TRANSTECTOR

White Paper

GPS Jamming

Increasing system resilience to counteract intentional and unintentional GPS signal interferences

Mark Hendrick, Engineering Program Manager

an INFINITE company

07/2011 | 1474-002 RevA

Abstract

High Power Microwave (HPM) jamming equipment as well as simple radio frequency transmitters can be readily deployed to disrupt the operation of civilian and defense Global Positioning System (GPS) equipment. This article describes the threat environment and counter measures to mitigate the effects of such jamming on GPS systems. Testing of critical GPS systems and equipment is suggested to obtain a level of operational confidence and understanding denial of service issues.

The intent of this paper is to make the reader aware of the vulnerability of GPS-dependant systems to intentional and unintentional interferences and to outline effective countermeasures to increase their resilience.

GPS Jamming - Increasing system resilience to counteract intentional and unintentional GPS signal interferences

Global Positioning System - GPS - has infiltrated modern life to such an extent that many people, systems and operations rely on its error-free functioning. GPS is used for navigation, synchronizing data on wireless networks and managing loads on vast power grids, making it an integral system within the transportation, telecommunication, manufacturing, electricity distribution, mining and construction industries, not to mention national defense. It has increased safety, accuracy and efficiency in all areas of applications and greatly contributed to further technological advancements. Its significance is also evident by the absence of a successful alternative.

The greater our societal reliance on this system is, however, the greater is also our vulnerability to attempts of interrupting the signals. Anecdotal evidence of intentional GPS jamming was highlighted as recently as in the March 10, 2011 edition of Korea Herald. This news story presented the concerns of Korean defense and commercial industry leaders towards episodes of intentional electromagnetic interference (IEMI) and high power microwave (HPM) attacks alleged to have been conducted by North Korea against Seoul. Dangerous jamming of GPS signals, however, can also be caused by cheap, presumably innocuous devices like radio frequency transmitters meant to protect personal privacy and prevent tracking of a vehicle's movement. In 2009, Newark airport in New Jersey experienced brief daily disruptions of its satellite-positioning receivers for a new navigation aid. The source of the interference was a truck with a simple jamming device onboard passing by each day on the nearby New Jersey Turnpike. It took two months to locate the source of the problem.

How does GPS work?

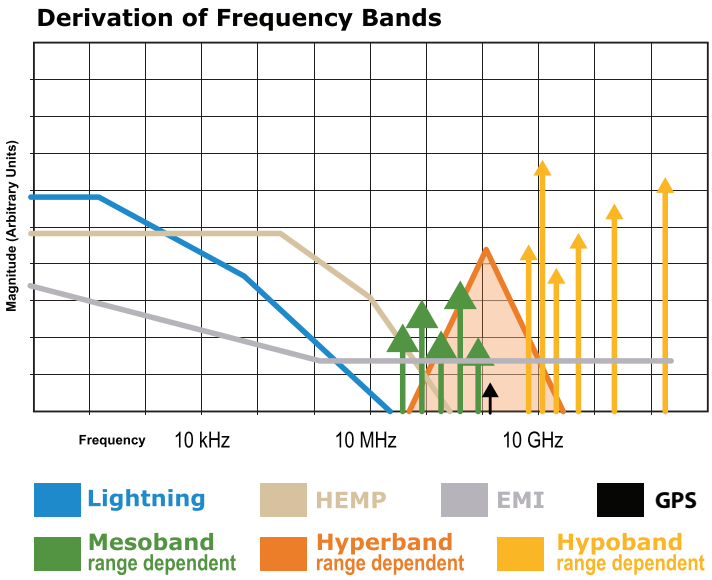
The Global Positioning System is a satellite-based navigation system, originally developed in 1978 by the U.S. Air Force and later made available for civilian use. It operates with the telemetry signals received from a network of 24 satellites circling the earth in a very precise orbit at 12,000 miles with a velocity of 7000 miles/hour (see Figure 1). Cell phones, vehicle navigation systems or similar GPS receivers obtain the information from the three strongest satellite signals above using triangulation, a method in which three separate points are measured to calculate position. Because of the high altitude of the satellites, the transmitted signals are very weak, usually broadcasted at a mere 50 W, which makes them vulnerable to accidental or deliberate interference.

