SAASM and Direct P(Y) Signal Acquisition©

Steve Callaghan
Spirent Federal Systems

Hugo Fruehauf
Zyfer, Inc.

With the clock running out on a deadline for installing new generation global positioning system (GPS) security components on military platforms, two key contributors to GPS encryption technology describe how the Selective Availability Anti-Spoofing Module enables direct acquisition of the P(Y)-code and the benefits that capability brings to military and civil users alike.

Extensive field experience and technology advances have combined to bring new levels of sophistication to use of the Global Positioning System (GPS) Precise Positioning Service (PPS). The Selective Availability Anti-Spoofing Module (SAASM), a new GPS receiver design currently being incorporated into military and agency user equipment, promises a more robust operational capability as a result of advances in cryptography, *keying* techniques, and direct signal acquisition of the P(Y) code [Precision Code (GPS; encrypted Y code)]. These will alleviate the security risks and logistics faced by military users as well as eliminate the dependence on open coarse-acquisition (C/A) code for obtaining initial access to the P(Y) code itself.

This article will discuss some of the key technology innovations behind SAASM and its implications for operational use of the PPS, particularly in the SAASM's application to time and frequency generation and synchronization for communications systems and command/control terminals.

The Need for SAASM

Civil use of the Standard Positioning Service (SPS), based on the C/A code at the L1 frequency, has produced a huge international market in which millions of low-cost commercial receivers have already been sold for civil navigation and timing applications. This global dispersion of GPS technology, however, means that some of these receivers are also now in the hands of current and potential adversaries of the United States and their allies.

Today, anyone with a C/A-code receiver can navigate with at least 10-meter accuracy most of the time and synchronize to Coordinated Universal Time (UTC) within better than 100 nanoseconds. This proliferation of commercial GPS receivers poses a major dilemma: How to protect U.S. and allied forces from hostile use of the civil signal during critical military operations while sustaining operation of the worldwide infrastructures that have been built on civil GPS such as communication networks, surveying, positioning, and civil aviation. Essentially, the problem revolves around methods for denying use of the open SPS to adversaries while sustaining authorized user access to the encrypted PPS.

Military planners have done a very good job thinking their way through this scenario and have improvised clever ways to solve the problem. Until recently, using GPS called for making the *in-the-clear* civil signal available to all users, but not at full capability. During certain military operations, the C/A-code signal could be degraded even more, a technique called selective availability, or SA.

However, a fundamental change has taken place in the political context in which military leaders and GPS users operate – from global strategic conflict to tactical, localized warfare – and in the accompanying implications for user equipment design.

