Microchip GPS Firewall
Обладнання для захисту від перешкод (jamming & spoofing) прийому GPS

Основні властивості

- Виявлення з сигналізацією та захист систем з використанням GPS від підміни сигналу GPS (spoofing) та навмисних перешкод сигналу GPS (jamming)
- Сумісний з будь-якою антеною GPS, яка працює в частотному діапазоні L1, L2, L5
- Живлення AC або за технологією PoE (Power-over-Ethernet) спрощує розгортання систем шляхом підключення **GPS Firewall** до інтерфейсу Ethernet
- Безпечний та простий у використанні веб-інтефейс з локальним та віддаленим інтерфейсом CLI

Захист систем GPS від загроз підміни сигналу GPS (spoofing) та навмисних перешкод сигналу GPS (jamming)

Вразливість систем GPS до втрат сигналу добре відома. Разом з швидким розповсюдженням GPS ці вразливості стали проблемою для критично важливих інфраструктур, які потребують даних позиціонування, навігації та синхронізації часу (PNT – position, navigation and timing) і одержують їх від навігаційної системи GPS.
Microchip GPS Firewall додатково встановлюється між існуючими антенами GPS та системами, які використовують сигнали GPS, чим забезпечує ефективне рішення для захисту як нових, так і вже впроваджених систем GPS без потреби системних змін.
Microchip GPS Firewall програмно-апаратними засобами постійно контролює сигнал GPS, в разі його спотворення виявляє та повідомляє про це і формує захист системи GPS від впливу спотворених зовнішніх сигналів.

Виявлення та захист систем GPS від spoofing та jamming

Microchip GPS Firewall використовує вбудований інноваційний програмний алгоритм, який аналізує сигнал GPS. Характеристики прийнятого сигналу GPS кожного супутника аналізуються та одночасно оцінюються на відповідність різноманітним критеріям.

Органічна інтеграція між існуючими антеною GPS та системою GPS

Microchip GPS Firewall підключається між вже існуючими антеною та приймачем GPS і може бути розміщений безпосередньо поруч із GPS-приймачем або поблизу місця введення кабелю від антени GPS всередину будівлі. Таким чином, вже задіяні GPS-антени підтримуються BlueSky GPS Firewall без зміни існуючої установки обладнання.

ПЗ з можливістю оновлення та безпечний інтуїтивний веб-інтерфейс

В основі роботи **GPS Firewall** – програмне прецизійне виявлення аномалій шляхом перевірки сигналів GPS на їх підміну (spoofing) на основі визначених критеріїв перевірки даних. В **GPS Firewall** використовується широкий спектр критеріїв для виявлення підозрілих невідповідностей одержаних значень часу та даних позиціонування. Як тільки ідентифіковано нові загрози, нові критерії та правила перевірки завантажуються у **GPS Firewall** після отримання нових релізів.