In This Issue

Welcome to *Time to Sync*—your source for the latest Timing and Synchronization industry news, products, events, and more!

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

Technology and Product Updates

BlueSky™ GPS Firewall: Breakthrough Technology to Secure Against GPS Jamming and Spoofing Threats

At the ION GNSS+, Microsemi recently unveiled its latest offering to secure infrastructure from GPS jamming and spoofing threats: the Blue*Sky*™ GPS Firewall. Microsemi's Blue*Sky*™ GPS Firewall filters the GPS signal in real time, removing anomalies from the GPS signal before it is consumed by the downstream GPS receiver. This creates an intelligent and secure barrier against jamming and spoofing, and prevents the GPS receiver from being impacted by such incidents.

Deployment of the Blue*Sky*™ GPS Firewall does not require any new cabling or alteration of the pre-existing antenna installation, and it is interoperable with standard GPS receivers. Additionally, the Blue*Sky*™ GPS Firewall incorporates an Ethernet interface for remote management and monitoring, and includes a secure web interface that any browser can use for configuration and setup of the device.

The dependency on Position Navigation and Timing (PNT) is increasingly important to critical infrastructure sectors such as telecommunications, energy, transportation, emergency services, financial services, and enterprise infrastructure, and is mainly provided through GPS. Best practice documents published by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) describe steps that can be taken to mitigate outages and disruptions with GPS reception.

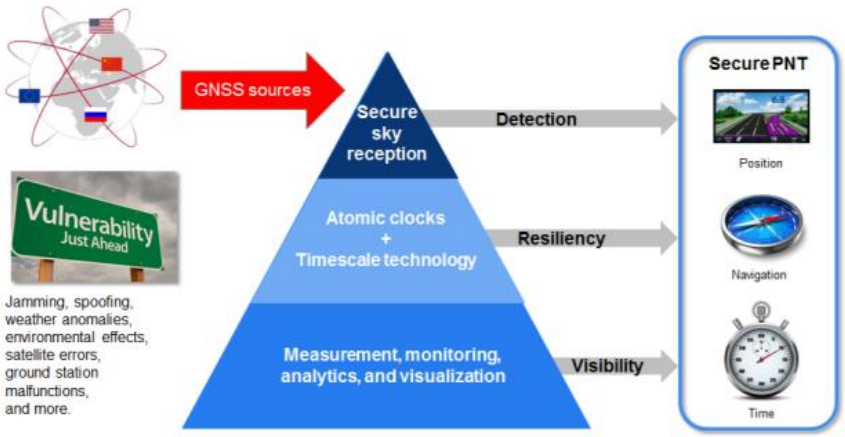

Figure 1: Secure PNT Requires Detection, Resiliency, and Visibility

Microsemi's new Blue*Sky*™ GPS Firewall provides critical infrastructure sectors with a first line of defense against GPS threats to help build out a secure, robust, and resilient PNT platform for their infrastructures.

The Blue*Sky* GPS Firewall includes a broad range of data validation rules based on real, live sky GPS threats, both intentional and unintentional. Similar to network security threats, new GPS vulnerabilities are on the rise and Microsemi is continuously tracking GPS signal manipulation including spoofing threats, jamming attacks, multipath signal interference, atmospheric activity, and many other issues that can create GPS signal anomalies, disruptions, and outages. These advancements are incorporated into the software platform of the Blue*Sky*™ GPS Firewall, which can be updated remotely using Microsemi's TimePictra™ management system.

Visit the BlueSkyTM GPS Firewall home page here or download the complete white paper on GNSS Security for PNT Applications.

Improved Immunity from GPS Jamming and Spoofing for Military Systems: SyncServer S650 SAASM

Microsemi recently announced the availability of the SyncServer S650 SAASM time and frequency standard incorporating a selective availability anti-spoofing module (SAASM) to provide a highly secure, accurate, and flexible time and frequency platform for synchronizing mission-critical electronics systems and instrumentation applications in the defense market, such as satellite communications and defense operational infrastructure.

