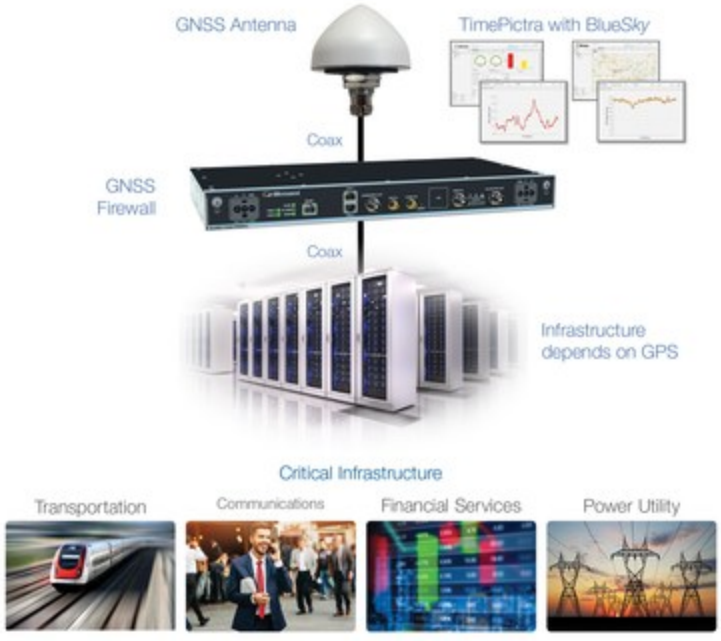
September 24, 2018

New BlueSky GNSS Firewall From Microsemi Provides Secure, Continuous Timing Integrity in GPS-Denied Environments

Showcasing at ION GNSS+ in Booth 612, Security-Hardened System Provides Resilience for Over 30 Days Without Live Sky Access

ALISO VIEJO, Calif., Sept. 24, 2018 /PRNewswire/ -- GPS revolutionized the world with its ability to provide accurate and cost-effective positioning, navigation and timing (PNT), yet its rapid adoption has caused critical infrastructure sectors to be overly dependent upon the satellite-based system. The signals transmitted from GPS and other Global Navigation Satellite System (GNSS) constellations can be a threat vector, which, if disrupted, could harm key critical infrastructure sectors including telecommunications, energy, transportation, emergency services and data centers. The susceptibilities of the GPS signal to attack, whether intentional or not, are viewed similarly as a cybersecurity threat. In recent months, there has been a dramatic increase in the number of reported GPS incidents, causing critical infrastructure providers to evaluate the security, reliability and resiliency of their GPS-based PNT dependency.



The new BlueSky™ GNSS Firewall from **Microsemi Corporation**, a wholly owned subsidiary of **Microchip Technology Inc.** (Nasdaq: MCHP), enables critical infrastructure providers to harden the security of their operations from GPS threats and deliver a more reliable and secure service. The security-hardened system provides protection against GPS threats such as jamming, spoofing and complete outage. It also supports a range of precision timing technologies, including atomic clocks, to enable continuous operation when GPS may be completely denied for extended periods. In addition, Microsemi is expanding the GNSS portfolio with the introduction of a BlueSky option to its TimePictra™ software management suite, providing centralized control and visibility of GPS reception across regional, national and global geographic areas.

"At last year's ION GNSS+ show we launched the BlueSky GPS Firewall Evaluation Kit to help customers understand GNSS vulnerabilities and how a firewall approach could provide protection," said Randy Brudzinski, vice president and manager of Microsemi's Frequency and Timing business unit. "We received valuable feedback from customers as a result of those evaluations and have incorporated new features in our second-generation BlueSky GNSS Firewall. In addition to expanded monitoring and reporting capabilities, this robust, future-proof platform is now equipped with atomic clock technology to provide security-hardened resiliency, including the ability to operate in a GNSS-denied environment for more than 30 days."

Microsemi has applied the same principles of a firewall used for network security to defend against GPS threats coming from the sky. Within the new BlueSky GNSS Firewall, the incoming GPS signal is analyzed in real time to detect a wide range of threats before connected GPS receivers and related systems are affected. The BlueSky GNSS Firewall incorporates an optional internal rubidium Miniature Atomic Clock (MAC) enabling continuous output of the GPS signal to the downstream GPS receiver in case of complete loss of live sky GPS reception. Alternatively, Microsemi's cesium clocks, such as the 5071A or TimeCesium 4400/4500, can be connected to the device, enabling UTC traceable time for more than 30 days.

Microsemi's BlueSky GPS Firewall platform features optional BlueSky software incorporated into its TimePictra management system. To ensure the BlueSky GNSS Firewall is equipped to defend against an ever-evolving threat, Microsemi updates and continuously tracks GPS signal manipulation, spoofing threats, jamming attacks, multipath signal interference, atmospheric activity and many other issues which can create GPS signal anomalies, disruptions and outages. These updates are available through a BlueSky subscription service. To learn more about Microsemi's GPS threat protection and security solutions, including videos demonstrating how the product provides secure and resilient protection, visit https://www.microsemi.com/company/technology/gps-threat-protection-and-security.

Product Availability
Microsemi's BlueSky GNSS Firewall is available for orders now with delivery beginning in November 2018. For more information, visit https://www.microsemi.com/product-directory/gps-instruments/4398-bluesky-gps-firewall or contact sales.support@microsemi.com.

Microsemi to Showcase BlueSky GNSS Firewall at ION GNSS+ in Booth 612
Microsemi's technical experts will be showcasing the new BlueSky GNSS Firewall, along with its full range of timing and synchronization solutions including the latest advancements in atomic clocks, timescale solutions, and PTP and NTP server systems, in booth 612 at the International Technical Meeting of the Satellite Division of the Institute of Navigation (ION

GNSS+), taking place Sept. 24-28 in Miami, Florida. To schedule a meeting with Microsemi at the show, register at https://www.microsemi.com/details/374.

About Microsemi
Microsemi Corporation, a wholly owned subsidiary of Microchip Technology Inc. (Nasdaq: MCHP), offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center 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; enterprise storage and communication solutions, security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, California. Learn more at www.microsemi.com.

View original content to download multimedia:http://www.prnewswire.com/news-releases/new-bluesky-gnss-firewall-from-microsemi-provides-secure-continuous-timing-integrity-in-gps-denied-environments-300716980.html

SOURCE Microchip Technology Inc.