In This Issue

We are pleased to introduce the sixth edition of our quarterly newsletter *Time to Sync*—your source for the latest Timing and Synchronization industry news, products, events, and more! *Time to Sync* keeps you updated on the latest news in the timing and synchronization industry and helps you stay connected.

In addition to the Timing and Synchronization products, Microsemi offers complementary product lines including Power-over-Ethernet (PoE) midspan/injectors, Carrier Ethernet switches, PHYs, software, and equipment/data link security. We look forward to sharing some of these with you when it is relevant while maintaining timing and synchronization news and trends as the focus of this newsletter.

We recently introduced two new variants to the IGM family that are ready for shipment—the IGM1100o (weatherproof IGM suitable for outdoor installations) and IGM1100x (for indoor installations with an external antenna).

The SyncServer S600 and S650 devices continue to garner more and more interest, especially within the enterprise community. New collateral is available for the SyncServer family.

- *S600*
- *S650*

We have also actively participated in several roadshows and conferences around the globe and generated interest from customers across multiple segments.

Time to Sync is intended to be informative and educational, and aims at helping you succeed! Please send any comments or questions, including suggestions for future articles, to timing@microsemi.com.

Technology and Product Updates

Mitigating GPS Vulnerabilities

The Global Positioning System (GPS) is ubiquitous as a source of timing for wired and wireless carriers. Mobile networks use GPS-referenced timing to synchronize frequencies in 2G/3G, LTE, and the more recent 4G (LTE-Advanced) technologies.

As these network operations become more and more dependent on precise timing and synchronization, the vulnerabilities of the GPS and other satellite systems is of growing concern. Results from a nine-month study conducted by the U.S. Department of Defense indicated an outage of approximately 12%, affecting approximately 4.5% of the United States. The following sections discuss some of the main types of GPS vulnerabilities.

Jamming and Spoofing

Jammers, in their simplest form, transmit a relatively powerful noise signal that crosses GPS frequencies, thereby causing the receivers to lose their lock on the satellite signal.

Spoofing is slightly more complicated. 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, GPS signals are recorded and then later broadcasted on the same frequency, but the timing information is no longer accurate.

Figure 1 · **GPS Jammer and Spoofing Equipment**

Equipment Failures and Interferences

Antennas and cables are subject to breakage. Nearby electronic equipment can malfunction or degrade and radiate energy that interferes with the GPS signal.

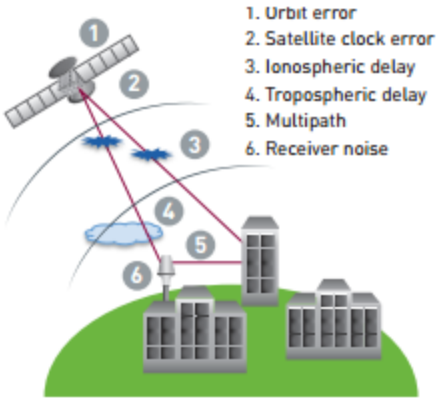
Environmental Factors

Lightning strikes or high winds can often destroy antennas. Sleet and ice can freeze over the antenna and impair their ability to receive the signal. Solar flares are bursts of energy from the sun that results in an increase in the radiation that can temporarily impact the GPS signals and cause errors in timing signals.

Errors Inherent in Space Based Systems

There are several sources of inherent error in space-based systems that can impact the accuracy of the calculations. As the following illustration shows, these include orbit error, satellite clock error, ionospheric delay, tropospheric delay, multipath, and receiver noise.

Figure 2 · **Sources of GPS Timing Errors**



The following sections discuss some ways in which GPS vulnerabilities can be controlled or reduced.

Rubidium Atomic Clocks

The first line of defense against the loss or impairment of GPS signals is to deploy clocks with robust holdover capabilities.

There are a wide variety of oscillator types—each with its own performance/cost value.

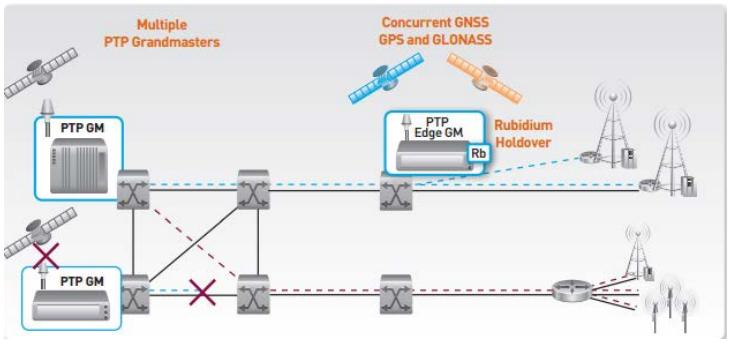
- Temperature Controlled Crystal Oscillators (TCXO)—synchronization requirements are comparatively simple, but holdover capability is limited.
- Oven Controlled Crystal Oscillator (OCXO)—synchronization requirements are slightly stringent, but typical holdover at the required specification is 1 hour (enough to wait out a solar storm or a jamming event).
- Rubidium Miniature Atomic Clock— high performance specification and a long holdover time (24 hours), can be deployed in the network where the cost is spread across multiple locations.
- Cesium—a primary reference in addition to the GPS (eliminates the risk of GPS vulnerabilities), but is extremely expensive. However, the preferred deployment is at centralized locations combined with network distribution of time, which allows its cost to be leveraged across multiple locations in the network.

