

Забезпечте свій час

Стійкість у світі змін



GPS та ширша сімейство супутникових систем, відомих як GNSS, зазвичай описують як технологію позиціонування. Її найважливіша функція — час.

Кожна мобільна мережа, фінансова транзакція, електромережа, дата-центр і система мовлення залежать від точного, спільного відчуття часу, яке безперервно передається на мільярди пристроїв через супутниковий сигнал, що досягає Землі слабше, ніж фоновий шум. Положення, навігація та таймінг часто розглядаються як три окремі можливості. На практиці основою є час. За точного часу система все ще може оцінювати положення за допомогою інерційних або альтернативних сенсорів. Навпаки — неправильно: саме положення не може забезпечити точний час. Ця основа зараз під масштабною атакою, і обидва методи атаки різко відрізняються. Глушіння переважує сигнал, поки приймачі не втрачають блокування: це порушує, але зазвичай помітно, і те, що добре спроектовані мережі можуть придушити за допомогою антен проти заглушення або зберегти якісний запас. Підробка — це більша небезпека. Вона не відмовляє у обслуговуванні, вона обманює, підкидаючи отримувачу переконливу підробку, щоб система продовжувала працювати, тихо вірячи у брехню. Зловмисники часто підробляють GPS, одночасно глушивши інші сузір'я, тому отримувач не може перевірити це і змушений довіряти підробці. Для критичної інфраструктури підробка таймінгу є найшкідливішою формою з усіх. Він повільно і навмисно відволікає мережу від UTC, спочатку наносекунди, потім мікросекунди, потім мілісекунди, і коли дрейф стає очевидним, синхронізація між сайтами може вже бути втрачена. Для операторів телекомунікацій це проблема стійкості мережі, а не навігації: точне визначення часу лежить в основі синхронізації, передачі 4G і 5G, ефективності спектра та бекхолу. Мережа залишається підключеною, поки сервіс тихо погіршується під поверхнею. Тривоги можуть не спрацювати, рух руху продовжується, але часовому орієнтиру, що керує всією системою, вже не можна довіряти.

Це відбувається на порозі Європи

Це вже не далека проблема. Він розташований на межі повітряного простору НАТО та морських шляхів і поширюється. У всьому Балтійському та Північному регіонах перешкоди майже постійні з 2022 року: європейські органи авіацію фіксують тисячі випадків глушіння щороку і немає ознак зниження темпів. Тривалі порушення вдарили по Фінляндії, балтійських країнах, північній Польщі та Швеції, зосереджених у східній частині Балтії та Фінській затоці, тоді як регулятори повідомляють про різке масштабування навмисної підробки, причому підозрюваних передавачів зросло більш ніж у десять разів за один рік. Занепокоєння настільки серйозне, що на початку 2026 року понад десяток європейських урядів спільно попередили, що втручання тепер загрожує морській безпеці та торгівлі.

І це не обмежується лише Балтикою. Авіаційні органи попереджають, що перешкоди GPS тепер простягаються по всьому ширшому діапазону повітряного простору — від східної частини Середземного моря та Чорного моря до Росії та Балтійського регіону, кордону Індії та Пакистану, Іраку та Ірану, а також Корейського півострова. Навколо Ормузької протоки, Червоного моря та Перської затоки він став звичайною небезпекою як для судноплавства, так і для авіації. Те, що раніше було час від часу неприємністю, тепер стало щоденною реальністю, і люди, які покладаються на цей сигнал, часто навіть не підозрюють, що сигнал був скомпрометований.

