MARKET INTRODUCTION

Focus Telecom

SETTING THE STANDARD
IN PNT PROTECTION

February2021

About Focus Telecom

- Founded in 1995, Focus Telecom has been a leading supplier of time and frequency synchronization solutions.
- The company has since emerged as an innovator in GPS security, developing unique, patented technologies and producing solutions that protect critical infrastructure against attacks on their Positioning, Navigation and Timing (PNT) systems.
- Focus Telecom's highly experienced team also offers consulting, cyber defence and turnkey solutions. Our end-to-end timing solutions generate, distribute and apply resilient time for multiple sectors: Communications, Government & Security, Finance & IT, Industrial, Transport and Energy.
- The company has recently started to extensively focus on the field of security to complement its timing expertise, with a variety of solutions such as satellite data communications systems (RT-Logic), video and control systems, and combat intelligence networks (RGB Spectrum).
- The company implements high standards according to ISO 9001:2015, certificated and approved by the Israel Standards Institute, as well as other global standard organizations - like IQNet.
- Additionally, Focus Telecom is approved by the Ministry of Defence, Israel Aircraft Industries, Elbit and other defence industry and government organizations.
- Having formed close and long lasting partnerships with suppliers and customers, Focus Telecom is well positioned to enable customers to build more reliable networks and systems supporting today's precise PNT standards.

Protecting against GNSS Jamming

- World heavily dependent on GNSS providing PNT information, >10 billion devices
- 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.
- Vital to protect integrity of the signals, especially location and time accuracy
  - Essential to receive good quality signals while staying protected from these attacks.

SETTING THE STANDARD IN TIME SOLUTIONS

GNSS NEEDS PROTECTION!

SETTING THE STANDARD IN TIME SOLUTIONS

Published at: Jun 26 2020 - 09:55 / **Updated at: Nov 19 2020 - 14:44**

"This has been going on for so many years now that I believe this is a part of the new 'normal' and we have to prepare for it", says District Police Chief Ellen Katrine Hætta.

FROM
PETER B. DANILOV

In recent years, the GPS net in Finnmark, Northern Norway has been going down on a regular basis due to jamming of signals.

District Police Chief Ellen Katrine Hætta first noticed jamming in 2017 and then notified the Norwegian Police Directorate.

The National Security Authority has analyzed the jamming and in September 2018 they verified that the jamming came from the east. The Norwegian intelligence services have concluded that Russia was behind it.

Jamming is a way of destroying a signal through sending out one signal that overshadows another one. In this way, jamming GPS signals brings communications and navigation systems down and they lose their function.

By Simon Harwood and Ivan Petrunin, Cranfield University

Published Wednesday, December 16, 2020

Timekeeping technology is struggling to keep up with the many aspects of modern life that rely on it, but more reliable and resilient solutions are on the horizon.

Even with the use of ultra-precise atomic clocks, time is a more fragile and unreliable commodity than we think. The UK government estimates that the time stamps used in London's financial trading are affected by between 80 and 120 GPS jamming incidents every month. In 2016, the decommissioning of a single GPS satellite led to 12 hours of IT and phone system errors globally.

BY **DANA A. GOWARD** 11-23-2020 06:10:03

"How to Steal a Ship" will be one of the presentations at a U.S. Department of Transportation workshop on the 3rd of December. The event will feature speakers from Maersk, the U.S. Coast Guard, MARAD, and the department's Research and Technology arm, among others.

Jamming, blocking signals, and spoofing - sending false signals to make a receiver report it is in a false location - have been increasing concerns for maritime operators over the last five years. A study by the German research institute DLR found interference on GPS frequencies during every phase of a year-long voyage between Europe, the Far East and back. In 2019, the U.S. Coast Guard brought interference with GPS signals as an "urgent issue" to the International Maritime Organization.

