A Holistic Approach to Protect, Toughen & Augment

Industry is Ready to Help With Resilient PNT

The Global Leader in Resilient PNT

Providing the world's most critical applications real-time, accurate, reliable positioning, navigation, and timing data.

Safety, Security and Reliability

OROLIA PROFILE

Founded in October 2006, Head Office in Washington DC, incorporated in 9 countries

450
Employees including 120 in R&D and Projects

$115m
2017 Revenue

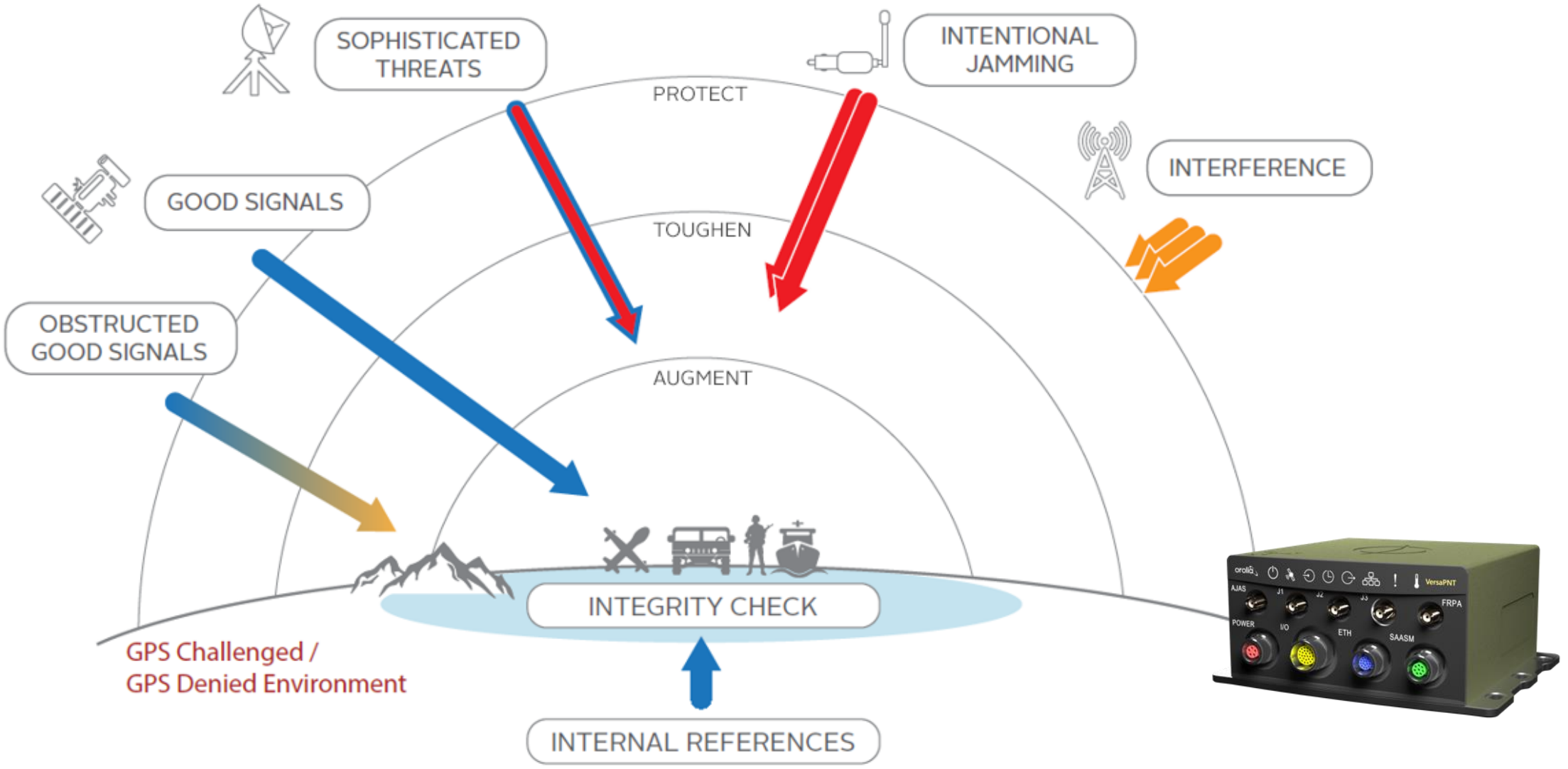
Sales in 85 countries

Worldwide-renowned brands in target segments

spectracom
spectratime
McMURDO
kannad
SARBE
netwave

Acquisitions since Incorporation
11

RESILIENCY, RELIABILITY, PROTECTION WITH INTEGRITY & TRUST



TOUGHENING GPS

SMART ANTENNA TECHNOLOGY

Orolia 8230AJ

infiniDome 1.01

Antcom 4 element

SATIMO
Galileo/GPS