Figure 1 – Constellation of GPS satellites

How does GPS Jamming work?

It is important to note that GPS radio signals use specific frequencies. Civilian applications use the frequency of 1575.42 MHz in the UHF band, while 1227.6 MHz is reserved solely for US defense applications. A jamming system does not need to be quite as precise, though. Since the GPS signals are very weak, they are among the easiest to jam and a variety of methods exist, some more sophisticated than others. However, all of them have in common that they try to block or interfere with the GPS signals by overriding them with their own signal using the same frequency as the GPS unit does. These noise signals can vary from narrowband Gaussian signals to simple continuous wave signals.

In Figure 2, relative frequency bands of lightning, electromagnetic and microwave signals are illustrated, which provides an overview of the various threats and their relative frequency spectra. The GPS bands are in the low GHz range and can be seen to overlap the orange peaks which represent the HPM jamming spectra. In fact, any electromagnetic environment that operates at the same frequency as GPS has the potential to jam, such as High Intensity Radiated Fields (HIRF) of RADAR, related radio transmission towers, ultra-wide band (UWB) sources and High Power Microwave (HPM) transmitters. Note the Magnitude is a function of V/m field strength at the receiver and is not intended as a quantitative scale of the severity of the pulse. For instance, lightning field strength from a 10km distance is much less severe than a nearby strike seen from 100m. The derivation of frequency bands and definitions is charted.



Band Classification	Approximately Equivalent to	Percent Bandwidth *(pbw)*	Band Ratio *(br)*
Hypoband (or narrowband)	HPM	*pbw* ≤ 1%	*br* ≤ 1.01
Mesoband	Damped SIne	1% < *pbw* ≤ 100%	*1.01* < *br* ≤ 3
Sub-Hyperband	UWB	100% < *pbw* ≤ 163.4%	*3* < *br* ≤ 10
Hyperband	UWB	163.4% < *pbw* ≤ 200%	*10* < *br*

Figure 2 - The GPS would appear as a whisper on the graph near the 1GHz frequency band. The signal is easily overwhelmed by the energy of the in-band transients.

Because of the societal risks that such interferences pose, any type of GPS jammer is unlawful to use in the U.S. In many other parts of the world including Europe, their use is however, only restricted. It is very easy to obtain simple jammers for as little as $50 from online sources worldwide or even build ones at home reaching GHz transmission levels. The simplicity of sourcing, as well as privacy concerns and illegal or outright terroristic intentions have driven the rapid rise in sale and use of such jammers. According to The Economist, the American National Space-Based PNT Advisory Board said, "...deliberate disruption of GPS was becoming more common, and that the systems in place to find and stop jammers were insufficient."

Counter Measures

The U.S. Air Force, still in control of the GPS satellites, acknowledges the system's vulnerability. Hence, jamming resistance measures are continuously being researched and improved. One such measure is a complex frequency algorithm built into the GPS, which uses adjacent bands in addition to the center frequency to allow the signal to effectively dodge jamming attempts. Combined with encryption and other hardware keys, these built-in measures provide a robust platform upon which our society has built a complex global GPS product market that is part of our daily lives.

In addition, ensuring signal availability in war environments has been a particular focus during the development of the satellite constellation and ground segment, as well as design of military user equipment. Nevertheless, as the two examples of the North Korean jamming attempt and Newark Airport

incident illustrate, the system is far from jam proof. To make jamming more difficult, in 2008 work began on Enhanced Loran (eLoran), a high power, ground-based system, meant to replace the original Loran, which was a ground-based terrestrial radio-navigation system first used by the American and British navies during the second World War. In Great Britain two research projects, called GARDIAN and SENTINEL are currently underway with the objective to provide real-time data about the reliability of GPS at sensitive locations and the position of a potential jamming device.