During a choreographed light show in Hong Kong in 2018, a jamming device caused 46 drones to fall out of the sky. The resulting property damage and loss of hardware cost an estimated HK$1M. Nearly all drones have safety protocols to send them home or to some safe landing location in the event of disruption. But those features proved ineffective at the Hong Kong show.

The Infrastructure Impact

- According to US Department of Homeland Security (DHS):
  - There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.
  - DHS considers 13 of the 16 critical infrastructure sectors to be critically dependent on PNT (Positioning, Navigation, Timing).
  - The other 3 sectors are considered to be somewhat dependent.

Ref: Proportional Defence by Omer Sharar, CEO, infiniDome

SETTING THE STANDARD IN TIME SOLUTIONS

What markets do we target?

Government

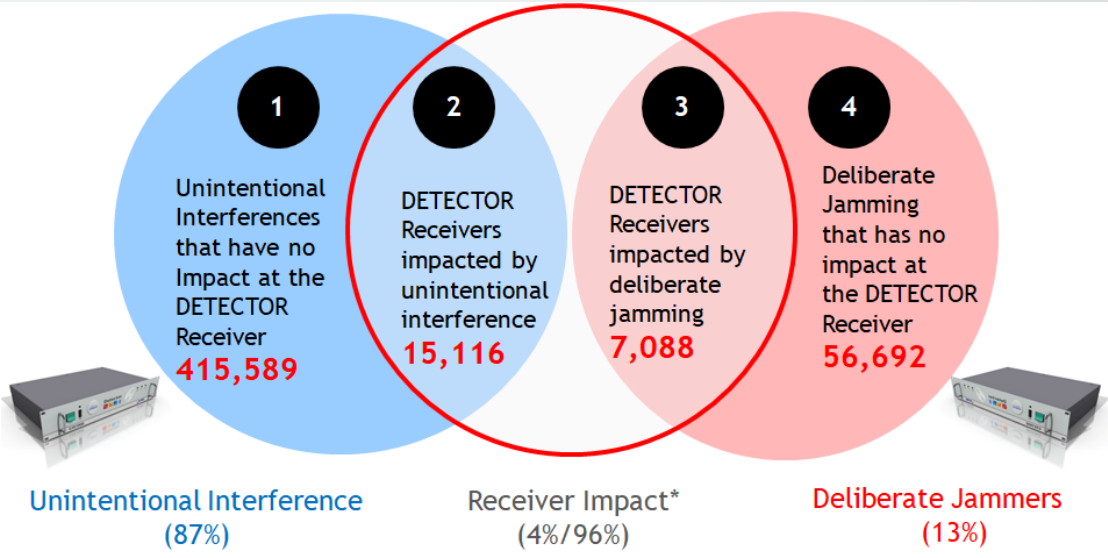
Military
Public safety (police, fire, ambulance)
Border control
Offices

** As defined by the EU Resilens Project*

SETTING THE STANDARD IN TIME SOLUTIONS

STRIKE3 monitored jamming events from 50 sites in over 20 countries

United Kingdom	Netherlands
Sweden	Belgium
Finland	Croatia
Germany	Latvia
France	New Zealand
Poland	Canada
Czech Republic	India
Slovakia	Vietnam
Spain	Thailand
Slovakia	Malaysia
Slovenia	Japan