GAJT 710MS

Controlled Radiation Pattern Antennas (CRPA) are the first defense in combatting jamming and spoofing

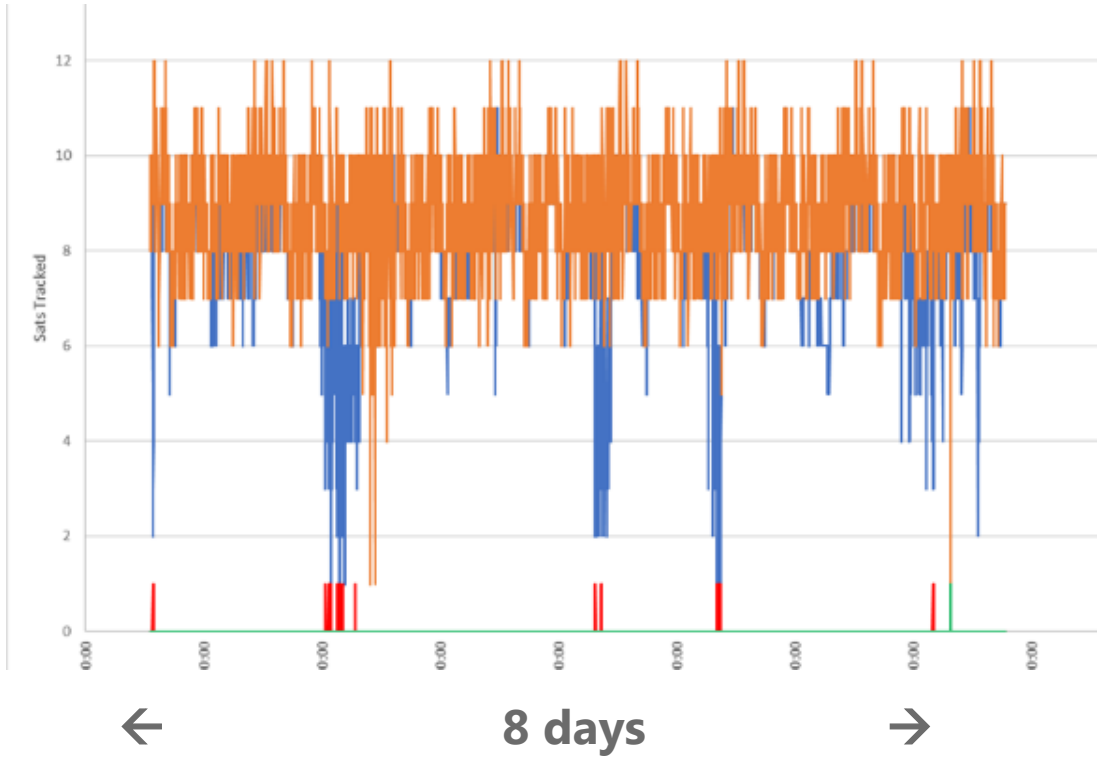
- Solutions range from affordable (~$1K) to very expensive (~$50K) and are available today
- Beams are focused on the satellite signals and focused away from the interference
- Can provide 20 – 50 dB of jamming protection

- **The most effective means of Anti-Jam (AJ) protection as the energy never enters the receiver**

EXAMPLE: SIMPLE AJ ANTENNA FIELD TEST FOR TIMING APP

- Two GNSS Time Servers with internal Rb Holdover oscillators: side by side, one with Standard the other with AJ Antenna
- Experiencing suspected “Privacy Jammer” interference – next to a trucking company
- AJ Antenna drastically reduced GNSS dropout (Holdover Events) over a one-week period

