



PATHFINDER

An informal newsletter published for the GPS user community by PM GPS. Information presented is based on published and submitted news items of interest to the general user. Widest dissemination and reproduction is encouraged. Newsworthy items are solicited for inclusion. Editor Mr. Don Mulligan at PM GPS, PM NAV SYS, Ft Monmouth NJ DSN 992-6137 or (732) 532-6137 or email: Donald.Mulligan@iew.s.monmouth.army.mil

Volume 11 Issue 2

Website: <http://army-gps.robins.af.mil>

April 2004

Signal Security for GPS Receivers !

PM's Corner



I am pleased to report we have received Milestone C Decisions for both next-generation GPS products! We have Low Rate Initial Production Approval for the Defense Advanced GPS Receiver (DAGR) handheld receiver. We also have Full-Rate Production Approval for the Ground-Based GPS Receiver Applications Module (GB-GRAM).

With these production approvals in hand we are now finalizing the DAGR Fielding Plan to begin equipping Army units with this lightweight state-of-the-art technology later this year!

At the same time, many weapons system managers are starting to embed the GB-GRAM in communications, navigation, vehicular and other systems to reduce overall size/weight and to eliminate cable-connected PLGR.

The October 2003 and January 2004 PATHFINDER have product details on DAGR and GB-GRAM. You can download those issues from the Army GPS website at <http://army-gps.robins.af.mil>.

This issue also highlights my concern for signal security. If you have questions, please contact me or my staff.

Skip Harborth, LTC, SC

Product Manager, GPS



The only PPS-rated handheld GPS receivers authorized for combat, DAGR on the left and PLGR on the right.

There is a critical distinction between SECURE and NON-SECURE GPS!

SECURE GPS means a receiver is equipped to access the Precise Positioning Service (PPS) signal! Only receivers purchased through the GPS Joint Program Office (JPO) and equipped with an approved security module and operating with COMSEC crypto-variable keys can access the PPS signal for enhanced accuracy, anti-jam and anti-spoof protections.

Using a military receiver without COMSEC or using a commercial GPS receiver equals NON-SECURE GPS. That could endanger your mission because you face a greater risk of signal interference or you might be spoofed and never even know it.

There is no commercial substitute for SECURE GPS!

How Can we Recognize and Counter GPS Jamming?

This article assumes the use of PLGR but the procedures apply to any GPS receiver

1. Basics about the GPS signal:

Low Power: GPS satellites transmit a low power signal which travels over 10,000 Nautical Miles to reach you. By then the power is below the local noise level so the GPS signal is susceptible to local interference.

Line-of-Sight: Like all radio signals, GPS relies on line-of-sight signal reception. Fortunately, the GPS satellites are high in the sky which allows the signals to reach you where terrain or structures may block signals coming from ground-based emitters. Even so, significant terrain features, heavy wet foliage or dense buildings, such as in an "urban canyon" can still disrupt the GPS signal.

At low angles (5-10 degrees) the signal from satellites on the horizon may also be distorted by atmospheric conditions.

Wide Coverage: Again thanks to the high-in-the-sky position, GPS has a very wide coverage area that is hard to jam completely. GPS receivers are designed to look for and collect signals from all directions.

Multiple Satellites: GPS is not dependent on a few satellites. There are 24 satellites on-orbit with a minimum of 4 in-view at any given time so a GPS receiver can usually 'find an alternate' when one satellite is temporarily blocked.

Your awareness of these strengths and weaknesses can improve your ability to detect and react to interference.

2. Basics about Signal Interference

Interference is defined as the radiation, emission or indication of electromagnetic energy, unintentionally causing degradation, disruption or obstruction of the function of the electronic equipment affected.

Okay, so how do we recognize the symptoms of GPS Jamming?

Some signal interference will be obvious, such as a display of erratic position location or speed.

