WWW.GPSWORLD.COM

GPS World

THE BUSINESS & TECHNOLOGY OF GNSS

NOVEMBER 2012

PNT with CURRENT COMPASS

PLUS

Aviation, Critical Infrastructure Needs
Cooperative Nav
Indoor Wi-Fi + MEMS + GNSS

The Need for a Robust, Precise Time and Frequency Alternative to GNSS

Mitch Narins, Per Enge, Ben Peterson, Sherman Lo, Yu-Hsuan Chen, Dennis Akos, and Michael Lombardi

Positioning, navigation, and timing (PNT) services are key enablers of both essential safety and security applications and economically beneficial capacity and efficiency applications worldwide. Whether users are ground-based, sea-based, or in the air, their primary/go-to source of PNT has become a GNSS, with GPS the most widely used. From the 2001 Volpe Center's GPS vulnerability report to the U.S. Department of Homeland Security's (DHS) GPS interference testing in 2012, the world has become much more aware of the vulnerability of GNSS-based services, particularly as the result of significant interest in using the spectrum directly adjacent to GPS for mobile communications services.

GNSS-supplied time and frequency support the vast majority of critical infrastructure sectors, but current services are not robust, and many users are not aware of their dependence upon GNSS.

While GNSS positioning and and navigation users are usually at least cognizant of the source of their services, many precise time and frequency users are oblivious to both the source of these services and their inherent vulnerability.

The Federal Aviation Administration (FAA) has initiated an Alternate Position, Navigation, and Timing (APNT) program to research alternative strategies. These strategies are necessary to ensure a safe, secure, and effective transition of the U.S. National Airspace System (NAS) to the Next-Generation Air Transportation System (NextGen). This column concentrates on the need for a robust time and frequency alternative to GNSS that will support aviation and have the potential to provide robust precise time and frequency services to other user communities.

The definition of robust that we prefer — as this is a systemic issue — is "the ability to overcome adverse conditions." Extrapolating this basic concept leads to this basic axiom: Robust time and frequency services denotes the provision of strong, sturdy, precise time and frequency services that are able to withstand or overcome adverse conditions. As we are dealing with radionavigation signals, the adverse conditions we must overcome can be categorized as interference.

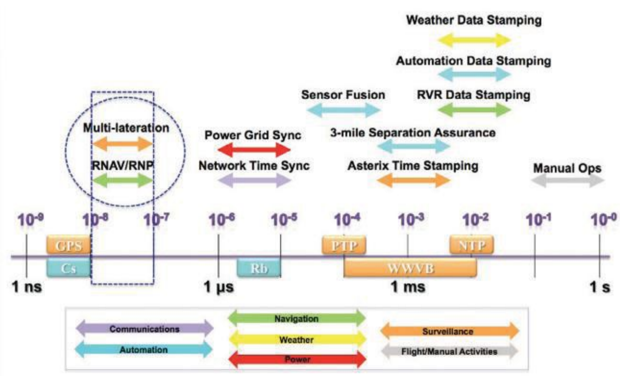
Radio-frequency interference can be intentional or unintentional; predictable or unpredictable; manmade or environmental; crude or sophisticated (jamming or spoofing); and/or widespread or localized. We envision a harsh radionavigation environment as one in which we must overcome some type of interference to arrive at the accuracy, availability, integrity, continuity, or coverage required by our specific applications. Additionally, in using the word "precise," we mean that the source of the robust time or frequency is accurate or stable enough to meet the needs of specific applications. This implies that the level of uncertainty is within acceptable parameters.

Timing is the means by which we precisely (accurately) position and navigate, the means by which we can safely and efficiently separate airplanes in flight. It has become increasingly apparent that it is through the denial or manipulation of precise timing that spoofers intend to adversely affect GNSS position and navigation users.