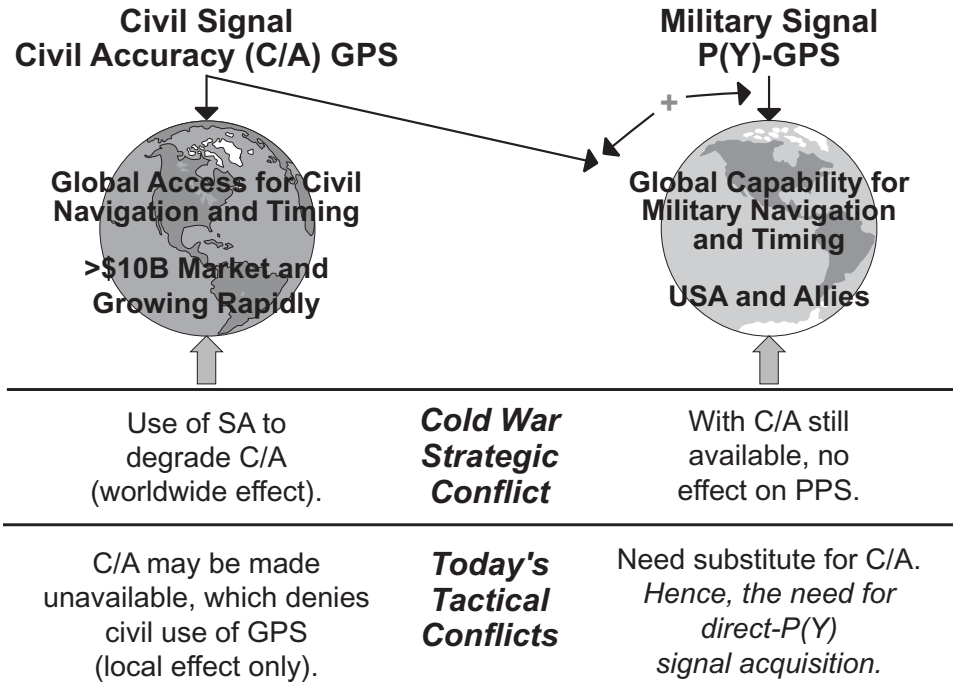
The Elimination of SA

The U.S. Air Force's satellite controllers can set the navigation and timing accuracy of the broadcast GPS signal to any level desired. Beginning in the early 1990s, the controllers intentionally degraded the civil C/A-code signal in GPS satellite transmissions to a horizontal positioning accuracy of about 100 meters, making the related vertical accuracy about 150 meters.

In May 2000, however, SA was turned off. This availability of the full-capability civil signal is the result of the new philosophy from U.S. military planners – to provide full civil accuracy, even with future enhancements and augmentations, while retaining the ability to locally deny the civil C/A signal in times of conflict.

This shift in thinking is actually quite profound. Previously, U.S. military planners relied on SA to make the civil signal unusable in case of a conflict, but the effect of SA cannot be applied regional-

Figure 1: *The New Warfare Realities*



ly and thus is worldwide in scope. Of course, during the Cold War, with its potential for strategic and global conflict, this seemed a reasonable approach. Today, however, with GPS integrated into almost every corner of our lives, the sweeping effects of SA would prove undesirable because they would be felt around the world. Consequently, the new scenario to deny the civil signal locally is very desirable, because it affects only a targeted region. The issues with strategic and tactical warfare scenarios are illustrated in Figure 1.

The Role of SAASM

Local denial of C/A instead of implementing SA has a drawback, however, and this is where one of the SAASM functionalities comes in: direct-P(Y) signal acquisition. The new warfighting environment requires authorized users to be equipped with receivers that allow them to continue using GPS signals while the *bad guys* cannot.

Traditionally, P(Y) code receivers need to initially access the C/A code transmitted by satellites, which repeats its pseudorandom noise (PRN) sequence every millisecond. This is needed to help acquire the encrypted military signal, which has a significantly longer PRN sequence. Use of C/A code enables the PPS receivers to obtain an accurate *time-tick* and with the transmitted hand-over word (HOW), enables alignment with the encrypted P(Y)-code (assuming the receiver has been crypto-keyed).

In the conventional SA signal-degradation scenario the civil signal is still present and, distorted as it may be, the PPS receiver can still use it to initialize. In a theater of operations in which C/A code is denied, however, a SAASM receiver with direct P(Y) code acquisition is the only practical option for continued use of GPS. A less desirable alternative is to have a precise (atomic) cesium clock in the user equipment that provides the ability to synchronize with the P(Y) code, an option not practically available to most users for various reasons, including cost, size, and weight disadvantages. We will discuss the other SAASM receiver functionalities next and return to a more detailed discussion of direct-P(Y) later.

Fielding SAASM

Most observers acknowledge that the military establishment as a whole lags far behind the commercial industry in the availability of state-of-the-art GPS receivers. Of course, many soldiers have commercial receivers, but these do not substitute for PPS receivers. The fielding of military PPS receivers has improved recently, but equipping of U.S. and allied military forces with the new SAASM hardware needs to be expedited for reasons that will become obvious in the course of this article.