Some signal interference will not be so obvious but, can still have the effect of gradually deteriorating the accuracy of information being displayed. Therefore it may be a good idea to periodically check your receiver's Accuracy Indicators as part of the mission routine. PLGR

has two such indicators: The Figure of Merit (FOM) and the Satellite Tracking Status page.

Your FOM reflects accuracy of position calculation (Table 3.7 in PLGR TM). In general, a FOM of 5 or higher in what appears to be a clear environment is reason to look for possible signal interference.

The Satellite Tracking Status Page will display the carrier-to-noise ratio (CN value) or

the amount of "noise" or potential interference in the signal. The acceptable range for CN values is 25-50db with 34db being the expected 'average' CN value. If your PLGR is showing CN values lower than 34db, you may be experiencing signal interference.

Outside of the PLGR Accuracy Indicators, what are the typical environmental factors that may cause signal interference?

Interference may come from natural phenomena or man-made sources, including:

1. **Masking:** A heavy canopy of wet foliage, a deep ravine or urban canyon can block line-of-sight to the sky. Your own body can also mask signals if you hold the PLGR too closely.
2. **Equipment malfunction:** Your GPS receiver may develop an internal fault or a nearby emitter may be experiencing a mechanical malfunction.

Warfighter awareness is critical.

Every user needs to:

- **Know the basics about the GPS signal**
- **Recognize the symptoms of GPS jamming.**
- **Identify the likely sources of interference.**
- **Know actions to reduce the effect.**
- **Know how to report interference problems when local procedures don't resolve the effect.**

Some Interference can be resolved before it occurs: Prevention through Mission Planning!

Address potential frequency interference before the mission by assessing the type of communications equipment to be used on the mission. Look at their operating frequencies. Use Frequency Management Procedures to take steps to avoid operating on L band frequencies near the GPS signals (L1: 1575.42 and L2: 1227.6 Mhz)

3. Unintentional Radio Interference: The proximity of your GPS receiver to L-band radio transmitters is a frequent source of trouble. It may be a radio collocated on the same vehicle or more likely, temporary proximity to a nearby radio transmitter.

4. Electromagnetic Interference (EMI): Similar to item 3 above but EMI may affect a larger number of users simultaneously. EMI conflicts may arise among weapons systems and even among components within weapons systems. This issue includes spectrum interference, meaning the broadcast frequencies used by various weapons systems. "De-conflicting" sometimes means changing frequencies and for obvious reasons this has to be managed by the Spectrum Manager at a central higher command in order to maintain connectivity and communications.

5. Intentional Jamming: This is an outright attempt to interfere with GPS. Low cost jammers can be set up with relative ease but they can also be located and eliminated when friendly forces are on alert for the potential and have the assets to address the threat. The more powerful the jammer, the more likely it is to be identified and eliminated.

Q: What can we do at the field level to mitigate the impact of jamming?

If the interference appears to be caused by masking, move the GPS receiver to restore signal reception. If the operational situation precludes moving, try to determine the direction the interference is coming from and get something between you and that direction to block the signal. If you are not moving, activate the Low Signal – Dense Foliage operating feature in PLGR; This uses Averaging Mode and you must remain stationary for the PLGR to make the best of available signals. In any case you have to deal with compromised GPS accuracy until you can move to a position that restores signal reception.

To verify a possible GPS receiver fault, switch to a different GPS receiver and see if it operates effectively where yours did not. If you suspect a fault with some nearby emitter, ask that system crew to check diagnostics for function, proper settings and antenna orientation. If it was a faulty GPS receiver, return it for repair!

If it appears to be a case of radio interference, are you too close to an external emitter? The solution may be as simple as moving away from it! Did you install another emit-

ter on the vehicle with your PLGR? Installation Kits are designed to eliminate conflict through careful placement of antenna and the use of shielded cables when placing PLGR on a vehicle with other radio transmitters. A local "field expedient" modification may not account for such design efforts. For handheld PLGR, try low angle shielding of the antenna to block interference from ground-based devices.

Q: If we can't eliminate the interference through local actions, how do we report it?

