Microsemi
Power Matters.™

Cesium Atomic Clocks to backup GNSS/GPS receivers in Communications Networks

White Paper
December 2014

Overview

The Communications Industry is just one of many industries that have serious concerns over Cyber security issues related to hackers and possible damage to infrastructure from terrorist activities. One of the components of Cyber Security that is a critical piece of the communications infrastructure is GNSS vulnerability. GNSS (Global Navigation Satellite System) technology includes GPS (Global Positioning System, United States owned and operated) along with Global Satellite Navigation Systems operated by China (Beidu) and Russia (Glonass). These Global Navigation Systems are used to obtain an accurate position or location but are also used to deliver accurate timing that is distributed in communications networks for a variety of applications. An interruption or degradation of the timing signals that are received or transported in the communications infrastructure can impact mission critical applications and services. In addition to providing location GNSS technologies allow for the extraction and distribution of highly accurate frequency references and time and phase transfer to applications in the one microsecond range.

The department of Homeland security in the United States is also concerned about Cyber Security issues related to GNSS vulnerability and the following links contain references to GNNS vulnerability aspects.

NIST Plans GPS Cyber security Research:
http://www.insidegnss.com/node/3919
http://www.gps.gov/news/2014/

GPS Disruptions:
Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced
http://www.gao.gov/products/GAO-14-15

There are multiple vulnerability concerns related to the use of GNSS receivers related to jamming, spoofing and outages.

GPS Vulnerabilities

GPS and other global system vulnerabilities take many forms: environmental and manmade, accidental and malicious, and errors inherent in a space-based system itself. Concern is so high the Department of Homeland Security launched the “U.S. GPS Interference, Detection and Mitigation Program” with the communications sector identified as a Critical Infrastructure and Key Resource (CIKR).

Jamming and Spoofing

Jamming is probably the most commonly cited threat to GPS today. Inexpensive civilian devices are easily found on the Internet, and with the advent of position tracking in commercial vehicles, drivers are using them to avoid being monitored. In their simplest form, jammers transmit a relatively powerful noise signal that crosses the GNSS frequencies causing nearby receivers to lose their lock on the satellite signal. Spoofing is more sophisticated. Instead of simply drowning out the GPS signal with noise, spoofers substitute a counterfeit signal with altered data. In a spoofing technique known as meaconing, GNSS signals are recorded and then rebroadcast on the same frequency, but the timing information is no longer accurate. The spoof signal has greater power which captures the receiver lock. The receiver continues to operate, but now bases its position and time calculations on the incorrect input.

Equipment Failures and Interference Not as exotic, but probably having greater operational impact, failures of GPS timing are often traced to problems with the GPS equipment and installation or other nearby equipment. Antennas and cables are exposed and subject to breakage. Nearby electronic equipment can malfunction or degrade and radiate energy that interferes with the GPS signal.

Environmental

Clouds, rain and snow alone have no meaningful effect on GPS signals; however, natural weather conditions certainly can have an impact. Lightning strikes or high winds often take out antennas. Sleet and ice can freeze over the antennas and impair their ability to receive a signal. Solar flares are bursts of energy from the sun resulting in an increase in radiation that can temporarily impact the GPS signals and cause errors in timing calculations by the GPS receivers

The most effective technology available that can be deployed as a backup to GNSS receivers that can help hold and maintain frequency, time and phase is Cesium Beam Atomic Clock Technology. A Cesium Atomic Clock is a self contained frequency reference that needs no external input or reference to produce a frequency output reference that meets or exceeds the Stratum 1 /G.811 performance standards for a PRS (primary reference source). By definition a Primary Reference Source must maintain accuracy and traceability to UTC and meet a frequency offset requirement of no more 1x10-11 from the global standard for time and frequency, UTC (Universal Coordinated Time).

A cesium atomic Clock is an excellent way to backup GNSS/GPS technology for frequency, time and phase applications. A cesium that is performing at an offset from UTC at 1x10-12 accuracy, this is typical performance for a Cesium, only accumulates one Pico second per second of phase compared to a UTC based device such as a GNNS/GPS timing receiver. With this level of performance a Cesium Clock can be used to backup GNSS/GPS with no degradation in performance for frequency applications and provides for holdover mode of operation for time and phase applications where you can use the following formula to determine what length of time it will take for the Cesium based reference to accumulate 3 microseconds in time or phase (+/-1.5 microseconds is the requirement for time/phase alignment of macro and small cells for LTE-TDD and LTE-Advanced technologies in wireless Communications). At the rate of phase accumulation of one Pico second every second the Cesium reference will accumulate a time and phase error of 86,400 Pico seconds per day (86,400 seconds in one day) which equates to 86.4 nanoseconds per day. To reach 3 microseconds of time and phase accumulation it would take approxamnetly one month so a Cesium Clock can be used to backup GNSS/GPS for both frequency and time/phase applications including the very stringent requirements for LTE.