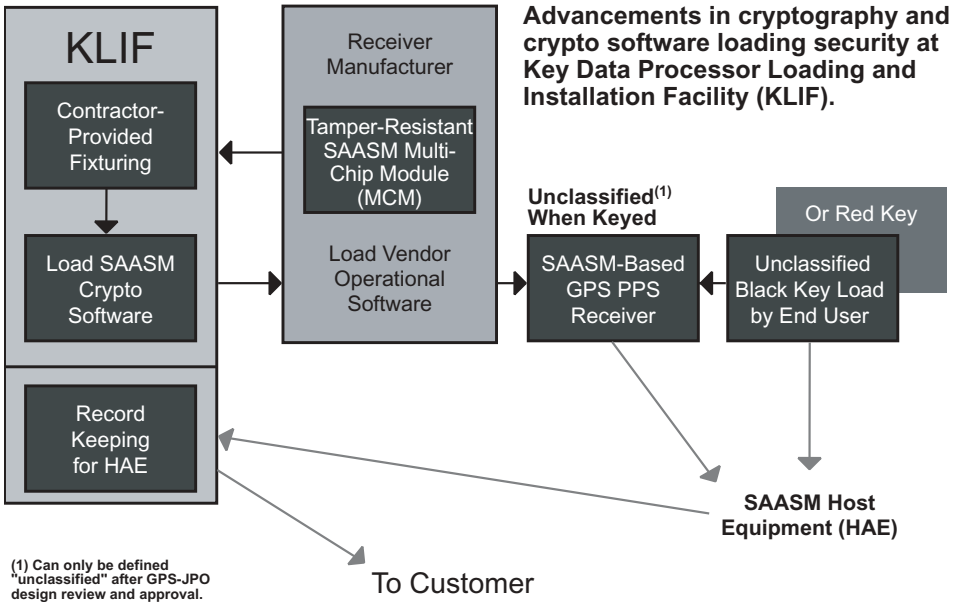


Figure 2: *Black-Key Software Loading Process*

> *"The new warfighting environment requires authorized users to be equipped with receivers that allow them to continue using GPS signals while the bad guys cannot."*

The logistically intensive nature of current-technology PPS hardware has slowed the distribution of equipment. Classification considerations surrounding distribution, use, and disposal of *crypto keys* as well as issues involving hardware, whether keyed or not, have contributed to this situation. If a current-technology PPS receiver falls into the wrong hands, key security may be compromised for a time, and long-range effects will be felt after the hardware is analyzed by a foe. No doubt, this fact has contributed to the phenomenon of PPS hardware reaching higher-ranking military officers first rather than combatants in the field.

Although SAASM is mostly understood as the new military GPS navigation receiver technology, it also will provide less well-known benefits for communications, time/frequency synchronization, and command/control terminals. Before exploring these benefits, it will serve us well to first understand the overall SAASM infrastructure.

The Security Boundary

SAASM inventors have come a long way toward making PPS receiver hardware more user-friendly and securely deployable. Having created a tamper-resistant security module for the most sensitive signal processing and cryptography functions of the receiver provides two important security improvements.

First, the software is very carefully controlled. As a matter of fact, the Key Data Processor (KDP) Loading and Installation Facility (KLIF) is the only place where the crypto software can be loaded. All SAASM receiver manufacturers must cycle their hardware through the KLIF. This so-called black-key software loading process is shown in Figure 2. Second, the tamper-resistant module provides physical security, significantly reducing the risk of compromise should the receiver fall into enemy hands. Figure 3 (see page 14) shows a typical SAASM receiver architecture with its tamper-resistant security module and the direct-P(Y)-code parallel correlator.

When a receiver is built into Host Application Equipment (HAE), the KLIF again enters the picture to reregister the final destination of the SAASM receiver hardware. Although the build-flow of the receiver is more complicated