	Standard Antenna	AJ Conical Antenna
Holdover events	40	4
Total time in Holdover	1 hour 32 minutes	41 seconds
Longest holdover event	14 minutes 26 seconds	17 seconds
Average holdover event	2 minutes 18 seconds	10 seconds
Satellite alarms	31	2



INTERFERENCE DETECTION & MITIGATION IN THE RECEIVER

Javad Triumph VS

Novatel OEM-7

Talen-X BroadShield

Modern receivers can filter jamming and interference, detect and reject spoofing

- Advanced Digital Signal Processing (DSP) techniques can remove many types of jamming signals from the GNSS reception
- Even the most sophisticated spoofers do not reproduce the GNSS signals exactly (RF characteristics, pseudoranging, Doppler, and data content) allowing them to be detected and rejected
- Multi-frequency/multi-constellation receivers are now prevalent and add a large measure of jamming resistance
- It is harder to jam multiple frequencies at once

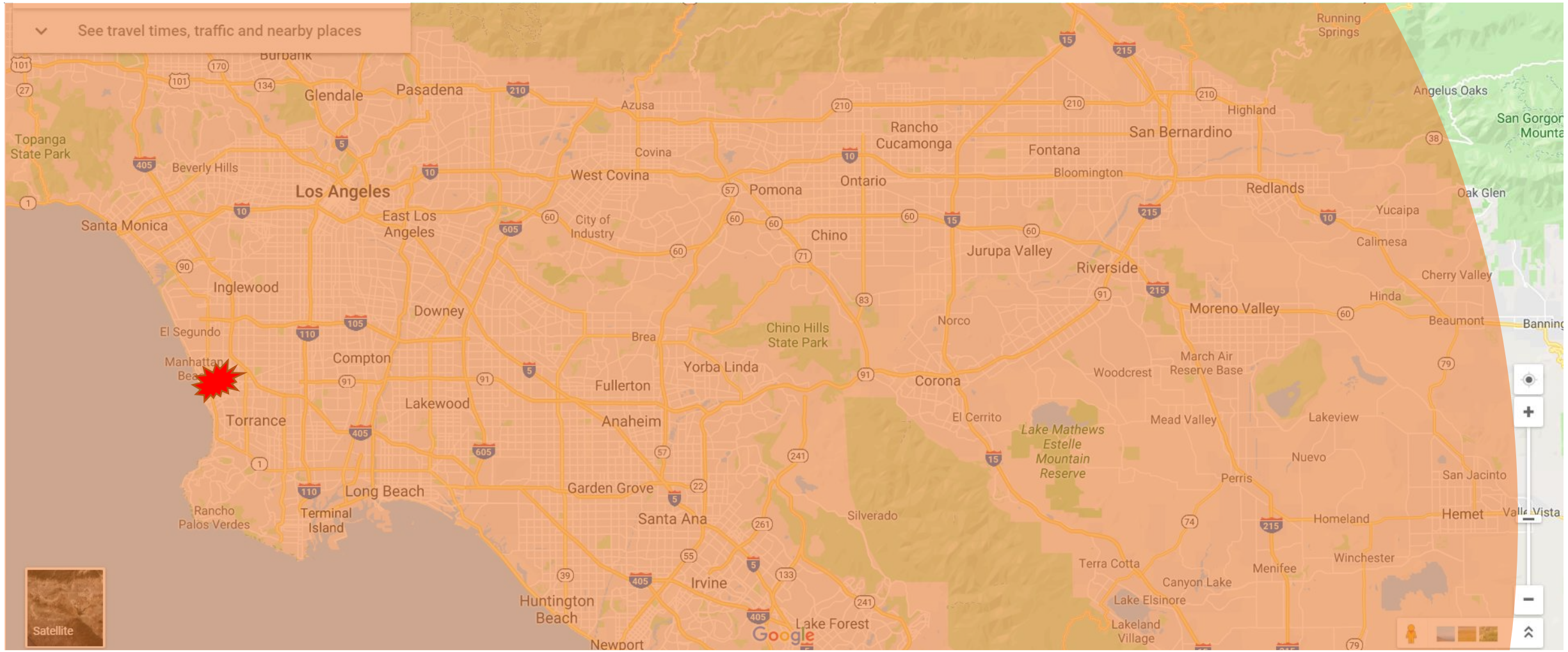
EXAMPLE: TALEN-X THREATBLOCKER

- *Operates with any GPS Antenna or Receiver*
- *>75 different algorithms to detect jamming and spoofing*
- *Filters out the most common jammers*
- *Developed jointly with The Aerospace Corp.*

