BroadShield (Patented)

GPS Jamming and Spoofing Detection Embedded into Your System

Assure Your PNT System

We want to integrate our patented GPS jamming and spoofing detection software into your hardware platform to assure the Position, Navigation and Timing (PNT) of your product. BroadShield's algorithms are carefully designed to detect interference and anomolies within the GPS signal and GPS spectrum. Orolia Defense & Security will work with product manufacturers to provide a software solution that can conform to the needs of your hardware.
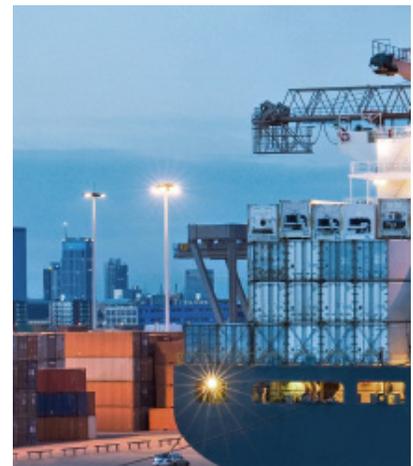

YOUR HARDWARE + **BROADSHIELD** = **ASSURED PNT**

WORK WITH US

We will work with your team to integrate BroadShield into your product without requiring any additional hardware.
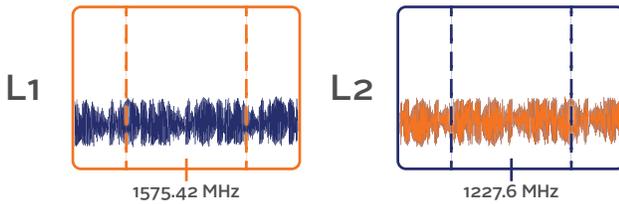
Detect and Defend

PNT systems are designed to provide accurate position and time while in uninterrupted or uncontested environments. However, while in these interrupted or contested environments, most PNT systems are unable to reliably provide position and time data because they are unable to recognized what is causing the disruption. BroadShield is a software library consisting of many patented algorithms designed to detect jamming and spoofing then immediately report the disruption to the PNT system. Leveraging this information enables the PNT system to take action to mitigate and protect from the jamming or spoofing.

Attacks On the Rise

An increased number of GPS jamming and spoofing attacks have been reported and documented in recent years. With high quality software-defined radios (SDRs) becoming more affordable, hardware capable of GPS jamming and spoofing are more available than ever. Open source projects have been found to turn these low cost SDRs into GPS jammers and spoofers. It is more critical now than ever to ensure the necessary precautions are taken to protect your PNT systems.

Trust in Orolia Defense & Security

Have trust in your products PNT solutions knowing that Orolia's BroadShield algorithms have been rigorously tested and field proven for over a decade. Our detection capabilities are regularly updated to conform to new and emerging threats. Our software works with many commercially available GPS receivers and runs on nearly any operating system. With the flexibility of converting our BroadShield algorithms into most major programming languages, no product is out of the question.

Jamming Signals

L1 1575.42 MHz   **L2** 1227.6 MHz

Need a Complete Solution?
Consider one of the options below.

OROLIA SECURESYNC **+ BROADSHIELD**

GPS SOURCE ED3 WITH VCAM **+ BROADSHIELD**

Spoofing

GNSS Simulators	Anomalies in the GPS Data
Data inconsistencies	Jumps in position and time

THREATBLOCKER **DETECTION + PROTECTION**

Integration - What is Needed

GPS receiver that can provide raw GPS NAV data to our software

Processing unit to run the BroadShield algorithms

Integration support — work with our team to make it successful

BROADSENSE NANO **DETECTION**