Amtest-TM s.r.o.
Svatováclavská 408, 686 01 Uherské Hradiště, Česká Republika
IČ: 26266890, DIČ: CZ26266890
Tel.: +420 572 572 028 Fax: +420 572 544 216
E-mail: supp@amtest-tm.com, Web: www.amtest-tm.com

Focus Telecom – Protecting critical infrastructure

Focus-Telecom has based its PNT security on years of experience to develop a line of smart security products that deliver front-end cyber solutions that protect critical infrastructure from jamming attacks

With a world heavily dependent on GNSS providing positioning, navigation, and timing (PNT) information, it is vital that the integrity of the signals, especially location and time accuracy, remain trusted. The quality of GNSS signals is affected by jamming, spoofing, and other cyber-attacks. Blocking GNSS signals can significantly disrupt an organization's systems or even disable the entire organization.

GPS Resilient Kit

- Blocking GNSS signals can significantly disrupt an organization's systems or even disable the entire organization. It is essential to receive good quality signals while staying protected from such attacks.
- Focus Telecom's GPS Resilient Kit is a cybersecurity device that comes with two antennas for monitoring and protecting time-critical infrastructures. It can be integrated with any GNSS receiver, either as a retrofit or in greenfield deployments.
- Using OtoSphere™ at its core, the GPS Resilient Kit not only protects systems against GNSS threats but also offers reliable monitoring and real-time reporting to infiniCloud via a cellular link, allowing for minimal downtime of critical PNT systems.
- The advantage of the GPS Resilient Kit is that when a jamming attack occurs, the user's GNSS Receiver will continue being locked to L1 and pass through most of the other frequencies.

Features

- Proprietary Interference Filtering Algorithm for maximum protection
- Minimal power consumption
- Based on proven OtoSphere™ technology
- Cloud-based monitoring with real-time reporting of jamming attacks
- Economic, compact solution, Latency: 100ns ± 15ns (fixed), Insertion loss: 6.5dB ±2dB
- Protected signal: 1575.42 MHz (GPS L1 C/A code)
- Pass-through signals: L5, Galileo E1B/C, GLONASS G1, Beidou B1 & B2, QZSS L1C, E5A

Link to the datasheet: Focus Resilient Kit v2_data sheet (filesusr.com)

RF Switch

- Protect PNT against GPS RF Vulnerabilities
- The ease with which a GNSS RF signal can be blocked or disrupted and the damage this can cause, have made every organization understand the paramount importance of protecting GNSS systems. Erroneous positioning, navigation, and timing (PNT) information in any part of the infrastructure can jeopardize security and disrupt user service.
- Most cyber-attacks on time systems are performed through RF signals entering time servers. One of the best ways to protect these systems is to isolate them by disconnecting their antenna, which mitigates exposure to GPS vulnerabilities such as GPS spoofing or jamming.
- The RF Switch is a programmable, hardware-based standalone solution that protects your PNT systems from vulnerabilities by isolating them from the RF signals coming from the antenna.
- During this time, the server maintains accurate time from its internal oscillator.
- Since an accurate oscillator also drifts over time, once every few days, weeks, or months, the antenna can be reconnected periodically to allow the time server to calibrate itself.

Features:

- Real bi-directional isolation
- Programmability for predetermined
- Disconnection of antenna feed
- Remotely accessible for immediate
- Disconnection or connection of GNSS
- Physical disconnection response Time <10ms
- GUI response time <1s
- Supports full L1 & L2 GNSS

Link to the datasheet: [Focus RF Switch data sheet v2 (filesusr.com)]

GPSensor

- Monitoring PNT Jamming Threats
- Monitor PNT for GPS Vulnerabilities.
- Visibility of jamming attacks is essential to protecting critical infrastructure.
- The GPSensor is a standalone device that monitors GNSS frequencies and reports intentional and unintentional attacks.
- It carries out regular monitoring of each site and transmits critical information in real-time over a cellular link, either to our InfiniDome cloud or to the customer's dedicated cloud.

Features:

- Easy to install and use
- Compact and portable

Amtest-TM s.r.o.
Svatováclavská 408, 686 01 Uherské Hradiště, Česká Republika
IČ: 26266890, DIČ: CZ26266890
Tel.: +420 572 572 028 Fax: +420 572 544 216
E-mail: supp@amtest-tm.com, Web: www.amtest-tm.com

- Regular monitoring of jamming threats at each site
- Alerts of intentional and unintentional attacks on GNSS frequencies
- Easily identify which site is under attack
- The intensity of the attack at any given moment and how it changes over time
- Duration of the attack
- Displaying daily/weekly GNSS & cellular data

Link to the datasheet: Focus GPSensor data sheet v3 (filesusr.com)

OtoSphere™

- Industry's only commercial GNSS protection solution
- The innovative device is a small, add-on module to any GNSS based system that protects it from GNSS jamming attacks.
- OtoSphere™ ensures continuity of autonomous navigation and timing signals.
- OtoSphere™ enables normal operation during jamming conditions.
- No other solution offers such protection and is as small, light, affordable, and easy to install. OtoSphere™ is unregulated by export control

Features

- Proprietary Interference Filtering Algorithm
- Small form factor:74 x 47 x 25 mm, 150 g
- Minimal power consumption: < 1 W (nominal)
- IP67 waterproof rating
- Automotive temperature grade compliant
- Protected frequency: GPS L1 (C/A Code)
- Passthrough frequencies: GPS L5 & Glonass G1 BeiDou Optional)
- Latency: 100ns ±15ns (fixed)
- Insertion loss: 6.5dB ±2dB

Link to the datasheet: Focus OtoSphere data sheet v1 (filesusr.com)