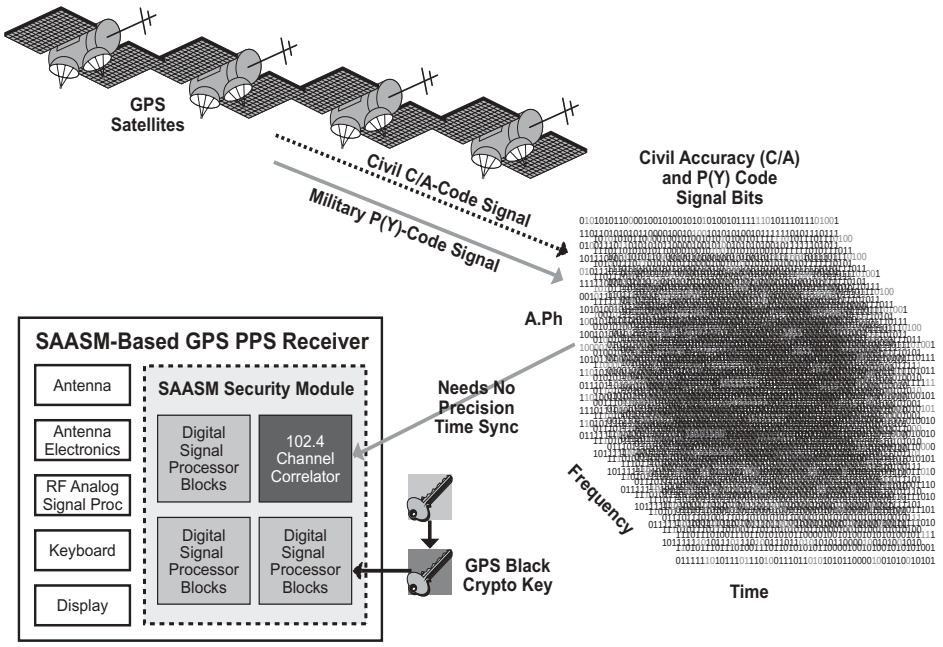


Figure 3: *Typical SAASM Receiver Architecture*

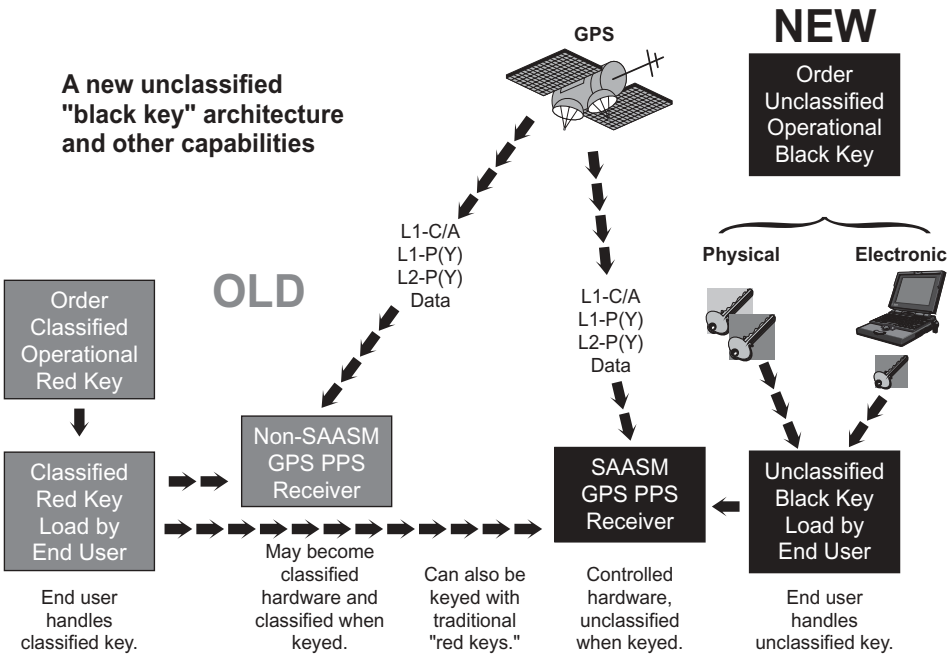
for the manufacturer as a result of the KLIF, the keying is simpler for the user and the hardware is unclassified, assuming that the HAE has been certified by the GPS Joint Program Office. The increased manufacturing complexity of the SAASM receiver comes from the fact that the receiver must be built in two sections, one being the security module and the other the motherboard to which the security module is attached after the KLIF software loading cycle.

The Black-Key Infrastructure

In addition to the security module and the secure software loading process, the keying architecture is being changed from a classified *red-key* infrastructure to an unclassified black-key approach. The current red keys require physical transfer of certain key and key elements to the user by secure means. This is generally called a *symmetric* or secret key architecture.

The symmetric approach creates a host of logistic issues, not the least of which are distribution, control, storage, and disposal of keys and key material. The SAASM black-key architecture on the other hand combines two cryptography methods – the symmetric key structure and what is called an *asymmetric key*.

Figure 4: *Old Versus New Black-Key Keying Process*



The asymmetric key technique has long been the basis for the public key infrastructure (PKI). The public key of a person or agency in the public key database is combined with a private key known only by its holder. The combined, mathematically related keys encrypt and decrypt information transferred cryptographically from point A to point B without keys being transferred in the process.

To obtain a maximum level of security and infrastructure synergism, SAASM combines the best of both techniques: It uses asymmetric key cryptography to securely transfer the symmetric key to the PPS user in an electronic fashion.

Most importantly, however, and contrary to the current PPS structure, the black key physically transferred is unclassified because the key itself is encrypted. This old versus new keying process is shown in Figure 4.

In addition to the black-key keying process, the SAASM receiver has been outfitted with other sophisticated capabilities to further enhance its operational usefulness for the PPS user.