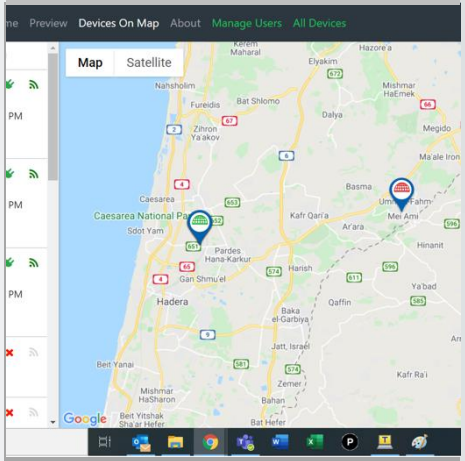


Courtesy of the European GNSS Agency (GSA), Strike3 programme

SETTING THE STANDARD IN TIME SOLUTIONS

Focus Telecom Product Portfolio

SETTING THE STANDARD IN TIME SOLUTIONS

GPS Resilient Kit	GPSensor	RF Switch	InfiniCloud
			
Protection & Monitoring in One. Protects time servers against GNSS threats while offering reliable monitoring and real-time reporting.	Standalone sensor. Alerts of intentional and unintentional attacks on GNSS frequencies. Regular monitoring of each site, displaying daily/weekly data.	Hardware-based standalone solution that protects your PNT systems from vulnerabilities by isolating them from the RF signals	Industry's first GPS jamming attack monitoring and management system. Control and visibility of GPS health and attacks for critical assets.

Confidential ©2021

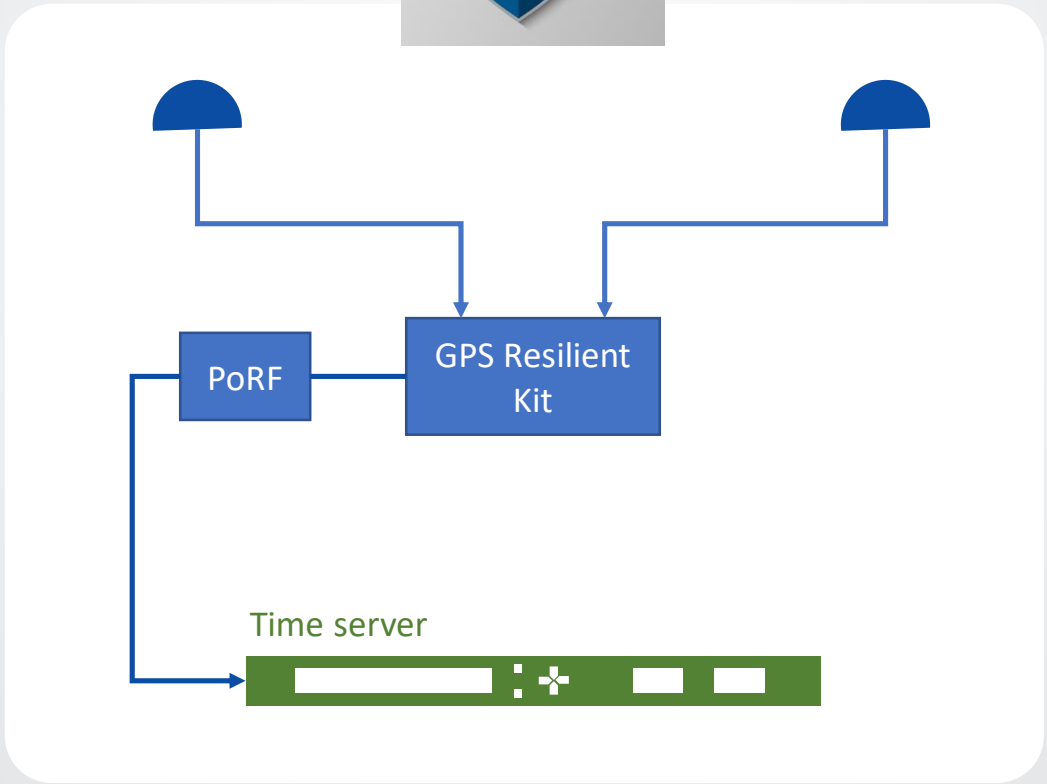
GPS Resilient Kit Applications

Monitor, report & Protect against GPS jamming threats in critical infrastructure:

- Financial centres
- Telecom centres
- Data centres
- Energy/Utility facilities
- Government
  - Military
  - Public safety (police, fire, ambulance)
  - Border control
  - Offices
- Hospitals
- Transportation
  - Airports
  - Hangars (civilian and military)
  - Shipping
  - Fleet management
  - Tunnels (auto & rail)
  - Underground/Metro
  - Bus Terminals
- Hi Tech campuses
- Retail
  - Large malls, underground parking
  - Warehouse automation & delivery systems