If the interference appears to be affecting a wide area or a large number of users, and there is no obvious local source, it may be time for the Unit Signal Officer to submit an Interference Report. The process varies by command and the following article briefly discusses the topic. Field unit Interference Reports provide the

"More than one operator has driven up to a TOC full of emitters and been surprised to find his GPS receiver is overwhelmed by the electromagnetic atmosphere! Move away to regain clear signals!"

basis for taking action at higher command level. Each Service has procedures to assess and remedy Electromagnetic Interference (EMI) issues. Ultimately, the Joint Spectrum Center is the DoD center for resolution of EMI conflicts. The JSC evaluates the source (commercial, DoD, Non-DoD, Host Nation or Coa-

lition Forces) and coordinates action at the appropriate level to resolve friendly conflicts or to eliminate hostile interference.

In the meantime, when interference is beyond your ability to influence, you have to deal with compromised GPS until the situation is resolved.

Conclusions:

Like any system that relies on radio signals, GPS signals may be vulnerable to interference.

Field operators need to be aware of both obvious and not-so obvious sources of potential interference.

Your fundamental countermeasure to GPS signal interference is Situational Awareness! Use GPS as an Aid to Navigation, not a substitute for navigation skills including terrain orientation & map-reading. Never become so dependent on GPS that you can't continue the mission without it!

Interference that cannot be resolved at the local level should be reported via the Interference Report.

Other key defenses include: Always operate with COMSEC crypto-keys; a

keyed PLGR has a higher level of protection against jamming; Be aware of the impact of terrain, structures and your proximity to other L-band receivers or transmitters.

For more information review FM 24-33 or contact Tony Callanan at JPO, DSN 833-2914.

The MIJI Report

Under Battlefield Spectrum Management, the Signal Officer is responsible for "Interference Resolution" at the lowest level possible. Often the problem can be traced to a local signal device (friendly radio or radar), non-signal device (welder or vehicle engines) or technical difficulties with some emitter device. When the unit determines signal interference is NOT being caused by a local source and cannot be resolved, it is time to submit an Interference Report.

Check with your Signal Officer about the proper format and routing of the Interference Report. Commands vary in organization as to whether the G2 or Electronic Warfare Officer (EWO) handles reports of unresolved interference. At higher levels of command the Meaconing, Interference, Jamming and Intrusion (MIJI) report is generated on the basis of Interference Reports coming from subordinate units.

The MIJI report advises the chain of command of unresolved interference and it may go to Theater Level and the Joint Spectrum Center where resources can locate and eliminate hostile interference.

For MIJI report procedures, see AR 105-3, "Reporting MIJI of Electromagnetic Systems", 31 Jul 1986.

SPOOFING THE GPS SIGNAL

Spoofing is a very different kind of interference. The "Spoofers" doesn't want you to know he is there. He doesn't want you to question the accuracy of your GPS data. His intent is to deceive you by generating a signal that mimics a satellite signal. He does this to insert a false value into your GPS calculations, thus creating errors in navigation or position data. He wants to lead you astray while you think your GPS data is correct. A spoofer can cause an un-keyed GPS guided munition to impact away from the intended target, causing collateral damage. Also, spoofed handheld GPS users may call in artillery fire or Close Air Support on erroneous locations. Spoofers are dangerous and devious.

In an unclassified newsletter we can't get into more detail but spoofing is hard to detect.

The best defense against spoofing is the consistent use of COMSEC crypto-variable keys to generate the "Y-code". To detect a "Spoofers", cross-check your GPS display for position against your map and terrain association. And cross-check your GPS display for ground speed against reality.

Understanding SECURE GPS!

"I thought the Presidential decision to eliminate SA allowed commercial receivers to perform to the same level of accuracy as military receivers, so why the fuss over using a PPS-rated receiver?"

Think in terms of the difference between SECURE and NON-SECURE Radio Communications and apply the same concept to GPS.