- *Proven 40 dB J/S protection in US Govt field tests*

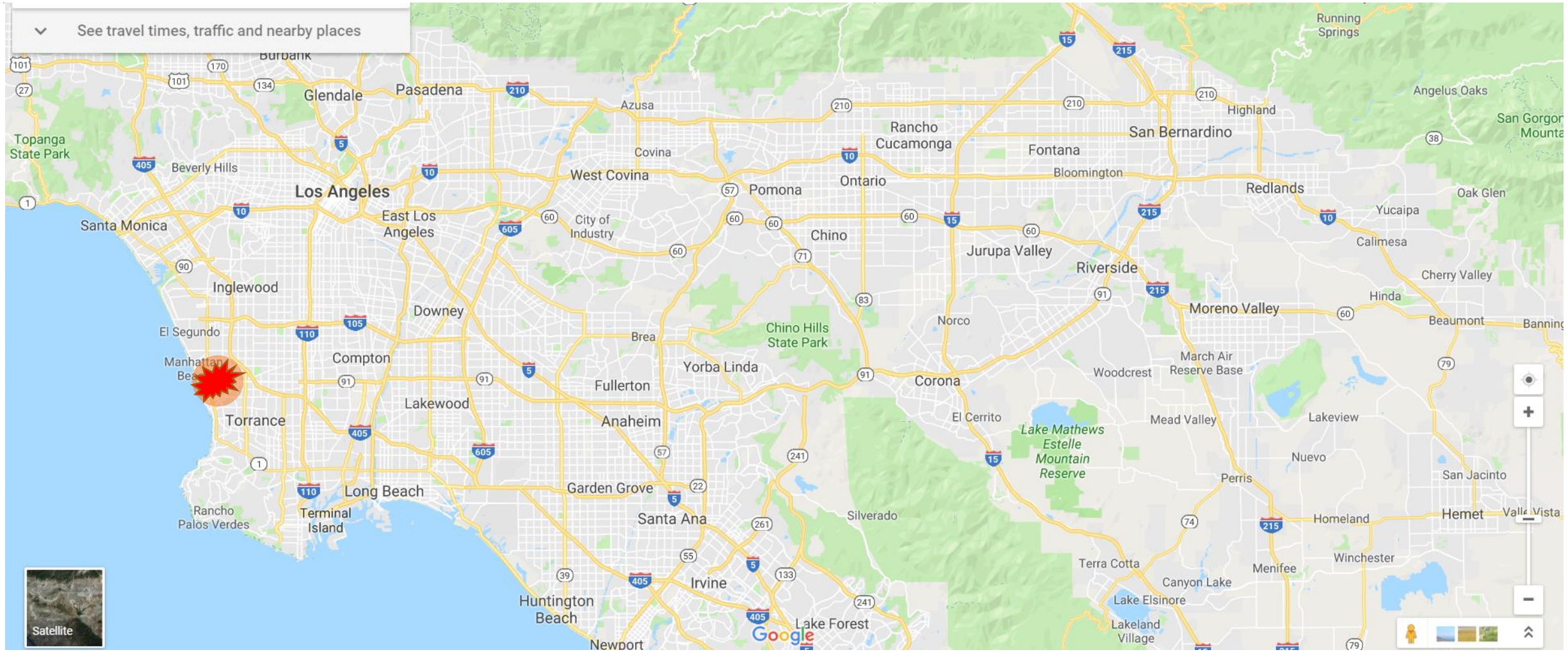
DENIAL AREA OF 100 WATT JAMMER WITHOUT THREATBLOCKER

CENTERED ON REDONDO BEACH