Direct P(Y)-Code Signal Acquisition

As mentioned earlier, P(Y)-code receivers have needed to initially access the C/A code in order to obtain an accurate time-tick enabling them to access the much longer P-code.

Until recently, direct acquisition of the military P(Y)-code signal without a very accurate clock was not practical or even possible. However, advances in signal processing speed and micro-miniaturization now allow for massive parallel data processing and bit correlation to compensate for the lack of accurate time. A comparison of the traditional PPS receiver with the SAASM direct P(Y) acquisition receiver is functionally demonstrated in Figure 5.

A key element in direct P(Y) code acquisition is the number of signal correlator channels and processing *bins* available in a receiver to match up locally generated PRN codes with the codes transmitted by the satellites. Figure 6 compares the C/A-code search process, which may employ only a few correlator channels, with the direct P(Y) acquisition process, using massive parallel signal processing with 1,024 or even 2,048 correlator channels searching for a code match. Depending on the number of correlators and the receiver design, the external time reference used to initialize the direct P(Y) SAASM receiver can now be a factor of 10,000 to 10 million less accurate than

before.

This means its UTC time reference can be off as much as ±1 second or so instead of the previous 100 nanoseconds. (Throughout this article, the reference to UTC is done for convenience. There is actually a time difference between UTC and GPS system time. This is due to the fact that UTC is maintained using *Leap-Second* updates, whereas GPS time is pure atomic time. The GPS system tracks leap seconds separately so that users can choose GPS time or UTC. The differences in these time scales are not germane to the discussions here.)

The receiver's P(Y)-code signal-acquisition time, generally referred to as the *time to first fix* (TTFF), is mainly a function of how well the initialization time reference is known and the severity of the jamming environment.

SAASM and Time/Frequency Users

In addition to a host of advantages for military applications in terms of navigation, positioning, and weapons targeting, SAASM brings benefits to the time and frequency synchronization community as well. Civil and P-code-equipped GPS time and frequency systems play a major role in both ground and space-based communications and command/control operations.

Three main categories of GPS-equipped communication terminals exist today.

- **The conventional C/A-only SPS terminal.** When the civil C/A signal is unavailable, this category of GPS-aided terminal goes into so-called *holdover* mode, using its internal oscillators. It eventually goes out of spec or down altogether if the C/A signal is not restored. Unfortunately, this category is by far the most widely deployed terminal for commercial and military applications.
- **The conventional military C/A-P(Y) PPS terminal.** Here, the situation is improved somewhat. If the terminal is operating on the P(Y) signal at the time that a C/A-code signal becomes unavailable, the receiver will stay online. However, if the P(Y)-code signal is interrupted or a power failure occurs, the system cannot reacquire the military P(Y) signal in the absence of C/A.
- **The new SAASM Direct P(Y) PPS terminal.** Not only will this category of terminal stay online without a C/A signal, but it can also start *cold* without it. SAASM goes a long way towards protecting the terminals against hostile jamming and spoofing. In a world facing terrorism threats, military and agency infrastructures should not only adopt SAASM technology, but high-value commercial assets should also become authorized users of SAASM. (*Authorized* refers to users who have government-approved security infrastructures in place and are authorized to receive crypto keys.)

