means Of Navigation AND The Future Mix Of Navigation Systems In ATC

Presented To The
ICAO/CANSO Conference
Shannon, Ireland
18 May 2005

By Langhorne Bond
Pittsboro, NC USA
(919) 542-6614

I.INTRODUCTION

Let me begin with a disclaimer. I am not opposed to the use of GNSS positioning, navigation, and timing. This is a canard spread by narrow minded salary men. Au contraire. GNSS is a wonderful technology and is improving transport navigation and creating wealth for people (and tax collectors!) around the world. In the near future GNSS use will be universal.

The fault lies not with the splendid technology but with those of us who manage it. We have failed to acknowledge the limitations of GNSS and to develop strategies to eliminate the risk it poses to safety, national sovereignty, and economics which are rapidly becoming dependent.

This is a manageable problem and can be dealt with by the application of existing technology at a low cost. But we must first abandon preconceptions and acknowledge the problem. Then the solution is easy.

II. GNSS VULNERABILITY

GPS, the US military's satellite system and currently the only functioning, universal GNSS system until the EU's splendid Galileo system comes on line, orbits at a medium altitude of 11,000 miles and transmits at a power of about 20 watts. When received on earth or by an aircraft the signal strength is 1-16 watt-one watt to minus sixteen power, or one ten quadrillionth of a watt. This is a tiny fraction of the power permitted to leak from your hair dryer or computer. Later versions of GPS or Galileo or augmentation systems will not substantially change this equation.

For those GNSS users which cannot ever lose the PNT service, two problems arise.

- In the aviation lexicon GNSS is a single thread system. There is no redundancy or backup in case of failure. In aviation it is received wisdom that everything sooner or later will fail-who can dispute that?-and there must be redundant, fail-safe protection. Neither augmentation systems nor more satellites solve this problem. This issue alone, Regardless of vulnerability prohibits GNSS sole means dependency.

- GNSS is highly vulnerable to interference because of its ultra low power. There are two generic types of interference: unintentional and intentional.

III. UN-INTENTIONAL INTERFERENCE

This includes national forces such as Ionospheric forces, and electromagnetic storms, and multi-path. This is not the place to go into the details but let me mention one event of many. On October 29, 2003 four months after WAAS vertical approaches were certified, an unexpected solar storm wiped out the WAAS vertical signal over the entire US for nearly 24 hours. This was repeated in November! Another event has been reported in January 2005. This would not be a problem if ILS or MLS were continued and carried.

Another source of unintentional interference is from existing transmitters such as TV stations and even ships radar. The US Navy is investigating this.

IV. INTENTIONAL INTERFERENCE

Intentional interference is potentially the most serious threat to GNSS signals. We who use GPS/GNSS as a wonderful civil utility tend to forget that satellite positioning systems are the most powerful military devices since the invention of the thermonuclear bomb. They can be used as high accuracy targeting systems by your side and by hostile forces. So it is mandatory that defense agencies be able to disrupt GNSS signals, before the bad guys put a cruise missile into the jet fuel tanks of an aircraft carrier or into the River Entrance of the Pentagon. Trust me; every defense department in the developed world is working hard to create technology to obliterate all types of GNSS signals. The details are properly secret, but the evidence is everywhere, most of it reported. In the US the time and location of tests are reported beforehand by the Coast Guard and FAA.

There are three types of intentional interference of GNSS…..

- Attack on satellites. This was detailed in the Rumsfeld Commission Report on Space Warfare, published just before President Bush took office. The Boeing Company makes an anti-satellite satellite described in the press as a "giant flyswatter". Very recently DOD announced an advanced satellite capable of A Sat use. Probably less than a dozen countries can now attack satellites.

- Noise Jammers. This is the simplest and cheapest type of intentional interferences. You can buy the parts for a noise jammer at Radio Shack and make one at home. The noise jammer transmits energy-white noise, or static-on the GNSS band and blots out the signal. Its effectiveness depends on the jammer's power and the distance to the receiver. If the S/NR fails off, the effect declines.

- Spoofers. Spoofing jammers, which transmit a sophisticated signal meant to fool the receiver into an incorrect reading, are effective over long distances and are harder to counter. A one (1) wall spoofer on Logan Airport, Boston, can disrupt GPS reception over 300 miles, basically line of sight. Source: Lincoln Labs, MIT.

Both noise jammers and spoofers can be placed in weather balloons, which are nearly impossible to bring down. Effective distance: 800 miles.

For an in depth discussion, check out the famous Volpe Center Report on GPS Vulnerability.

V. ATTACKERS

Who would disrupt GNSS? To start with, the US. President Bush's December 2004 new policy is a lot more candid than the 1996 PDD which it supersedes. The <u>preferred</u> military jamming will be localized or theatre based, with every effort made to avoid "unduly" interfering with civil users. This is probably a correct statement of Western defensive jamming policy now.

But jamming can be used as an offensive weapon against hostile forces and civil targets and populations. Jamming and counter jamming has now been used in Kosevo and both Iraq wars.