The new SyncServer S650 SAASM is designed for use by the U.S. Department of Defense (DoD) and other government agencies, as well as their approved suppliers, and received the GPS Directorate Security Approval to incorporate a military-grade GPS SAASM receiver module. This enables U.S. armed forces to confidently deploy features of Microsemi's popular commercial SyncServer S650 in a military-grade configuration. In addition, the integrated SAASM module adheres to industry standards allowing for a migration path to GPS military code (M-Code) support.

The SyncServer S650 SAASM is designed to generate precise time and frequency signals to synchronize high-bandwidth mission-critical communications systems and critical infrastructure requiring the highest levels of security support. In addition to offering superior low phase noise performance, the device is compliant with the Joint Chiefs of Staff SAASM GPS mandate and developed for authorized military users only.

The SyncServer S650 SAASM is a highly versatile time and frequency system with the company's FlexPort™ technology for multiport, user-definable output signal configurations for time codes, pulses, and a variety of signal types essential for system synchronization. This makes the SyncServer S650 SAASM ideal for DoD electronics system engineers synchronizing mission-critical, system-level instruments. This is coupled with Microsemi's NTP Reflector™ technology for robust security, accuracy, and reliability of network-based time services such as Network Time Protocol (NTP) and Precision Time Protocol (PTP).

Click here to visit the SyncServer S650 SAASM home page.

Interested in a regular SyncServer S650? Click here to visit SyncServer S650 home page or take a look at the Enterprise Network Time Servers or GPS Instruments.

New SyncServer S80 NTP Network Time Server Delivers Precise, Secure Time Stamps for Physical Security Networks

Microsemi also recently announced the availability of the SyncServer S80 Network Time Server that integrates the GPS antenna, receiver, and Network Time Protocol (NTP) timing server into a single ruggedized, environmentally-hardened unit ideal for outdoor installation with physical security systems. The high-reliability device, well-suited to synchronizing the timing for IP security cameras, access control devices, digital video recorders (DVRs), or network video recorders (NVRs), or operate as the master clock for time display networks common to transportation like railways and airports, education institutes, and even small enterprise networks, secures accurate time to reduce network exposure to vulnerable public time servers or external attacks such as denial of service (DoS).

The SyncServer S80 is designed to provide ultra-accurate, nanosecond caliber NTP time stamps using the security-hardened NTP Reflector™ technology. Unlike other NTP servers often used for IP camera time stamps, Microsemi's NTP Reflector also works as a central processing unit (CPU)-protecting firewall, shielding the S80 CPU from excessive NTP request loading, which negatively affects time stamp accuracy, reduces availability of time stamps, and can leave the device susceptible to CPU freezing or system reset. The S80 is ideally suited for video networks with tens to thousands of IP cameras, with no degradation in NTP server performance while operating as the trusted source of accurate time on the network.

The network-ready SyncServer S80 is designed for easy integration into existing physical security networks and serves as the primary source of accurate time for the essential time stamps on security video footage. Equipped with Power over Ethernet (PoE), the device easily connects into an existing PoE infrastructure that runs power, timing, and video feed through a single cable. In cases where the Ethernet infrastructure is in place but PoE is not available, the S80 can be powered through the addition of a Microsemi single-port PoE injector or a managed 6-, 12-, or 24-port PoE midspan. Because the S80 is also ruggedized for outdoor installations, it can connect to the network right alongside an existing outdoor camera installation, with the addition of a Microsemi PDS-104GO 4+1 managed outdoor switch. Once connected to the network, the S80 is ready to be the source of authoritative NTP time stamps for all video camera recordings.

The SyncServer S80 will be available for purchase in November 2017.

Visit the SyncServer S80 webpage, download the SyncServer S80 datasheet, or visit the complete range of Enterprise Network Time Servers.