SETTING THE STANDARD IN TIME SOLUTIONS

Protected Sync Server Concept



SETTING THE STANDARD IN TIME SOLUTIONS

GPSensor + InfiniCloud

Ideal GNSS Surveillance Solution

- Visibility of jamming attacks is essential to protecting critical infrastructure.
- GPSensor deployed in multiple sites to collect data on jamming attacks and GNSS performance.
- InfiniCloud management system gives a geographical view to determine the extent of the problem & location of the attacks as well as overall GNSS performance.

SETTING THE STANDARD IN TIME SOLUTIONS

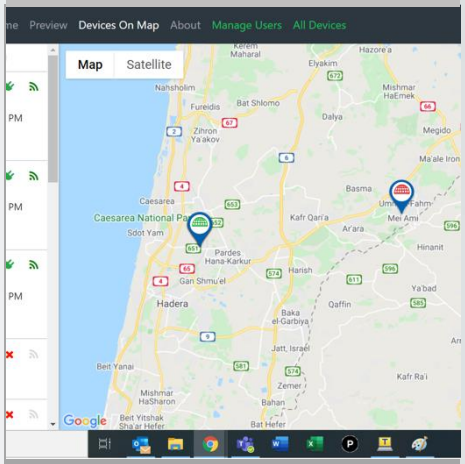
RF Switch Applications

- Energy/Utility facilities
- Financial centres
- Telecom centres
- Data centres
- Military
- Public safety (police, fire, ambulance)
- Airports
- Shipping

SETTING THE STANDARD IN TIME SOLUTIONS

infiniDome Product Portfolio

SETTING THE STANDARD IN TIME SOLUTIONS

GPSDome™	OtoSphere™	OEM Board	InfiniCloud
			
Small, add-on or retrofit module that provides protection against GPS jamming, ensuring continuity of navigation and operation during jamming disruptions.	Small, add-on module for any GNSS-based system that protects it from GNSS jamming attacks using a proprietary Interference Filtering Algorithm	No other commercial solution offering such protection is as small, light, affordable or as easily integrated as our OEM Board	Industry's first GPS jamming attack monitoring and management system. Control and visibility of GPS health and attacks for critical assets.

Introducing GPSdome™

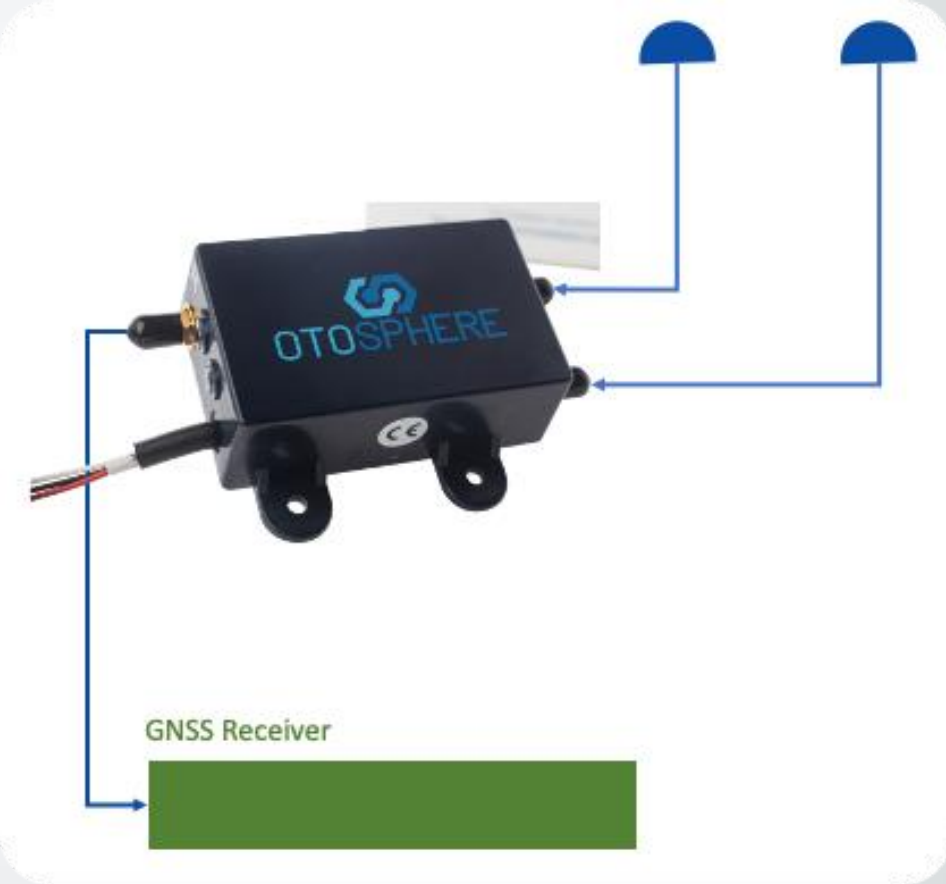
Only Commercial (non-ITAR) GPS Anti-Jammer