NON-SECURE GPS:

Commercial GPS receivers use the Standard Positioning Service (SPS) signal. Un-keyed receivers, civilians and adversaries have equal access to the worldwide SPS signal.

SECURE GPS:

Military-rated GPS uses the Precise Positioning Service (PPS) signal. Only a military receiver operating with COMSEC crypto-variable key can access the PPS signal for greater positional accuracy and protection from jamming or spoofing signals.

But back in June 2000, President Clinton directed that Selective Availability (SA) be turned off; Didn't that make SPS and PPS equivalent?

No. The President directed the JPO to set the level of intentional error in the SA signal to zero. His action had no influence over unintentional or intentional sources of signal interference or hostile attempts to spoof the GPS signal. So there are still plenty of sources of signal interference unrelated to SA.

Your BEST protection against jamming is a receiver that knows to look for it and has Accuracy Indicators. Your ONLY protection against spoofing is a receiver that uses the PPS signal to generate the "Y code" and implement defense against false signals.

Military rated GPS receivers (PLGR, DAGR and GBGRAM) have these capabilities. They are far more SECURE than a commercial GPS receiver that assumes clear signals and no threats.

SECURE GPS

The Only Way to Go!

GPS Systems Used in Army Aircraft

15 years ago, few Army aircraft were equipped with GPS. At that time, the official program called for the installation of the AN/ASN-149 2-channel GPS set to Modernized Cargo and Utility aircraft and the use of the Miniaturized Airborne GPS Receiver (MAGR) then in development for Attack aircraft. However, this plan was quickly overtaken by the operational needs of the first Gulf War.

Hundreds of 'Stand-alone' commercial GPS sets, known as Small Lightweight GPS Receiver (SLGR) were quickly installed in Army helicopters. By 1997 most SLGRs were displaced by an upgraded SLGR with military-rated GPS known as the Stand-alone Airborne GPS Receiver (SAGR). The SAGR was intended to serve as an 'interim' GPS system until more advanced equipment was ready. About this time, plans to equip the AH-64 Apache fleet with the MAGR and the CH-47D Chinook fleet with the 2-channel set were shelved in favor of fully integrated solutions that combined GPS with a primary navigation technology in the same box.

As a result, by the mid-1990s, the program to equip the Army's Modernized Aircraft fleet with GPS was based on two items, the Doppler/GPS Navigation System (DGNS) and the Embedded GPS Inertial (EGI) Navigation System. These systems incorporated military-rated GPS as a secondary means of navigation to augment the primary Doppler or Inertial systems. As the 1990s drew to a close, the installations of DGNS and EGI were well along and nearly all of the SLGRs/SAGRs were removed from interim service in Modernized Army Aircraft.

During this same timeframe, the AN/ASN-175 Cargo Utility GPS Receiver (CUGR) was installed in most of the UH-1H/V fleet. The SAGR was reissued to provide

standalone military-rated GPS to AH-1 Cobra, the remaining OH-58 fleet and a few Modernized Aircraft awaiting their new systems. A small number of 2-channel sets were refurbished to provide GPS to selected fixed wing aircraft and a small number of MAGR were installed in IEW aircraft.

Today, Product Manager Aviation Mission Equipment (PM AME) is working on the next-generation of integrated GPS for Modernized Aircraft. Both the upgraded AN/ASN-128D DGNS and EGI-II will incorporate SAASM-based GPS technology in a 12-channel all-in-view IFR-certifiable state-of-the-art GPS-aided navigation system. A multi-mode receiver can be added to the EGI II and a PCMCIA data transfer device can be added to the DGNS. In each case, the added item will provide new capabilities to meet requirements of Basic Area Navigation (BRNAV).

Unlike the modernization program for DGNS and EGI, there is no plan to upgrade the CUGR to SAASM-based GPS capabilities. The 500+ UH-1 and OH-58 aircraft in the Army's Non-modernized Aircraft fleet will "soldier on" with the CUGR in the current integrated or standalone configurations. There is no plan to upgrade CUGR to meet BRNAV requirements.