Applications Corner

Improved Mobile Backhaul Network Reliability with IEEE 1588-2008 (PTP)

The delivery of synchronization to next-generation base stations will rely on PTP grandmaster clocks deployed in the network. Sync packets flow from the grandmaster clock to the slave clocks in these base stations. Mobile base stations—including 3G, LTE, and LTE-Advanced—all require frequency synchronization of 16 ppb to assure high quality of service and avoid dropped calls. In addition, TDD and LTE-Advanced networks also require tight phase synchronization of 1.1 µs.

The loss of physical layer sync has generated a requirement for new base station designs incorporating PTP slave clocks that will meet the 16 ppb requirement using packet technology. Such PTP slaves in the base stations rely on access to a carrier-class PTP grandmaster clock deployed in the mobile access network.

PTP Slave Locking Considerations

The slave clock establishes communication with the grandmaster by requesting a reservation for a synchronization flow, specifying parameters such as message rate and reservation duration. Initially, the slave free-runs at an indeterminate frequency

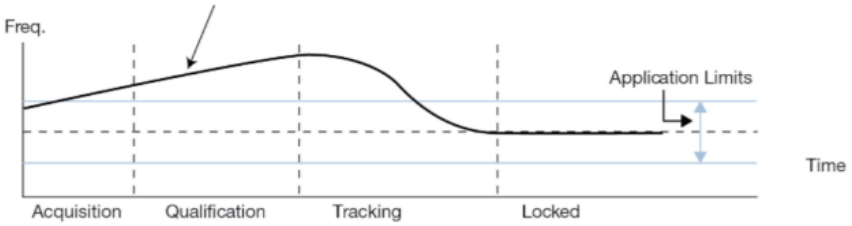

Figure 2: IEEE 1588 PTP Slave Clock Acquisition and Locking Process

process of aligning the frequency and time to the master takes place in the tracking stage. By the time the locked stage is reached, the slave is well within the application limits and able to maintain the target level of performance over the long term.

Network deployment and reference network test models have been established to assist carrier engineering staff develop specific deployment rules for IEEE 1588-2008 synchronization solutions in their networks. To provide failover protection, there are two main approaches to consider: network-based redundancy and built-in grandmaster hardware redundancy.

- **Network-Based Redundancy**
  In network-based redundancy, two grandmasters are employed. These may be co-located, but they are most often at different geographic locations to provide maximum protection against failure, as shown in the following illustration.

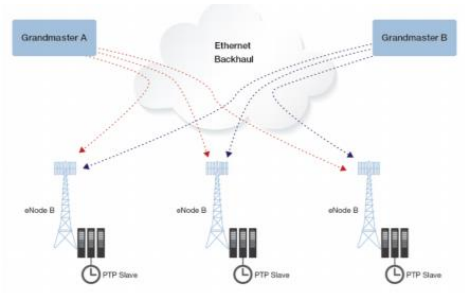

Figure 3: Network-Based Redundancy

  Network-based redundancy protects against network failure in the vicinity of the grandmaster as well as failure

of the grandmaster itself, because the second grandmaster is normally connected by a separate access link into a different part of the network. However, there are some significant issues created by switching between two different grandmasters.

- **Built-in Grandmaster Hardware Redundancy**
  A more robust method of providing grandmaster redundancy is to implement a carrier class IEEE 1588-2008 grandmaster clock with built-in hardware redundancy. A fully redundant grandmaster clock employs an active and standby clock, synchronized to redundant primary reference sources (for example, GPS or T1/E1), as shown in the following illustration.