Від порад до обов'язку

Протягом багатьох років отримання часу вважалося хорошою практикою. Це змінилося. Уряди та регулятори тепер повідомляють операторам телекомунікаційних мереж і критичної інфраструктури, що від них очікують дій. У Сполучених Штатах Виконавчий указ 13905 визначив відповідальне використання PNT, вимагаючи, щоб порушення або маніпуляції часами мали мінімальний вплив на національну безпеку, економіку та критичні функції, і федеральні агентства з моменту публікації офіційних найкращих практик для стійкого PNT у сферах зв'язку, фінансів, комунальних послуг і транспорту. У Європі Директива NIS2 покладає на ключових операторів зобов'язання щодо стійкості, дедалі частіше включно з цілісністю термінів, від яких вони залежать; Galileo впровадила автентифікацію сигналу, щоб користувачі могли підтвердити справжність сигналу, а Європейська комісія створює сервіси для виявлення та виявлення перешкод у регіоні. У Великій Британії національна рамка PNT встановлює рекомендації щодо стійкості для операторів критичної інфраструктури, підкріплені значними новими інвестиціями в Національний центр таймінгу. Повідомлення послідовне. Один супутниковий сигнал більше не є прийнятною однозначною точкою відмови. Від вас очікують, що ви виявлятимете перешкоди, доведете справжній час і продовжуєте бігти, коли небо стихне.

Забезпечте свій час

Питання вже не в тому, чи буде GNSS заважати. Це те, чому ти довіряєш, коли це так. Стійкість починається з верифікації: джерела таймінгу автентифікуються, перевіряються з незалежними джерелами, моніторяться на наявність аномалій і забезпечуються достатньою кількістю ресурсів для забезпечення операцій під час порушення. Альтернативні наземні, геостационарні та низькоземні орбітальні джерела додають додаткові рівні впевненості, щоб довіра до часу більше не залежала від одного сигналу, що надходить із космосу. У сучасному світі проблема вже не в тому, щоб знайти час. Це доводить, що час, який ви отримуєте, є справжнім.



VIAVI закриває цю прірву двома ідеями, які проходять крізь усе на наступних сторінках.

TrustedPNT: ніколи не довіряйте, завжди перевіряйте. Замість того, щоб припускати, що сигнал хороший, системи VIAVI автентифікують, перевіряють і кваліфікують кожне джерело таймінгу, а потім безшовно переключаються на те, якому довіряють, якщо інше буде скомпрометовано. Атака не має права голосу.

SecureTime: більше ніж одне джерело. Проблема — ставити все на GPS. SecureTime додає незалежні, складніші для атаки джерела поверх стандартного GNSS:

- altGNSS LEO — зашифрований, незалежний від GNSS сигнал, який подається через мережу Iridium на низькій навколоземній орбіті, точний до понад 65 наносекунд UTC.
- eGNSS та altGNSS GEO — автентифіковані сигнали, що подаються з геостационарної орбіти (живляться Fugro AtomiChron на Inmarsat) з вбудованим виявленням фальсифікації та точністю до кількох наносекунд.
- Позиціонування LEO (LOCUS), незалежне від GNSS таймінгу з підтримкою позиціонування платформ у русі. Разом із сильними залишками та наземними джерелами це означає, що ваш час залишається надійним навіть тоді, коли GPS цього не робить.



Зупинити загрозу на антені

Захист на передовій для цінних сайтів і платформ, перш ніж поганий сигнал потрапить до вашого приймача.

Смарт-антена фазованої решітки AJAS-DF

Розумна антена, яка пригнічує глушіння і відкидає підробку в точці входу, і повідомляє, звідки йде загроза. Він захищає чотири ключові навігаційні діапазони (L1, L2, L5 та Iridium) і використовує пеленгацію, щоб показати азимут глушнику або спуферу, а також справжню північ. Вбудований транскодер передає вашому існуючому обладнанню чистий GPS L1-сигнал, тож він переходить у застарілі системи без редизайну. Чому це важливо: це не просто підтримує PNT під час атаки, а й перетворює вашу антену на сенсор, який визначає джерело. Достатньо міцний для військової техніки та цінних активів, а також однаково пристосований для цивільних об'єктів, таких як аеропорти, електростанції, дата-центри та стільникові вежі.