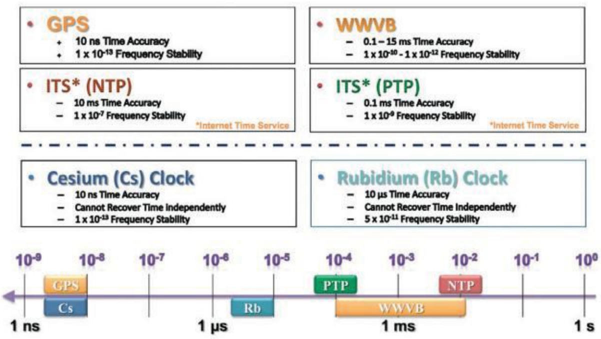
The problem is clear: current GNSS time and frequency are not robust, many users are not aware of their dependence on GNSS time and frequency, and GNSS time and frequency services support the vast majority of critical infrastructure/key resource (CIKR) sectors. **TABLE 1** lists the 18 CIKR sectors recognized by the DHS and shows that 15 of these rely on GNSS-provided time. As a part of the transportation sector, the FAA clearly recognizes the need for precise time and has

Critical Infrastructure/Key Resource Sector	Uses GPS Timing?	
	Yes	No
Communications Sector	✓	
Emergency Services Sector	✓	
Information Technology Sector	✓	
Banking & Finance Sector	✓	
Healthcare & Public Health Sector	✓	
Energy/Electric Power and Oil & Natural Gas SubSector	✓	
Nuclear Sector	✓	
Dams Sector	✓	
Chemical Sector	✓	
Critical Manufacturing	✓	
Defense Industrial Base Sectors	✓	
Postal & Shipping Sector	✓	
Transportation Sector	✓	
Government Facilities Sector	✓	
Commercial Facilities Sector	✓	
National Monuments and Icons Sector		✓
Agriculture and Food Sector		✓
Water and Wastewater Sector		✓

▲ **TABLE 1** Critical infrastructure/key resource sectors timing sources.



▲ **FIGURE 1** Current NAS precise time requirements.



▲ **FIGURE 2** Some sources of time and frequency.

maintained a significant non-GNSS based infrastructure to ensure the safety and security of the NAS; however, as the NAS migrates to NextGen, the need for precise PNT services, and hence for robust alternatives, will only increase.

FIGURE 1 shows the span of time users in the NAS, from the relatively unchallenging applications for which seconds will suffice down to the most discriminating applications requiring time slices measured in billionths of a second (nanoseconds). The most widespread use of time in the NAS is for the time-stamping of data. Every data transmission, from radar returns to voice communications, is time-stamped and retained as a means to review NAS operations and, if necessary, investigate incidents. As the FAA adopts the Asterix surveillance standard, all surveillance data will include a time stamp calculated to tens of milliseconds (ms).

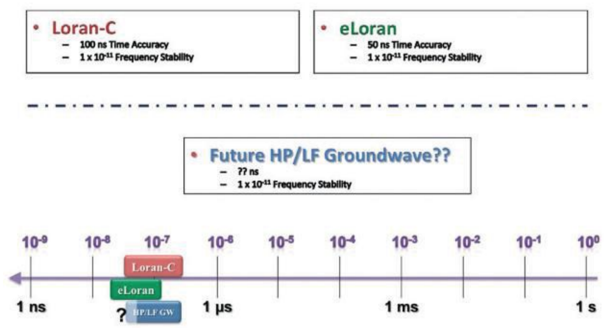
Communications networks rely on microsecond (µs) time, as does the electrical power grid. But the most discriminating users are those who utilize time for positioning. Remembering the rule of thumb that a nanosecond (ns) is approximately equal to a foot (~ 0.98357 feet), ensuring positioning to 10 meters (~ 32.81 feet) accuracy in a time difference of arrival system would require approximately 30-ns accuracy. Historically, many navigation systems have relied upon internal stable clocks to make less demanding measurements. The innovative solution employed by the developers of GPS to fly precise atomic clocks negated the need of such precision within user equipment. This availability of inexpensive, accurate, and highly reliable GNSS time has enabled advances throughout our critical infrastructure. To safeguard these advances, robust alternatives must be sought out and implemented.

FIGURE 2 shows some sources of time available to users. Although GPS' 10-ns accuracy far exceeds the requirements of the majority of users, its cost has become so miniscule in relation to other systems' components that it has become the most widely used precise time and frequency utility on Earth.