In addition to military users, jamming by terrorists is a real, here and now threat. A carefully staged attack on a stormy night could cancel instrument approaches in a region wide area. Dozens of planes could not find a runway and would crash.

In 1997 I said to the Air Traffic Control Association: Jammers should be declared the fourth weapon of mass destruction.

VI. THE MISSING T

Sophisticated GNSS experts are now referring to PNT-positioning, navigation, and timing. GPS provides a precise stratum I atomic timing signal. For a long time no one said much about it. Not now, not since 9/11.

Many, perhaps most, of our modern IL networks depend on precise time in nano seconds-billionths of second-from GPS. Power grids, financial transactions, cell phones, data-transfers, and the internet are now dependent on GPS and will go down if GPS is disrupted. It is now understood that the greatest GPS vulnerability of developed nations is the loss of GNSS/GPS precise time.

Aviation interests should not think that they just use GPS for positioning. Take a close look at your comm. and surveillance systems. It is very likely that they use, or transmit data through systems that use, GPD precise time.

So: in aviation all three elements of CNS-communications, navigations and surveillance-are dependent on GPS.

VII. PROTECTION STRATEGIES

Here is the dilemma: how to take advantage of the wonderful things that GNSS can do without risk of going down in flames.

Most users of GPS/GNSS can lose the satellite service and get along well enough using the old methods. Back packers, cor navigation systems, farmers, surveyors, and users of hand helds are in this category.

But it is another matter where safety of life is at stake. Every aspect of aviation ATC, GN, and S-depend on GPS/GNSS for safety of life. Aviation is a classic safety of life service and cannot lose CN or S, ever. The same is true for marine nav systems, as the UK and Irish maritime agencies have recently stated.

There are a number of mitigation strategies designed to protect GNSS receivers from interference. Filters and antenna designs are on this list, and they are useful additions. However, almost no civil receivers are equipped with A) J features, and B) you can be sure that the advanced military jammers will always defeat the protections. If you are designing the AJ you will always leave a porthole for your own jammers.

The best protection, as the Volpe Center report pointed out, is a redundant dissimilar PNT system. At present the aviation users nav systems are protected because we retain ILS, VOR/DME, and inverted systems. This gives us virtually perfect protection because of the multitude of powerful, independent terrestrial transmitters. These have been described as costly and unnecessary by GNSS acolytes. I find them comforting and safe. In the oceanic and transpolar routes, GPD plus inertials will do the job nicely. If GPS is lost the MU system will get you home safely. But inertials alone will not serve in precision approach or even PNP terminal maneuvering.

VIII. ERGO WHAT?

I am delighted that the January 2005 CANSO publication “Demystifying GNSS” stated that GNSS is “most unlikely” to become a universal sole means of navigation. Three cheers for the CANSO ATC safety folks.

So the question arises, what do we retain as a backup to GNSS? Obviously we will keep all our ILS's, plus a high accuracy RNP 0.3 nav system. The DME/DME FMS's will do the job but are horribly expensive and the coverage for GA is poor.

Also, what does the retention of backup systems for every phase of flight do to the business case for augmentation systems such as WAAS-EGNOS and AAS' GBAS? There are lots of terrestrial users of SBAS and GBAS but I'm not sure the aviation should pay the whole cost.

IX. LORAN

Which brings me to my favorite subject-LORAN. At the dawn of GPS it was said that LORAN was useless old technology and deserves a decent funeral. What a difference a decade makes! LORAN is now the hottest new PNT technology in the world. The US is nearly finished with a nationwide modernization of its LORAN system. Secretary Mineta announced that enhanced LORAN-aka E-LORAN-can provide RNP 0.3 for aviation and harbor and entrance approaches for vessels. Of course, more of us in the LORAN mafia think LORAN is an alternative to GNSS. Instead, GNSS plus LORAN takes advantage of the splendid accuracy of GNSS and virtually removes the vulnerability risk. LORAN is the best friend GNSS ever had. For example….

- The 25 LORAN transmitters in the US, now fully modernized, can replace NOE-repeat NOE-VOR/DMES at about 1/10 the cost. I know, the airplanes aren't equipped with LORAN, so it will take time. And today everyone, even GA, is demanding that FAA cut costs. Why not pay for converted receivers by FAA and save $150 million per year?

- The LORAN transmitters can carry GPS augmentation signals a la WAAS. Why pay for GED satellites when you can get WAAS to the receivers for a one time cost to add to the LORAN transmitters of about $20 million. Some six northern European LORAN transmitters are doing just that right now. It's called Eurofix and was invented at the Technical University of Italy.

- LORAN, like GPS, transmits a precise, atomic time signal to Stratum One Standards. LORAN is the only available precise time backup to GPS. LORAN can make secure the entire IT telecom network in the world, most of which has no alternative primary source to GPS. Take note, ANSD's: your comm. And surveillance systems are probably at risk.

X. IN CONCLUSION

The movement to take advantage of the wonderful performance of GNSS has brought along a series of risks which we are only now comprehending.

We must…..

- Understand and accept the risk
- Sort through the available backup radio PNT systems, with their short and long term costs.
- Embrace modern LORAN