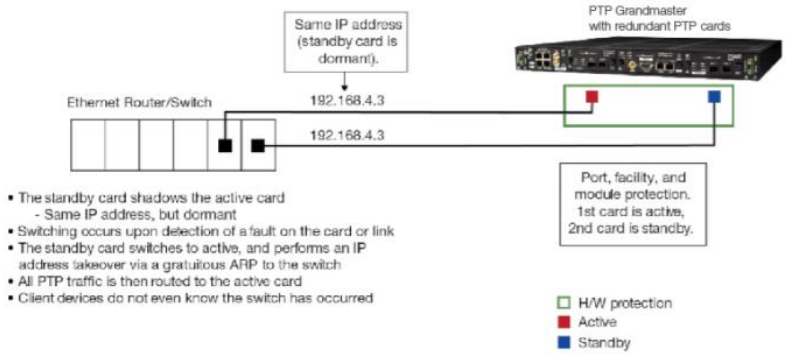

Figure 4: Built-in Hardware Redundancy

The major advantage of this configuration is that because the active and standby clocks share a common reference and common network location, the PTP slave devices see no synchronization offset during a failover switching scenario. The slave clocks will all remain locked to the redundantly protected grandmaster, and will not be forced to acquire, qualify, and track to a new grandmaster clock with an unknown offset, or connected through a different network path.

In summary, some reliability issues affect both redundancy methods. The failure of a primary reference source (PRS) is an important issue in the design of a grandmaster, particularly if accurate time is required as well as frequency. For frequency applications, backup may be provided using a T1 or E1 frequency reference. In the event of a PRS failure, a T1/E1 input reference that is traceable to a Stratum 1 clock source will keep the PTP time stamps from drifting and is an acceptable redundancy engineering practice. The failure of the slave or its access link will only affect the network element(s) dependent on that slave. The impact on the overall network is low. It is not common practice to provide redundant links or clocks to the base station in cellular networks due to the cost of such protection.

Underwater Exploration with Chip Scale Atomic Clocks (CSAC)

Sensors employed in undersea applications rely on precise timing to be effective. However, because time from GPS is unavailable underwater, these sensors have generally relied on OCXOs for stable and accurate time stamping within the sensor. Now those applications have a better option: the SA.45s chip scale atomic clocks (CSAC). Compared to OCXOs, the SA.45 CSAC maintains far higher accuracy for far longer periods, uses much less power, and maintains a much more stable frequency in spite of the wide variations in temperature experienced.

One such undersea application is reflection seismology (or seismic). In seismic applications, oil exploration firms place a grid of geophysical sensors on the ocean floor to determine likely spots where oil will be located. The sensors can be dropped over the slide of a ship or laid down by a remotely piloted vehicle. The sensors can be independent or a cable can connect the row of sensors. Each sensor typically includes a hydrophone, a geophone, and a TCXO or OCXO that is used to timestamp the data received by the other two devices. Once the sensors are in place, a powerful air gun or array of air guns launch a sonic pulse from the ship. The ship moves in a pattern that allows the air gun to be fired from many different angles relative to the sensor grid. Some of the pulse's energy reflects off the ocean floor, travels through the layers of rock, and eventually reflects back to the sensors on the ocean floor where it is detected and time stamped. Once the ship has finished its predetermined pattern, the sensors are retrieved along with the time stamp data.