WWVB is a 60-kHz radio time service provided by the U.S. National Institutes of Science and Technology (NIST). Its performance at a user receiver depends in part on the ability to properly account for the propagation of ground wave, thus the 0.1- to 15-ms range in its accuracy. Still, it provides sufficient accuracy to many users. Thanks to the proliferation of the Internet, two means of distributing precise time are available to users: Network Time Protocol (NTP) enables derivation of precise time from many sources, both government and private sector (such as NIST, U.S, Naval Observatory, Microsoft, Apple), and the emerging Precise Time Protocol (PTP). With carefully controlled network architecture, time accuracies of 10 ms for NTP and 0.1 ms for PTP can be achieved.

Atomic clocks are routinely used throughout the infrastructure to provide precise time references, although not as widespread as many might think. Cesium standards provide time uncertainty equivalent to GNSS' 10 ns, while Rubidium standards can provide 10 µs. Note that while atomic standards can flywheel time quite well, they cannot independently recover accurate time if it is lost.

FIGURE 3 depicts the high-power, low-frequency ground



▲ **FIGURE 3** Other sources of time and frequency.

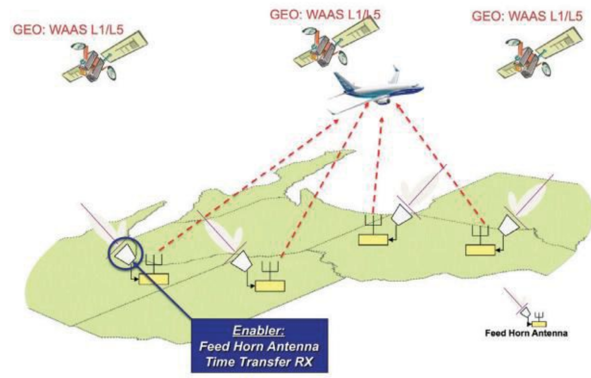
wave (HP/LF GW) alternatives. While Loran-C is no longer available in North America, its 100-ns accuracy is still being provided at many places in the world. Some of these locations have enhanced their original Loran-C coverage to provide improved time services that support 50-ns time delivery. Current DHS research seeks to determine if a new HP/LF GW can deliver an even more precise time service. These results have yet to be published, but may yet provide another robust alternative.

Robust Time Transfer

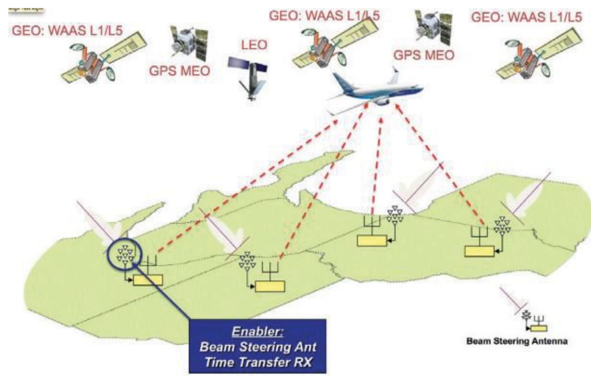
The challenge of robust time transfer, both on the ground and to aircraft, involves more than just accuracy. As with other aspects of PNT, there is an integrity component of time: can the information being provided be trusted? Recent demonstrations of spoofing based on exploiting receiver clocks highlight the need for both precise and authenticated sources of time.

Precise and authenticated time synchronization is an essential enabling element for two of the alternatives the FAA is exploring in its APNT initiative: the wide-area multi-lateration (WAM) alternative and the passive pseudo-ranging alternative. The goal is to provide a time service/source that allows APNT services to support a required navigation performance 0.3 (RNP 0.3) and to provide the navigation integrity and accuracy necessary for Automatic Dependent Surveillance-Broadcast (ADS-B) systems to support three-mile aircraft separation. GPS is the key enabler of this capability; however, because of its vulnerability to interference, it is critical that a robust APNT solution, able to overcome adverse condition, be provided in the event of GPS outages and interference. The availability of precise and trusted time synchronization is integral to achieving the navigation accuracy performance.

In addition to GPS outages and interference, there is a real need to guard against GPS spoofing, which has the potential for impacting safety and security. The availability of a robust PNT alternative that also provides users with precise time both on the ground and in the air can aid in the detection of and mitigation of such impacts.