The small number of MAGR and 2-channel sets will also continue in service "as-is". The SAGR is being removed from inventory. The CUGR is offered as an alternate solution for SAGR users.



The evolution to integrated aircraft navigation systems using SAASM-based GPS technology for Modernized Aircraft continues...



Photos of Modernized Army Aircraft, UH60 top and AH64 above, courtesy of www.usarmyaviation.com

For information on the 2-channel set contact Johnny Walker at the Georgia office. For information on CUGR and SAGR, contact Don Mulligan at the NJ office.

For more information about PM AME managed GPS systems, contact John Kaczynski at DSN 897-0206.

Update on the CUGR

The AN/ASN-175 Cargo Utility GPS Receiver (CUGR) is used in Non-modernized Aircraft



Almost 400 CUGR-equipped UH-1 aircraft serve the Active Army and the National Guard in utility and medical evacuation roles.

Photo - courtesy usarmyaviation.com

CUGR is used in integrated or standalone configurations in over 500 UH-1H/V and OH-58A+/C Non-modernized Aircraft. Recent changes in the Army Aviation Master Plan have delayed the retirement schedule for these aircraft and the CUGR provides aircrews with an advanced military PPS-capable GPS aircraft navigation system.

Although the manufacturer's warranty expired in October 2003, all depot repair is still performed by the vendor because CUGR is a Modified Non-Developmental Item (NDI) Program with Contractor Logistics Support (CLS) for the life of the product.

What has changed is that instead of direct user-to-vendor warranty repair service, the field command can now use standard supply procedures (turn-in faulty items and requisition replacements).

The CECOM Logistics Readiness Center (LRC) and Acquisition Center have established the contract and organic depot accounts needed to support repair.

For more information, the updated **CUGR Support Plan** is available electronically from PM GPS.

Don Mulligan, PM GPS, DSN 992-6137.

Joseph Alaimo, CECOM LRC CUGR Item Manager,

PLGR Software Status

Tan PLGR—613-9854-005
Green PLGR—613-9868-008

In February 2003, CECOM released MWO 11-5825-291-30-4, TCTO 31R-2PSN11-507 to update PLGR software to correct a software filter reset deficiency that may cause intermittent position and timing errors. Initially, Army users were advised to update Standard PLGR Baseline II (tan) to version 613-9854-005 and Enhanced PLGR Baseline III and above (green) to version 613-9544-101. The guidance for Enhanced PLGR Baseline III and above (green) was later changed to recommend version 613-9868-008.

The delay in recommending version 613-9868-008 for enhanced PLGR was due to concern for potential disruption of host platform software. Testing through the summer of 2003 resolved this concern and PM GPS then endorsed 613-9868-008 for enhanced PLGR.

Why are there two versions of PLGR software you ask? The standard PLGR (tan) does not have sufficient chip capacity to handle PLGR+96 software. The enhanced PLGR has greater chip capacity. Because of this hardware difference, there will always be two versions of current PLGR software.

An important point: Since tan PLGR can't host version -008 (PLGR+96), it can't provide the targeting module contained therein. That module allows PLGR to work seamlessly with laser range finders. To do the same job with a tan PLGR requires a lot of manual entry and we strongly recommend PLGR+96 in a green PLGR when you work with laser range finders.

PLGR returning from depot repair will carry the software noted by color at the top of this column.

The Bottom Line: PLGR+96 software version 613-9868-008 is preferred operating system for enhanced PLGR. If you operate tan PLGR, use version -005.

Contact your MWO Coordinator or CECOM LAR to get the software and to borrow PLGR Reprogramming Kit #5825K3118004ANS. You can also download the software from the CECOM RDIT website at <http://www.sed.monmouth.army.mil/RDIT/> or contact PM GPS. The RDIT website has information and Points of Contact for USAF, Navy and USMC users.