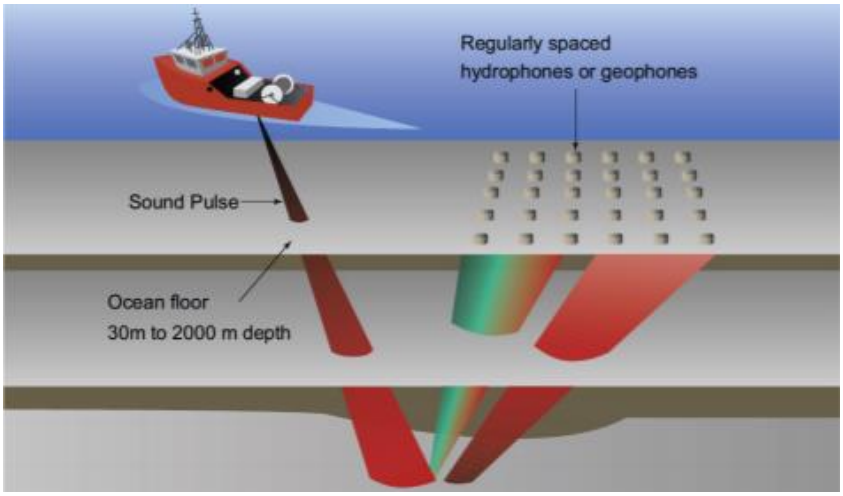

Figure 5: Sonic Pulses and Underwater Exploration

Because the sonic pulses travel at different speeds through different materials, the time it takes to reflect back to the sensors off the various rock layers is different depending on which materials the pulse traverses. When timing data is post-processed, it creates a picture of the layers of rock and sediment beneath the ocean floor, showing which locations likely hold oil or gas deposits. The more precise the timing, the more accurate the images of where oil and gas actually exist.

Why CSAC: Benefits in this Application

- **Improved Accuracy**
  During a typical deployment, the sensors can be underwater for several weeks at a time (deploying the sensors, taking measurements, and retrieving sensors takes time, even more so if the weather conditions are not optimal). Through the deployment, the OCXOs are aging, producing a time stamping error that varies as the square of the time under water. The CSAC's

low aging rate, which can be even 1/100th of a good OCXO, greatly reduces the time stamp error as sensors are deployed for longer periods.

- **Reduced Power: Lower Battery/Sensor Costs**
  Batteries are typically the biggest expense in underwater sensors and the number of sensors in a typical grid is increasing. Because the SA.45s CSAC consumes 1/10th to 1/20th of the power of an OCXO, it requires much less battery power so sensors can be smaller and cost less. Alternatively, sensor manufacturers can choose to retain the existing battery capacity and use the CSAC to create sensors for much longer missions.

- **Reduced Effects from Wide Temperature Swings**

  Today, most marine geophysical sensors are calibrated to GPS on the deck of the boat before being dropped into ocean. Because the water at the bottom of the ocean is often just a few degrees above freezing temperature, the sensor can see a temperature change of 30 ^{o}C or more from its calibration temperature, causing a shift in frequency and a linear error in time. Some sensors use software models to correct for this error, but the best approach is to minimize the error to begin with. With a temperature co-efficient of ±5.0x10^{-10} over its entire temperature range, the SA.45s CSAC can offer a 10x to 1000x improvement over OCXO and TCXO alternatives.

For more information on how CSAC can help address your applications, please contact us at sales.support@microsemi.com or timing@microsemi.com

Smart Antenna for Telecom Network Monitoring

The integrated GNSS master (IGM) portfolio is often viewed as an excellent small 1588v2 PTP grandmaster at the edge of the network to serve clusters of base stations. As with phase requirements, eNodeBs need to be served from grandmasters as close as possible to the edge to meet stringent phase requirements. However, customers may consider GPS/GNSS at the edge and may view GPS/GNSS as an alternative to a 1588v2 grandmaster like IGM. But GPS/GNSS and PTP 1588v2 are not two conflicting technologies; GPS is a source whereas 1588v2 is a distribution mechanism. The question is not really GPS versus 1588, but what is the best way to distribute time. The choice is between a legacy solution and a smart solution.

The legacy way to distribute time from a GPS signal is to use a traditional antenna, a coax cable, and a splitter for distribution. This traditional way is not flexible, does not scale with densification needs for LTE-A and 5G, does not present any backup solution, does not provide any management capabilities, and does not evolve with standards.

On the other hand, the IGM portfolio is a smart antenna bundled with a 1588v2 grandmaster. It offers the same ability to distribute time from GPS/GNSS, but also offers the ability to leverage Ethernet rather than coax cabling for a much more scalable and cost-effective solution. It offers backup in case the GPS signal goes down, management capabilities including monitoring, and the ability to evolve with standards, to serve legacy base stations and also new technologies.

As shown by the following, a smart antenna, Ethernet, and a smart splitter (1588 grandmaster) is the right way to leverage GPS in mobile networks.