▲ **FIGURE 4** Robust space-based time transfer.



▲ **FIGURE 5** Robust space-based time transfer, CRPA.

Robust Time-Transfer Alternatives

Highly Directional (Feedhorn) Antenna for space-based time/frequency synchronization is well recognized and well understood. There are many ways of using satellites for time transfer based on one-way measurements, for example, common view. The challenge, however, lies in the susceptibility of such sources to interference, both intentional and unintentional, jamming, and spoofing. Even low levels of interference can cause loss of lock and subsequent time/frequency synchronization issues for GPS.

A direct approach to overcoming interference is to mechanically prevent it from reaching your receiver by using a highly directional antenna to focus on the wanted signals and keep unwanted interferers at bay. This would be difficult and rather expensive if the source of the good and trusted signals were from moving satellites, and the antennas had to continuously and precisely track them. Thankfully, geostationary satellites (GEOs) can provide precise time services without the need for elaborate tracking mechanisms. Three of these GEOs are the ones employed by the FAA to provide Wide-Area Augmentation System (WAAS) services. WAAS is working to populate its Time Message — WAAS Message 12 to allow users to focus in on one of its three GEOs and derive time services; **FIGURE 4** depicts this potential solution. One must also note that this alternative is clearly limited to stationary users whose line-of-sight to the GEOs are unimpeded and for sufficiently long periods of time unchanging.

CRPA. While GEOs may provide an acceptable alternative for many fixed-base applications, they become problematic if the antenna doing the mechanical filtering is on a mobile platform such as an airplane, ship, truck, or person. It would be much better if the antenna itself could identify the source of good time and filter out the bad. For this, controlled-reception pattern antennas (CRPAs) are much better suited for prolonging the necessary service performance.

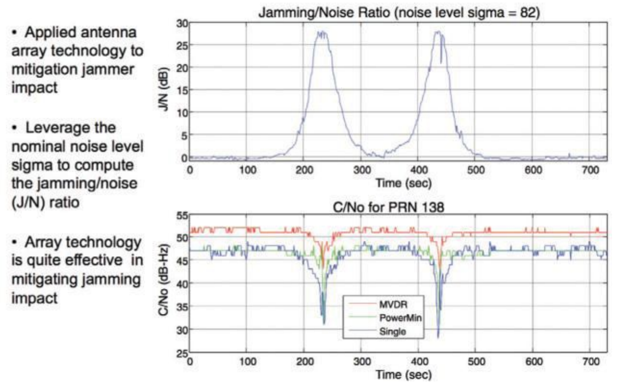
While CRPAs were first developed for military applications, commercially developed CRPAs are now available for non-military customers. For the threat of a single jammer considered here, CRPA antenna technology is extremely effective. While the military has utilized these applications for some time, some of the technology is now available for civilian applications as well.

Because CRPAs can reinforce wanted signals and attenuate unwanted ones, this solution is able to avail itself from signals emanating from medium- and low-altitude satellites (MEOs and LEOs) as well as GEOs, potentially making it a more robust alternative. **FIGURE 5** depicts this alternative.

The capability of a CRPA constructed by our Stanford University-based authors was demonstrated during recent trials at a DHS-sponsored GPS interference event conducted on the White Sands Missile Range in New Mexico. A 250-mW jammer was driven down a road; the Stanford equipment was set up 5 meters from the road. **FIGURE 6** shows the jammer approaching and passing the test setup, turning around, and passing a second time. It also shows CRPA response to the jammer, effectively providing more than 30 dB of protection to the receiver. Two types of CRPA processing were conducted: minimum variance distortionless response, which steers both beams and nulls, and power minimization, which only steers nulls.

Unlike the previous alternative, it is clear that CRPAs can provide robust solutions to both fixed and mobile users.

Wireless Ground-Based Sources. Within the NAS there are ground-based signals that have the potential to provide robust time transfer to aircraft. The ADS-B system, operating in the L-band, provides services via Universal Access Transmissions (UAT) at 978 MHz and on the Mode S Extended Squitter (ES) at 1090 MHz. The UAT signal structure already accommodates time and ranging, but is primarily used by



▲ **FIGURE 6** 250-mW jammer, CRPA results.

general aviation and business aircraft. Commercial aircraft use the Mode S ES service, which, while better suited to handle multipath due its larger bandwidth, has congestion issues.