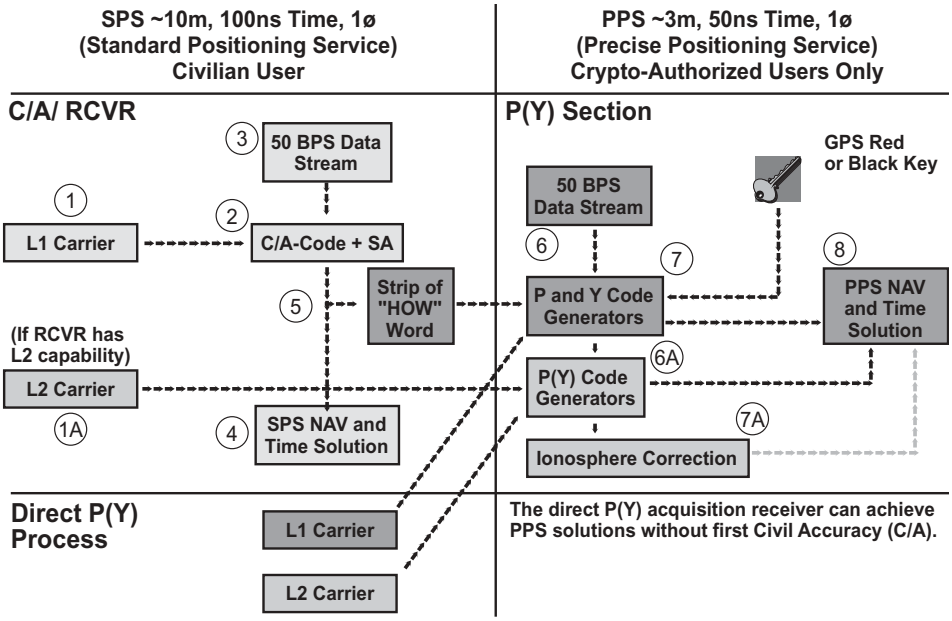


Figure 5: *Traditional PPS Versus SAASM Direct P(Y) Functionality*

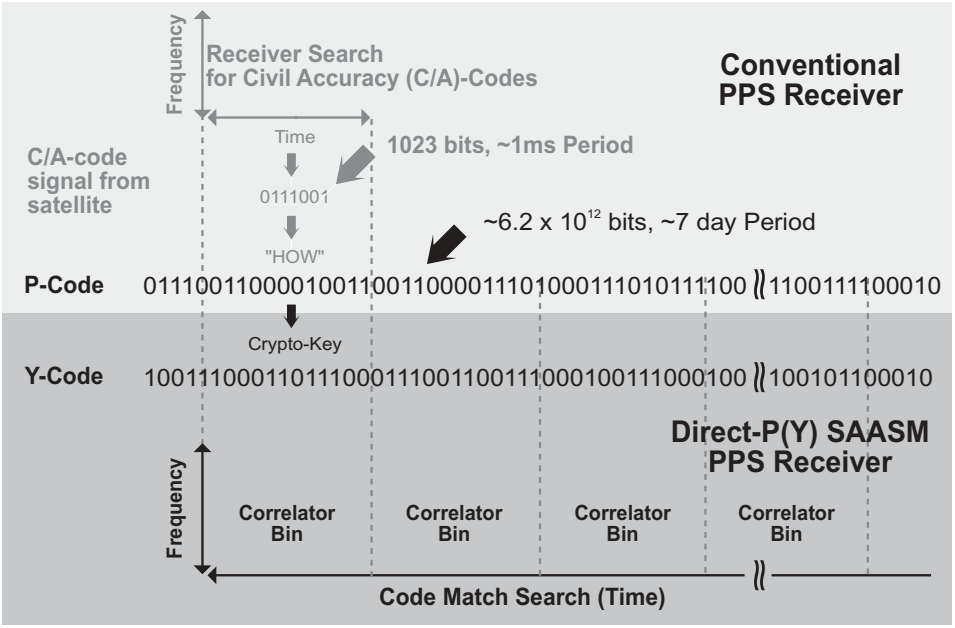
Types of Direct P(Y) SAASM Receivers

Two primary categories of direct P(Y) SAASM receivers exist, each with different operational requirements and values of initialization parameters – the weapons navigation/targeting receiver, such as might be incorporated onto a rocket or artillery projectile, and the communications time/frequency receiver.

The weapons navigation/targeting receiver must have the capability to acquire the P(Y) signal very rapidly in the absence of C/A, because the weapon's flight time may only be a minute or so. To facilitate rapid acquisition, the GPS host platform provides the weapon's receiver with very accurate initialization parameters, such as projectile position as it exits the launch tube, and GPS time.

Although the GPS host platform can provide the weapon to be launched with a time accurate to better than 100 nanoseconds, the accuracy is subsequently degraded by the effects of the launch environment on the weapon's GPS

Figure 6: *Conventional Search Versus Massive Parallel Signal Processing*



receiver oscillator. As a result of the requirements and the support available from the GPS host platform, the weapons receiver can deal with a time uncertainty of milliseconds and a position inaccuracy within a few meters. Only several hundred parallel correlator channels are needed to satisfy rapid P(Y)-code acquisition.

In comparison, the communications time/frequency receiver generally does not need to acquire satellite signals as rapidly as its weapons system counterpart, mainly because it is assumed to be stationary or moving not faster than a truck. More importantly, however, it does not have the benefit of a GPS host platform system – in other words, it has to operate on its own. Since acquisition time is generally not a driver, the initialization parameters can be significantly less precise, for example, time uncertainty in the seconds. As a result, this category of receiver is correlator-intensive, requiring at least 1,000 or more correlation channels to handle the relatively large position and time uncertainty.