- Придушення глушників до 50 дБ у чотирьох діапазонах
- Визначення напрямку для загроз, плюс Північ
- Чистий вихід GPS L1 для оновлення plug-and-play

Забезпечте час у вашій мережі

Гросмейстер і центральні тактики, які підтримують синхронізацію телекомунікацій і критичної інфраструктури, були побудовані стійкими з нуля.



SecurePNT EdgeGM 7000

Компактний, стійкий гросмейстерський годинник для мережевого краю. Він використовує таймінг із кількох орбіт (стандартний багатодіапазонний GNSS плюс альтернативи LEO та GEO) та з наземних джерел, автентифікує кожну з них і безперешкодно переключається на надійний референс. Усе це розміщено у напівстійкому пристрої з високошвидкісним PTP до 25G. Чому це важливо: надійний, стійкий таймінг на межі без компромісу у швидкості. Коли потрібно перейти з 10G на 25G, це ліцензія на програмне забезпечення, а не просто заміна. Створено для 5G і 6G, відкритого RAN, AI-дата-центрів та приватних 5G.

- Багатоорбітальне стійке таймінг (GNSS, LEO та GEO)
- До 25G PTP гросмейстер і NTP-сервер
- Форм-фактор півстійки, шлях оновлення програмного забезпечення

SecurePNT 6200



Стійкий PNT-такт для критичної інфраструктури, що працює на платформі з нульовою довірою, багатоджерелом. Він поєднує GNSS з альтернативними джерелами LEO та GEO, а також може посилювати застарілий такт, подаючи чистий, надійний сигнал. Чому це важливо: стійкість для майданчиків, які не можуть терпіти збій у таймінгу, і спосіб захистити існуючі годинники за частку вартості їх заміни. Опції утримання підтримують вас навіть тоді, коли всі сигнали зникли.

- Комутація з нульовою довірою, багатоджерела
- Вбудований ретрофіт-транскодер для застарілих тактів
- Рубідієвий або керований духовкою залишковий варіант, відповідає PRTC-A та NEBS

Стійкість без заміни

Вам не потрібно розбирати обладнання, яке ще працює. Вони додають сучасної стійкості GPS-годинникам і приймачам, які ви вже використовуєте.



Захищений модуль µPNT-440

Вбудований модуль, який розташований між антеною та застарілим GPS-годинником і подає йому чистий GPS-L1-сигнал, створений із надійних альтернативних джерел. Застарілий годинник працює як зазвичай, навіть коли GPS глушить або підробляється. Чому це важливо: додати стійкості існуючому набору без переробки системи, на площі, достатньо малі, щоб її можна було вбудувати майже будь-де.

- Лінійне модернізування антени та тактового сигналу
- Мультиджерела: GNSS, LEO та GEO
- Precision Holdover, повністю вбудований



RSR Transcoder 2.0

Міцний пристрій, який приймає сучасні гарантовані PNT-входи (M-Code, SAASM, інерціальні системи та інші сигнали можливості) і перетворює їх у стандартний GPS-радіочастотний сигнал, який вже розуміють існуючі приймачі. Розроблений для транспортних засобів, літаків і портативного тактичного використання. Чому це важливо: він поєднує сучасні захищені PNT-джерела та величезну встановлену базу застарілих GPS-приймачів, з передачею часу понад 5 наносекунд і підтримкою прихованої роботи з вимкненням світла.

- Перетворює M-код, SAASM та інерціальні входи у GPS L1/L2 RF
- Тактична та міцна, випробувана за MIL-STD-810
- Автоматичне виявлення типових військових і комерційних приймачів



Впроваджуйте стійкість у власні продукти

Для інтеграторів та OEM-виробників, яким потрібен гарантований таймінг у власних системах. Частотні стандарти та приймальні модулі у малих, малопотужних, вбудованих формах.



LN Rubidium GPSDO

Рубідієвий, дисциплінований GNSS-частотним стандартом для найнижчого фазового шуму та найкращої стабільності у компактному, енергоємному модулі з сильним збереженням при падінні GNSS. Чому це важливо: референсний таймінг, де чистота сигналу та збереження сигналу мають найбільший значення, а також чисте оновлення для тих, хто вже користується лінійкою GPSDO VIAVI на масштабі чіпа.

