

Saving SAASM

by Robert Huffman

I recently picked up the February issue of *GPS World* and was quite interested in Glen Gibbons' editorial concerning the current state of GPS and how much it is being taken for granted. To borrow Glen's words, "GPS is not some big smorgasbord in the sky, a natural phenomenon like the sun, or an inexhaustible and free cornucopia of precise positioning and timing."

From both the commercial and defense perspective, these words ring a nagging truth. From the military point of view, it's even more critical that we not fall into the trap of relying on GPS for precise positioning without going to great lengths to protect the integrity of the GPS signal. No one knows this better than the Air Force Joint Program Office (JPO), which has been working to improve security provisions for military GPS for some time.

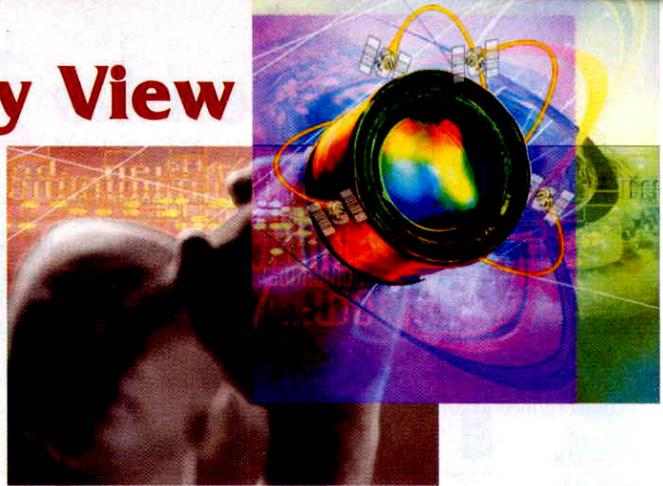
In recent years, the JPO plan to create a highly secure GPS receiver architecture has resulted in the development and certification of selective availability/anti-spoofing modules (SAASMs). This innovation replaces the precise positioning service-security module (PPS-SM) and auxiliary output chips (AOCs) now used by military GPS receivers to remove selective availability and to track the encrypted Y-code. This legacy PPS-SM/AOC technology will soon be obsolete and unavailable.

A pivotal point of military GPS technology, SAASM has been a hot button for quite some time. In fact, many in the GPS community have heard speculation that SAASM is just too hard to implement, and, therefore, won't happen. "Let's just wait a few more years for the new military signal (M-code)," seems to be the conclusion of this line of thinking.

Talk about taking the GPS signal for granted! Who really knows how long a few more years will be? Although M-code will answer many of the security issues for the future, what about the present? The M-code signal will be implemented on 12 modified Block IIR and 12 modified Block IIF satellites, that are planned for launch between 2005 and 2010. Under the present launch scenario, an operational constellation of 18 M-code satellites will not come into operation until 2016. M-code-capable receivers may become available in 2008 at the earliest. Program managers will have to decide when to convert from SAASM in 2002 to M-code in 2008. With the nation presently fighting a war against terrorism, this is not the time to take backward steps.

From a military perspective, we all understand the need for protection. As a national asset, GPS is increasingly becoming the golden arrow that leads us to battle. The loss of this golden arrow would be a major step backwards. Threats to the United States and allied forces' ability to provide precision guided capability to their weaponry are real and must be countered now, not in 2008 or later.

SAASM clearly provides a solid set of upgraded security features. For instance, SAASM-based products can acquire the Y-



code directly, allowing warfighters to minimize dependence on the civil signal structure susceptible to interference and jamming. This advantage is realized in a 10- to 20-dB antijam margin with direct-Y-code acquisition.

Advances in materials, fabrication processes, and production equipment have substantially increased the efficiency of SAASM manufacturing. The antitamper-coating process has matured to the point that production yields approach 95 percent or more. Quality design and component-handling practices adopted from the commercial industry have also aided in the process improvements during the past two years.

Meanwhile, new cryptological methodologies have replaced the highly cumbersome and antiquated paper-tape method for delivery of key data, allowing the development, transfer, and

"SAASM is real and ready to go."

storage of SAASM crypto-keys to be provided as unclassified information. This simplification of the delivery infrastructure allows the keys to be handled and maintained at an unclassified level.

Additional innovative features such as over-the-air rekeying, satellite authentication, and contingency recovery have enhanced the functionality of a SAASM-based design over the one implemented in legacy technology. This mountain of new capability at times looked unscalable. As the result of heavy investments by government and corporate America, however, new SAASM technology is here and ready to take its place in GPS history as the next enabler for the warfighter. SAASM is the right solution for today and is, without doubt, a better security solution than the current PPS-SM architecture.

The point of my concern is, simply, let's not take the GPS signal for granted. For those who don't believe SAASM is real or doable, I invite them to visit any of the GPS contractors who have worked hard to make this new capability a success. SAASM is real and ready to go. ☺



Robert Huffman

became president of Interstate Electronics Corporation (IEC), a division of L-3 Communications, in October, 2001. He previously served as IEC's vice-president of marketing and sales and vice-president of engineering, and has worked at IEC since 1984. He has a B.S. in electronic engineering from California State Polytechnic University.