As discussed earlier, the TTFF is mainly a function of how accurately the initialization parameters can be specified, especially time, which in turn determines the size of the P(Y) signal bit-field to be searched. Initialization data can either be provided automatically, as in the case of the GPS host platform and weapons receiver, or by keypad entry or use of a portable clock as in the case of communications time/frequency receiver.

One additional element is the GPS almanac broadcast in the GPS satellites' navigation message, which plays an important role in the acquisition initialization process. The almanac is a library of satellite information, including estimates of satellite ephemerides (orbital positions) and a host of other parameters needed for the receiver to determine its own position.

The almanac that a receiver has loaded in its memory since the last time it received GPS signals should not be older than a week. Without access to the C/A-code signal, a receiver making a cold start cannot obtain the broadcast ephemerides of the satellites it is attempting to acquire. As a result, the receiver uses a stored almanac or *library* to estimate satellite positions. Because the GPS constellation is relatively stable, a week-old almanac should do the job, but a younger data set will speed up the TTFF process.

For the wristwatch initialization, the receiver will use the latest almanac in its memory – the one loaded during the last time the receiver was on-line. Using a portable clock for initialization brings the added advantage of the latest almanac stored in its memory. Its dataset will likely be only a day or so old, again, as recent as the last time the portable clock was in the standby mode receiving the C/A signal.

The SAASM Mandate

In 1998 the chairman of the Joint Chiefs of Staff issued a SAASM deployment mandate. It requires PPS users to procure SAASM only, use black keys only, and cease fielding non-SAASM GPS equipment after Oct. 1, 2002. This mandate has not changed since then, and waivers must be requested for non-compliance.

Also, The Department of Defense has revised security regulations for builders of host applications equipment. Makers of such equipment must first have a government security structure in place and, additionally, must go through rigorous design reviews of their HAE architecture. A list of authorized SAASM receiver and SAASM HAE developers may be accessed through the GPS Joint Program Office Web site at <http://gps.losangeles.af.mil>.

Conclusion

The SAASM receiver and its direct P(Y)-code acquisition capability will prove to be a powerful tool in the hands of our military and authorized users. What C/A has done for the GPS boom in civil community, SAASM will do for the military user and authorized community. SAASM provides solutions for some very critical operational complexities:

- Depending on the design of the HAE, the equipment fielded will be unclassified, even after keying.
- It makes for a more secure receiver were it to fall into the hands of adversaries determined to compromise our crypto technology secrets and crypto keys.
- The crypto black keys are unclassified and can be distributed in an unclassified manner.
- The receiver can acquire the military crypto signal directly without the aid of the civil C/A-code signal.

As a result, civil and military users can enjoy a symbiotic relationship, allowing full-accuracy civil GPS SPS operations while protecting our military from adversaries using civil GPS in an area of military conflict. The military is on a fast track according to the latest Joint Chiefs of Staff mandate – no non-SAASM-based GPS hardware can be fielded after the year 2002 without a waiver.◆

Original Article

This article was originally published in *GPS World* and is available at <www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=25974&pageID=1>. GPS World is a monthly business-to-business publication focusing on innovations and best practices that provide a competitive edge for the user/developer community employing global positioning and timing technologies.

About the Authors

Steve Callaghan is director of engineering for Spirent Federal Systems. Previously, he served as chief systems engineer and architect for the NAVSTAR GPS selective availability antispoofing module (SAASM) and key data processor program and was responsible for the design of related security algorithms and approval processes. In February 2002, he received a Joint Staff certificate of appreciation for his support of the GPS precise positioning service SAASM security architecture. He has a Bachelor of Science in biomedical and electrical engineering from the University of Southern California.

Hugo Fruehauf is president, chief executive officer, and chief technology officer of Zyfer, Inc., a wholly owned subsidiary of Odetics, Inc. He was the chief engineer for the design and development of the initial Block I GPS satellite system for Rockwell International (now Boeing). Since then, he has focused on GPS applications for communications, time and frequency synchronization, network data security, and tactical weapon systems targeting. While group vice president at Alliant Techsystems, he influenced the development of the first SAASM receiver and the direct-P(Y) code acquisition functionality. He is a graduate of DeVry Institute of Technology in electronic engineering.