Another alternative being explored is the use of ground-based pseudolites co-located with FAA's DME and ADS-B ground-based transmitter (GBT) sites. One means of utilizing pseudolites would be for each to broadcast its time of transmission and allow the aircraft to calculate the time of arrival. As DMEs in their normal mode provide true ranging, the combination of pseudolite and DME shows promise. However, it does require that all ground stations be precisely synchronized (remember a nanosecond is a foot!). An alternative means of using pseudolites is also being discussed. Proffered by researchers at Ohio University, it may be possible to use carrier-phase measurements of DME transmitters to derive position without the need to synchronize ground sites. This, along with other options, has not been ruled out.

Wire-Based Sources. As mentioned previously, precise time services (milliseconds down to microseconds) are available through wired sources. Recognizing the need for robust, GNSS-independent time as well as trusted sources, the FAA's Telecommunications Infrastructure has introduced both NTP and PTP services to ensure that air-traffic control facilities will be able to maintain their services in the event of a GNSS outage.

When using wire-based time services, it is important to ensure that the source of the data can be trusted and, especially with PTP, the forward and backward communications paths are the same. While an acceptable alternative to most users, wire-based services cannot currently fulfill the needs of nanosecond time users.

Important Conclusions

While concentrating on precision/accuracy, one must not lose sight of integrity. As we have become more and more aware of spoofing, users must ensure that the source of their precise time is from trusted sources, and one of the means to do this is through authentication. One definition of authentication describes it as "the mechanism whereby systems may securely identify their users. It provides answers to the questions: "Who is the user? Is the user really who he/she represents himself to be?" In our situation, the user is the one needing to authenticate the system, but the same principles apply.

For centuries people have used shared secrets to authenticate things: the secret password or passphrase or handshake. In the modern era of data transmission, we have migrated to more sophisticated means employing both public (known by all) and private (secret) keys. Because it is important to authenticate the source of time information, we have also begun investigating ways to incorporate authentication into our solutions by employing either a private key infrastructure or a symmetric key solution. The work is still in its early stages, and we mention it here to ensure that one does not forget to include authentication into the mechanism for achieving time precision. In summary:

- Time is an important GNSS product, often overlooked;
- Many users are not aware that they are dependent on GNSS time;
- GNSS is vulnerable!
- There are robust alternatives, and there is a need to identify and incorporate them into operations to ensure safety and security and to mitigate significant economic impact;
- Precise time is particularly important to certain discriminating ground-based and airborne users, in the NAS and elsewhere;
- For many applications, authentication is as important as accuracy; and
- Today's status quo may not/will not be an acceptable alternative in the future as GNSS services continue to proliferate and are used to support more and more critical operations.

MITCH NARINS is the chief systems engineer within the Federal Aviation Administration's (FAA) Navigation Programs office. He has served on the board of the Institute of Navigation (ION) and is a recipient of ION's Hayes Award. He continues to champion the need for robust PNT services to support aviation's and the world's critical infrastructure.

PER ENGE is the Kleiner Perkins professor of engineering at Stanford University; he directs the Stanford Center for Position, Navigation, and Time.

BEN PETERSON is a retired U.S. Coast Guard captain, former chair of the USCG Academy Engineering Department, and a member of the research staff in the Department of Aeronautics and Astronautics at Stanford.

SHERMAN LO is a senior research engineer at the Stanford GPS Laboratory. He is the Associate Investigator for the Stanford efforts on alternative position navigation and timing (APNT) for the FAA.

YU-HSUAN CHEN is a postdoctoral scholar in GPS Lab at Stanford University. He obtained his Ph.D and M.Sc. in electrical engineering from National Cheng Kung University, Taiwan.

DENNIS AKOS is an associate professor with the Aerospace Engineering Science Department at University of Colorado at Boulder, a visiting professor at Luleå Technical University, Finland, and a consulting associate professor with Stanford University. He completed his Ph.D. degree in electrical engineering at Ohio University.

MICHAEL LOMBARDI is a metrologist with the Time and Frequency Division of the National Institute of Standards and Technology in Boulder, Colorado.