- Revolutionary cyber product
- Retrofit protection of all GPS receivers
- Wields military tech in a minimal package
- Protects against jamming of GPS signals
- Uses a “front-end” approach which rejects high-powered interferences before they reach the receiver

SETTING THE STANDARD IN TIME SOLUTIONS

OtoSphere™

- Core of Focus Telecom products
- Proprietary Interference Filtering Algorithm
- Small form factor: < 70 x 48 x 24mm, 150g
- Minimal power consumption: < 0.8W (nominal)
- IP67 waterproof rating
- Automotive temperature grade compliant
- Protected frequency: GPS L1 (C/A Code)
- Passthrough frequencies: GPS L5 & Glonass R1 (BeiDou Optional)



SETTING THE STANDARD IN TIME SOLUTIONS

GPS Jamming – Ranked #1 Threat to UAVs

- UAVs highly vulnerable to GPS jamming attacks.
- All UAVs today depend on GNSS for position and timing accuracy - growing need for accuracy and universal position
- Even when equipped with backup systems like an INS, video analysis or a stationary reference point, GNSS is still required as it's the only absolute method for localization.
- Although considered a vulnerability, the incredible accuracy enabled by GNSS cannot and will not be replaced today
- UAVs cannot even hover in place without GPS because they don't know what "in place" means
- Intentional jamming is no longer a phenomenon limited to theaters of military operations where attacks on positioning and navigation systems accompany efforts to deny communications and electronic surveillance to the enemy.
- Today anyone can buy a GPS jammer online for as little as $30, and those devices are easy to use.

SETTING THE STANDARD IN TIME SOLUTIONS

Fleet protection

- GPSdome & OtoSphere ensure continuity of the navigation and timing signals used by emergency services, logistics, security, and commercial operations. No other device that offers the same level of performance, is as small, light, affordable or as easy to install and conceal as GPSdome & OtoSphere.

Applications

- Designed with in-vehicle applications in mind, GPSdome & OtoSphere are also suitable for a wide variety of other platforms such as personal backpack platforms, stationary applications and many more

Benefits

- Simple to install - GPSdome & OtoSphere are retrofit solutions which do not require changes to existing GPS installations. This keeps installation time to a minimum.
- Many installation options - Its small size and low power consumption makes GPSdome & OtoSphere ideal for installations where space and power are limited, making it suitable for covert applications.
- Widely compatible - GPSdome & OtoSphere can be deployed to add protection to existing installations which have a GPS receiver with external antenna.

SETTING THE STANDARD IN TIME SOLUTIONS

SETTING THE STANDARD IN TIME SOLUTIONS

Thank you

For more information visit

www.pnt-security.com

FocusTelecom