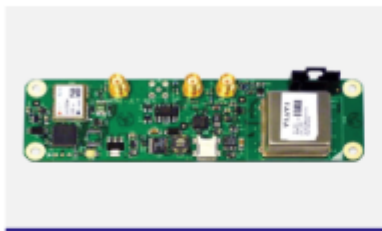
- Ультранизькофазовий шум і найкраща стабільність у класі
- Затримка на субмікросекунду
- Менше 5,6 Вт



Micro-JLT GNSSDO

Генератор наступного покоління з дисциплінованим GNSS, створений для великого обсягу та низької вартості, з найкращими розмірами, вагою, потужністю та вартістю на ринку. Він сумісний за формою та функцією з популярним FireFly-IIA. Чому це важливо: стійкий таймінг у масштабі для бюджетних конструкцій, з варіантами, готовими до умов сильних ударних ударів і вібрацій.

- Найкращий розмір, вага, потужність і вартість у своєму класі
- Багатосузір'я GNSS
- Варіанти, сумісні з FireFly-IIA, з подовженою температурою та низькою перевантаженістю



Mini-JLT

Заміна Trimble Mini-T GPSDO, що вже давно закінчилася, з кращою стабільністю та фазовим шумом, а також корисними опціями, такими як зовнішній вхід 1 PPS, вбудований акселерометр і USB. Чому це важливо: чистий шлях оновлення для всіх, хто спроектований навколо Mini-T, без переробки плати.

- Заміна Trimble Mini-T з функцією Formfit
- 72-канальний багатосузір'яний GNSS
- Покращена стабільність і фазовий шум



Приймальний модуль STL-2600 LEO

Приймальний модуль, який фіксується на сигналі STL Iridium на низькій навколоземній орбіті для GNSS-незалежного таймінгу, що можна простежити до UTC. Сильний запасний варіант на випадок, коли GPS не можна довіряти. Чому це важливо: додає незалежне, важче заглушуване джерело таймінгу до будь-якого дизайну.

- Iridium STL таймінг на низькій навколоземній орбіті
- Краще за 65 наносекунд до UTC
- Низька потужність



Захищений приймальний модуль STL-1000 LEO μ PNT

Ультрамалий модуль M.2, який поєднує прийом GNSS та Iridium STL для гарантованого таймінгу в умовах обмеженого простору. Чому це важливо: багатоджерельне гарантоване таймінг у найменшому можливому об'ємі, для вбудованого та OEM-використання.

- Форм-фактор M.2
- GNSS плюс Iridium STL
- Зазвичай менше 1 Вт

Підтримуючі компоненти

SecureTime altGNSS GEO-L Гвинтова антена

Стійка до погодних умов гвинтова антена, яка подає альтернативний сигнал GEO у продукти VIAVI GEO-L, включаючи SecurePNT EdgeGM 7000L, SecurePNT 6200L та μ PNT GEOL-2600.

- Діапазон GEO-L
- IP67, створений для зовнішнього монтажу
- Пари з продуктами VIAVI GEO-L



Загроза тут, регулятори чіткі, і виправлення не обов'язково означає починати з нуля. Чи ви забезпечуєте національну мережу, захищаєте один критично важливий об'єкт, чи створюєте стійкість у власних продуктах — VIAVI має свій шлях. Поговоріть з VIAVI про доказ концепції і дізнайтеся, наскільки надійний ваш таймінг, перш ніж хтось інший це зробить.



viavisolutions.com

Зв'яжіться з +1 844 GO VIAVI | (+1 844 468 4284)

Щоб дістатися до найближчого до вас офісу VIAVI, відвідайте viavisolutions.com/contact

© 2026 VIAVI Solutions Inc.

Характеристики та описи продукції в цьому документі можуть змінюватися без попередження. Запатентовано за адресою viavisolutions.com/patents secureyourtime-br-pnt-nse-ae 30195118 900 0626