Cesium clocks can be used to backup GNSS/GPS for both local and wide area disruptions. The following section describes how PTP (Precision Time Protocol) can be used in conjunction with Cesium

Atomic Clocks to protect GNSS/GPS receiver failures and disruptions at both the local and wide area levels. PTP is the telecom implementation of IEEE 1588 timing over Ethernet and can be used to transport the Cesium based reference to GNSS/GPS locations using the G.8265.1 PTP profile. Please refer to the below diagram for an illustration example.

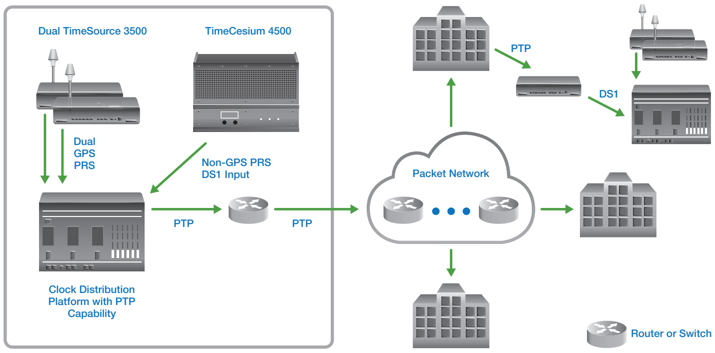

Figure 1: Area Timing Hubs

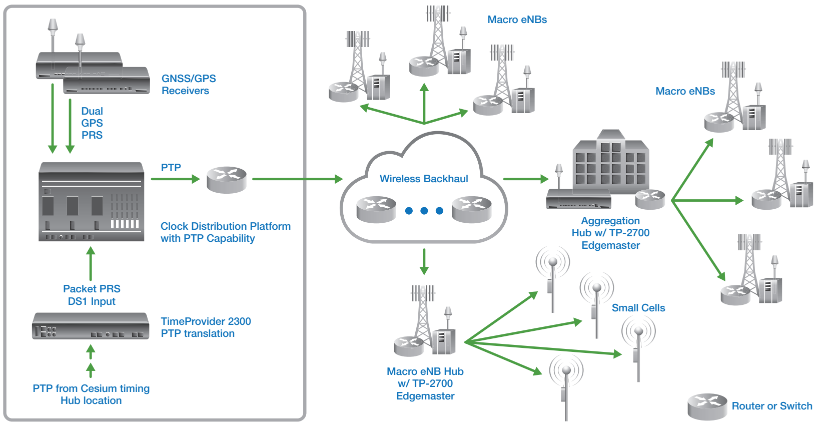

Figure 2: Cesium referewnce from timing PTP Hub for LTE protection

As you can see from the diagram this architecture allows for protection in a local area GNSS/GPS outage and also a wide area outage by relying on the autonomous nature of the Cesium Atomic Clock Standard. Using the G.8265.1 PTP profile for telecom frequency applications is an important consideration as this profile allows for the PTP client to adjust the number of time stamps per second it receives to make sure it can properly filter the effects of packet jitter and delay introduced by the network. For frequency reconstruction the PTP client device that reconstructs the frequency accuracy must have a rubidium oscillator in the client device in order to filter the packet delay variation introduced by the network transport equipment in order to produce a highly accurate and stable frequency reference. This highly accurate Cesium frequency reference that is reconstructed using PTP has the same intrinsic attributes of the Cesium Atomic Clock and will provide for one month of time and phase holdover to 3 microseconds as well a providing a frequency reference that will not degrade over time.

For any communications providers that have concerns or need to demonstrate to regulators or customers that their network is protected from GNSS/GPS Cyber Security vulnerabilities the approach described in this paper is a solution that has been tested with proven results and is a cost effective method to backup GNSS/GPS technology for both local and wide area outages.

Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer's responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided "as is, where is" and with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
email: sales.support@microsemi.com
www.microsemi.com

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,400 employees globally. Learn more at www.microsemi.com.