Network Distributed Time

Network distributed time consists of a GPS primary reference incorporated into a time server or a grandmaster clock. The timestamped packets are distributed through a timing protocol embedded in the equipment to clients or slaves at other locations in the packet network.

Network distributed time also provides backup against other sources of timing disruptions such as simple equipment failure or human error. The following illustration shows an example of network distributed time.

Figure 3 · **Network Distributed Time**



Timing and synchronization is more critical than ever as service providers continue to evolve their networks and operations. Vulnerabilities of the current and planned GPS systems have caused governments and network operators to investigate and deploy solutions that mitigate the impact of GPS impairments and outages.

The solutions mentioned have their own advantages and challenges with respect to technical feasibility and cost. Contact Microsemi to understand more about how you can protect your network against GPS vulnerabilities.

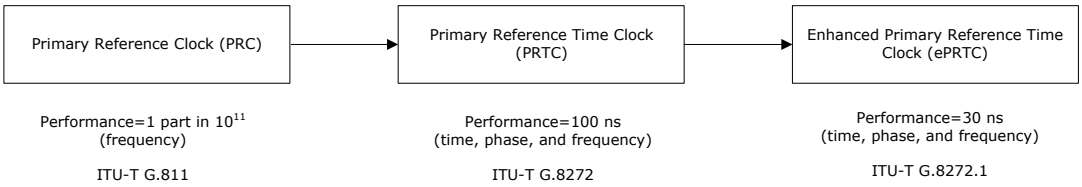
The Enhanced Primary Reference Time Clock (ePRTC)

When looking at the evolution of primary reference standards as developed by the ITU, G.811 was the original requirement for a Primary Reference Clock (PRC). The G.811 requirement describes a PRC that delivers 1 part in 10^{11} frequency accuracy, and is suitable for timing and synchronization of other clocks within a network. As packet timing requirements evolved, ITU developed the Primary Reference Time Clock (PRTC) standard to include the requirements for time and phase for transport over a packet network. This standard is known as G.8272 and was originally published in 2012. The G.8272 standard describes a clock that delivers <100 ns phase and time performance suitable for packet networks.

However, there are plans to develop a new standard in order to increase performance for phase and time to meet the requirements of emerging mobile access network technologies and improve security for protection against GPS outages.

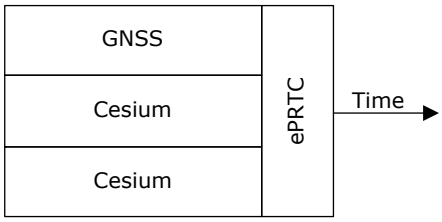
The new standard (G.8272.1) is called the Enhanced Primary Reference Timing Clock (ePRTC). G.8272.1calls for performance levels and reliability that will set the foundation for time, phase, and frequency for many years to come. The following illustration shows the evolution of primary reference standards over the years.

Figure 4 · **Evolution of Primary Reference Standards**



The core components of an ePRTC solution are GPS, atomic clocks (typically cesium or better), and an ePRTC system. The ePRTC system is shown in the following illustration.

Figure 5 · **Enhanced Primary Reference Clock (ePRTC)**



An ePRTC supports a high level of accuracy (<30 ns) and is subject to more stringent output performance requirements than today's PRTC systems. It is an autonomous source of time that utilizes one or two co-located atomic clocks to provide the required performance for both time and frequency, even when the GPS is completely lost.

Finally, an ePRTC delivers a higher level of operational reliability to ensure operators can maintain required time and frequency service performance for long periods even when the GPS is completely lost.

The objective of the ePRTC solution is to generate time by producing its own independent, autonomous time scale. The time scale provides time, phase, and frequency that are aligned and calibrated to the GPS signal over time. The time scale is generated and maintained autonomously based on the stability of the atomic clock(s). The frequency stability of the atomic clocks serves as a reference for the ePRTC time scale. This is

the key distinguishing feature when comparing an ePRTC to a PRTC. In case of a PRTC, time comes directly from GPS. In the ePRTC, the time scale is locally generated.

A new white paper on the ePRTC system is coming soon. Contact us to be informed when the paper is available.