Frank Rowe – Software, DSN 468-9511

Ed McAuley - Reprogramming, DSN 992-6136

Darlene Philips —Reprogramming Kits, DSN 992-8406

PLGR For Sale? No, Not at Any Price!

If you shop on eBay, you may have seen a PLGR offered for sale and wondered "what's that all about?"

The fact is that once in a while, a PLGR is offered for sale on Ebay to the highest bidder. The problem is that such an offer is illegal.

Each case is referred to the Defense Criminal Investigative Service (DCIS) as a violation of the statute for Theft of Government Property, Title 18, United States Code, Section 641. DCIS takes action to recover the government property, trace ownership and possibly recommend prosecution against the individual offering the item for sale.

The military-capable PLGR is defined as a high value pilferable item. Due to the internal crypto-variable security chip, it is never allowable to dispose of a military-capable PLGR by any means other than demilitarization at a designated depot. This includes



***Neither Standard nor Enhanced
PLGR is ever authorized
"for sale"!***

disposing of a PLGR through the Defense Reutilization Management Office (DRMO) because even the DRMO is not allowed to sell a military-capable PLGR, ever!

The Bottom Line is that the offer-for-sale of a military-capable PLGR will be treated as a case of stolen government property. Period.

Selling PLGR on EBay? Not such a great idea. If your unit really has "surplus" PLGRs, the proper action is to notify your supply chain-of-command or Base Logistics for cross-leveling within the command or installation to fill someone else's shortage. Your alternative is to contact PM GPS who will provide disposition instructions. You may not

dispose of military-capable PLGRs through DRMO, personal sale or by any other means.

Diana Wright, PLGR Product Manager at Warner Robins GA, DSN 468-5096.

GPS HELP HOTLINES:

Georgia Field Office: DSN 468-3518 Willie.Jackson@robins.af.mil

Monmouth Field Office: DSN 992-6133 Dennis.Rotenberry@iews.monmouth.army.mil

How To Contact PM GPS

Product Management Office (PMO)

LTC Harborth, PM
Mr. David Williamson, DPM
(310) 363-6676 DSN: 833-6676
david.williamson@losangeles.af.mil

Monmouth Field Office (MFO)

Mr. Allen Hart, Chief (732) 532-3523 DSN: 992-3523
allen.hart@iews.monmouth.army.mil or
Suzanne Reinhardt-Smith, (732) 532-5758 DSN 992-5758
Suzanne.reinhardt-smith@iews.monmouth.army.mil

Georgia Field Office (GFO)

Mr. Johnny Walker, Chief (478) 926-3288 DSN: 468-3288
johnny.walker@robins.af.mil or
Mr. William Burnette (478) 926-1109, DSN 468-1109

Who to Call?

For GPS integration and new products, call the PMO.

For equipment authorizations, Deferred Maintenance, Fielding, host vehicle installations and New Equipment Training, call the MFO.

For sustainment support including software, supply, technical publications and accessories, call the GFO.

Or visit the WEBSITE: <http://Army-gps.robins.af.mil>

If you need further assistance, contact the editor Donald.mulligan@iews.monmouth.army.mil and we'll put you in contact with the right office.

***The Future of Military-rated GPS is Fast Approaching:
The Next Generation Handheld GPS Receiver and Embeddable GPS Receiver
are equipped with SAASM technology
to access the Precise Positioning Service (PPS) Signal for military performance.***



***“Its Not Just GPS,
Its SECURE GPS!”***



LEFT: The 1 pound AN/PSN-13, Defense Advanced GPS Receiver (DAGR), now entering production. DAGR joins PLGR as a PPS-capable GPS receiver.

RIGHT: The 4 ounce Ground-Based GPS Receiver Applications Module (GB-GRAM) embeddable receiver now in production. GB-GRAM puts PPS-capable GPS “inside” Land Warrior and a growing list of advanced weapons systems.

PM GPS
SFAE-IEWS-NS-GPS
BLDG 563
Fort Monmouth NJ 07703
Mail Account 89