Traditional	Smart Antenna and Splitter
No resilience	Network failover
No holdover	Oscillator, PTP input, thermal algorithm
No backup to GPS	APTS, asymmetry correction
No scalability (coax)	Densification and 5G capable (Ethernet)
Legacy, not designed for large scale	Future-proof (multiple protocols)
No management/monitoring	Monitoring, location, automation, SDN

New Collateral

White Papers

- Improving Mobile Backhaul Network Reliability with Carrier Class IEEE 1588-2008 (PTP)

Network deployment and reference network test models have been established to assist carrier engineering staff to develop specific deployment rules for IEEE 1588-2008 synchronization solutions in their networks. To provide failover protection, there are two main approaches to consider: network based redundancy and built-in grandmaster hardware redundancy.
The paper discusses the advantages and disadvantages of each technique, and describes features built into Microsemi hardware to provide carrier-class reliability and performance.

- GNSS Security for PNT Vulnerabilities
  The dependency on position, navigation, and timing (PNT) has become increasingly important to critical infrastructure sectors such as communications, energy, transportation, emergency services, financial services, and cloud data centers. This demands critical infrastructure to construct a secure and robust PNT network that is resilient to GPS errors as well as any sky-based delivery channels such as Galileo, GLONASS, BeiDou, or another. This paper describes a solution for securing GNSS to support PNT applications as used by critical infrastructure.

- Best Engineering Practices for Cable Timing Architecture
  From the beginning, cable networks required good synchronization: first, because the physical transmission medium is shared by cable modems and poor synchronization could cause interference and crosstalk; second, because services such as T1/E1 circuit emulation and high-quality video required good timing. As high-bandwidth services such as live video and video-on-demand migrate to Ethernet and OTT distribution, cable operators are faced with increasing competition from traditional wireline and mobile wireless service providers. This has led to the development of DOCSIS 3.1 and creation of the second version of the modular CMTS, known as Modular Headend Architecture, Version 2 (MHA-V2). This paper talks about the details of the new standard DOCSIS 3.1 and how PTP systems are being adopted by the cable networks.

New Video Available

- Introduction to the All-New BlueSky™ GPS Firewall
  The term global positioning system (GPS) was once used to describe the satellite-based positioning, navigation, and timing system most widely used for civil applications. Tracking multiple GNSS satellites is now commonplace in the age of smartphones and vehicle navigation systems. This application note describes the typical use cases and benefits of multi-GNSS technology and presents data showing achievable time accuracy.

Events Calendar

You can find us at the following events to learn more about the products and solutions offered by Microsemi.

- Upcoming Events
  - International Time and Sync Forum (ITSF) (6–9 November)
  - ATIS: Time and Money Workshop II (23 January)
  - ION: Precise Time and Time Interval Meeting (29 January–1 February)

    - Cisco Live, Barcelona (29 January–2 February)
- Recent Events
    - EFTF–IFCS (10–13 July)
    - IEEE–ISPCS (27–29 August)
    - ION GNSS (25–29 September)

North and South America
Microsemi, Inc.
3870 North First Street
San Jose, CA 95134-1702
Toll-free in N. America: 1-888-367-7966, Opt. 1
Telephone: 408-428-7907
Email: FTD.Support@microsemi.com
Internet: www.microsemi.com

Europe, Middle East, and Africa (EMEA)
Microsemi Global Services EMEA
Altlaufstrasse 42
85635 Hoehenkirchen-Siegertsbrunn
Germany
Telephone: +49 700 3288 6435
Fax: +49 8102 8961 533
Email:
FTD.EMEASupport@microsemi.com
FTD.Emeasales@microsemi.com

Asia Pacific
Suite A201, 2nd Floor,West Wing,
Wisma Consplant 2, No. 7,
Jalan SS16/1, 47500 Subang Jaya
Selangor, Malaysia
Toll-free in N. America: 1-888-367-7966, Opt. 1
Telephone: 408-428-7907
Email: FTD.Support@microsemi.com