End Market Corner

SyncServer S600 Network Time Servers with Dual Power Supplies for Modern Data Centers

Power is a key concern in modern data center design and management. While efficiency and cooling are high priorities, so is reliability—surviving power fluctuations or outages and returning to normal operations as fast as possible. Accurate time is a key element in bringing a mission-critical data center back online quickly in the event of a power service interruption. As systems restart, one of the initial activities is often synchronizing the time to an accurate network time server. A time server that is dual-corded and has dual power supplies provides several levels of time service protection in power failure scenarios.

The dual-corded SyncServer S600 has hitless dual power supplies, which are inter-connected in the SyncServer at the circuit level. The power supplies share the load equally and there is an active power management system constantly monitoring the operation. If the power to one cord is lost or if one power supply fails, the entire load is instantly picked up by the remaining energized power supply with no interruption in time services to the network.

If there is only a single source of power available to the S600 time server, having the power supply connected to the two power supply circuits of the time server provides protection against a single power supply circuit failure. If a power supply circuit in the SyncServer unit fails, the other instantly picks up the entire load, just as in the dual-corded scenario.

Power is very valuable in a data center; it is conditioned and closely monitored because it is a major component of operating expenses. However, sometimes a surge may occur, which can affect the equipments in the data center. Failure of a single power supply in a dual power supply time server can be subtle. To overcome this issue, each power supply in the SyncServer S600 is continuously monitored. In the event of a power supply failure, notification is instantly provided to the network operator through an SNMP trap, email, alarm relay, and/or LEDs on the front of the unit. This notification allows the operator to schedule maintenance on the server at an appropriate or convenient time.

The SyncServer S600 network time server is purpose-built to deliver exact hardware-based network time protocol (NTP) timestamps. The unparalleled accuracy and security is rounded out with outstanding ease-of-use features for reliable network time services that are ready to meet the needs of the user network and business operations today and in the future.

The dual power supply option in the SyncServer S600 is available in the customer build-to-order configurations. However, due to the popularity of the option, it is now also available in the preconfigured SyncServer S600 choices (as of September 2016).

Importance of Network Time Synchronization for Enterprise Operations

Quality time in an enterprise network is critical for operating the network in a reliable and secure manner and supporting the applications. It is essential for the performance of the network as well as compliance and forensics. Network operations require time-synchronized information to ensure optimal network performance. It is often not until a problem occurs that organizations become aware of the importance of time synchronization (either as a contributing factor to the problem itself or as a necessary tool to diagnose the problem). Many network processes are dysfunctional without time synchronization.

The following sections discuss some of the network time synchronization applications.

Log File Accuracy, Auditing, and Monitoring

Server log files and subsequent reports enable assessment of network activities. This includes firewall and VPN security-related activity, bandwidth usage, and various logging, management, authentication, authorization, and accounting functions. NTP server security and deployment typically enhances the ability to achieve better log file accuracy (or to satisfy any other timing requirement).

Network Fault Diagnosis and Recovery

Most IT organizations are measured on their ability to maintain full flow network operations. Strict limits on allowable downtime are some of the most common quality of service (QoS) metrics in place, and every IT department is acutely aware of them. In the event of a failure, accurate network timing is crucial for fault diagnosis and recovery.

File Timestamps

The integrity of any file system relies heavily on the name and dates of the files. Individual files typically track the dates for creation, last access, last archive, and last modification. In a distributed file sharing system, a master file is maintained by a network file sharing (NFS) server for the remote clients. NFS is network time-dependent—when presented with duplicate file names, it saves the latest copy.

The following are some of the security features that play an important role in making SyncServer suitable for the previously mentioned applications.

- Password access
- NTP MD5 authentication and NTP autokey
- Access control lists
- TACACS+, RADIUS, and LDAP authentication

The network requires quality, safe, and easy-to-deploy timekeeping. Redundant time sources, holdover schemes, power sources, authentication options, and hardware components serve the primary mission of accurate, reliable, and secure time services to the network, as do features that make timekeeping easier to monitor and control (including an intuitive web interface and support for SNMP so the server can alert administrators to out-of-bounds conditions such as a DoS packet flood). While it is certainly possible to source time for free from an Internet time server that lacks these critical attributes, it is important to consider the critical network and business operations that hinge on such a fundamental and essential attribute as accurate, secure, and reliable time.

Remember, great timing is just the start!

Latest Collateral

The Enhanced Primary Reference Time Clock (ePRTC) as a Solution for GNSS Vulnerability Whitepaper

The threat of GPS vulnerabilities is real. Events such as signal anomalies, regional disruptions, and global outages have prompted governments across the globe to find solutions for this serious threat.

In this white paper, Microsemi describes the all-new ePRTC solution to counter GPS vulnerabilities.