For the purpose of this discussion, the software algorithms and signal discrimination techniques employed by GPS system designers will not be covered in more detail. As apparent from the high-level efforts of the U.S. government and major research institutions, complete protection from GPS jamming does not exist yet, but systems can be made more resilient to necessitate much closer and stronger exposure to a jamming source for it to have any negative effect.

The most effective approach to identifying successful counter measures would include exposing your GPS system to a thorough jamming test, which would establish its base line resilience and allow for quantitative data showing effectiveness of various jamming mitigation efforts. Numerous qualified laboratories that specialize in these testing services exist in the U.S. and abroad. Ideally, the hardware should be set up on the test range, with various configurations of antennae and receivers, along with band-pass filters and surge protection. Testing on the equipment variables can then establish the most robust combination of equipment, installation and protection counter measures.

While laboratory testing obviously provides the most reliable information about a system's vulnerability and best protection scenarios, costs of upward from $5000 per test may not always make it feasible. In that case, it is recommended to follow the subsequently outlined best practice approach of installing additional hardware countermeasure including high performance band pass filters, RF limiter devices and shielded cable runs.

High performance band pass filters installed onto the antennae systems can significantly mitigate jamming effects. A properly engineered solution would allow only the precise GPS frequency to pass into the amplifier circuits of the receiver, reducing the effective coverage area of the jamming transmission by attenuating all of the out-of-band HPM noise that otherwise passes into the receiver antennae. Further installation of RF limiter devices within the receiver can reduce the peak in-band energy that does pass. Unless the jamming source is close enough to overload the diode limiter devices within the receiver, a well designed filter can provide reasonable protection from permanent damage.

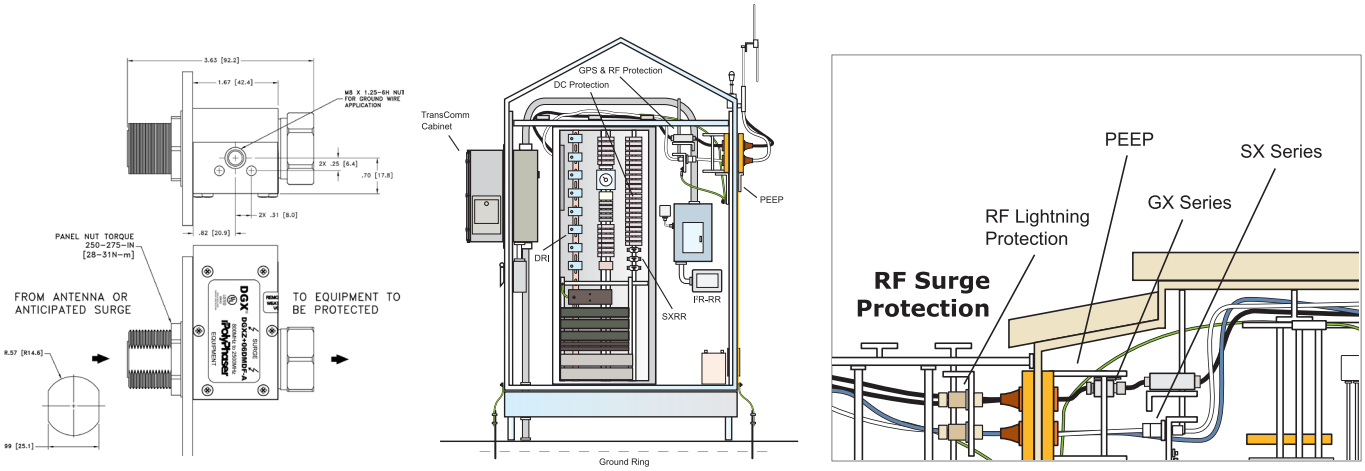


Figure 3– Filter and GPS equipment block diagrams and installation

A protected system block diagram would further include such elements as shielded cable runs to the screened shelter. The screens should be soldered, welded or joined to create an enclosure with filtered entry ports for power and the GPS antennae. Many of the same essential protection elements apply for commercial communication applications, in particular the point of entry panel (PEEP) is grounded to the Master Ground Bar (see Figure 3). The ultimate shielding effectiveness of conventional control systems can provide as much as 26dB uV/m Shielding Effectiveness (SE) up to 500MHz, with even higher SE attenuation afforded possible.

For over 40 years, Transtector and PolyPhaser have designed and engineered advanced filter and surge protection devices and worked closely with government agencies and top defense contractors as well as major commercial clients. The following discussion outlines our product portfolio applicable to GPS interference mitigation efforts.

To create a more robust network, PolyPhaser's SX and DGXZ series protectors offer effective filter and surge protection qualities to limit the in-band energy onto a GPS receiver. Correct product selection should consider factors such as connector type, Voltage Standing Wave Ratio (VSWR) and specific requirements for precision filter designs.

The SX series filters are designed for applications using multiple transmitters or high power transmitters and where dc is not required to pass on the coax. These products utilize a patented spiral L-C filter design to achieve much lower let-through voltage and throughput energies than other dc-blocked gas tube, quarter-wave and dc continuity protectors. The SX filter will withstand surge events with greater than 17kA surge discharge, once a day for over 20 years. Smaller surges do not affect the protector's dielectric materials.

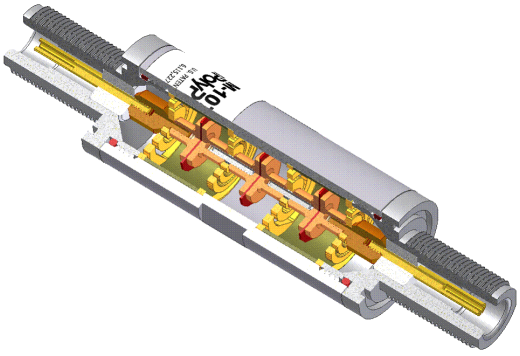


Figure 4 – 7th order band pass filter concept

The device pictured is based on the highly successful SX spiral inductor 2-pole filter design. This image of a 7-pole filter, with precise band pass and out of band rejection figures is deployed on critical applications.

PolyPhaser's GX series, including the DGXZ products, feature separate circuits for the RF path protection and the DC pass protection. This extra filtering provides the lowest let-through voltage for a DC pass product. The unit comes equipped with an integrated lid and mounting flange that can be used for grounding. The flange incorporates a captive 8mm PEM stud. A six AWG ring terminal and a dedicated wire strap is recommended to effectively ground this device.

Counter measures to guard against HPM jamming are available and offer varying degrees of resistance to jamming. A concise measure of resistance can be achieved through testing, simulation and evaluation of GPS systems. The topics of standardized testing, system vulnerability analysis and the description of the threat environment remains under active research with defense and commercial agencies.

References

EMC UK 2010, Anthony Wraight – “Electromagnetic Pulse and High Power Electromagnetic Environment and Assessment Methods”, 2010

National PNT Advisory Board - “Jamming the Global Positioning System – A National Security Threat: Recent Events and Potential Cures”, 4 Nov 2010

The Korea Herald, Song Sang-ho – “S. Korea behind North in electronic warfare”, 10 Mar 2011

GPS World – Data Shows Disastrous GPS Jamming from FCC-Approved Broadcaster - http://www.gpsworld.com/gnss-system/news/data-shows-disastrous-gps-jamming-fcc-approved-broadcaster-11029, 1 Feb 2011

Garmin – “What is GPS” - http://www8.garmin.com/aboutGPS/

The Economist, from the print edition | Technology Quarterly – “GPS Jamming: No jam tomorrow” - http://www.economist.com/node/18304246, 10 Mar 2011