DENIAL AREA OF 100 WATT JAMMER WITH THREATBLOCKER

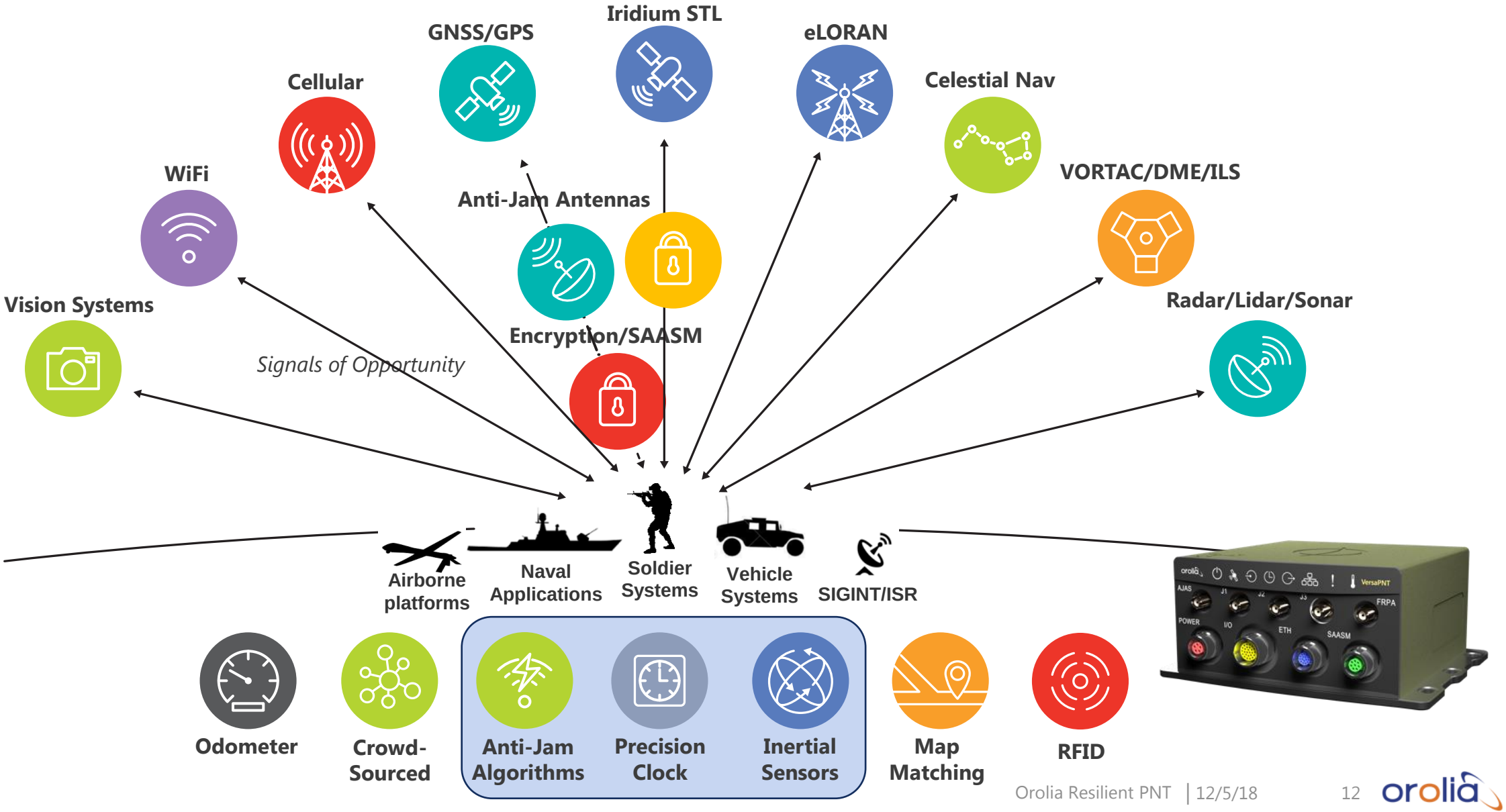
CENTERED ON REDONDO BEACH



35 dB improvement

AUGMENTING GPS

WE SIMPLIFY THE INTEGRATION OF RESILIENT PNT

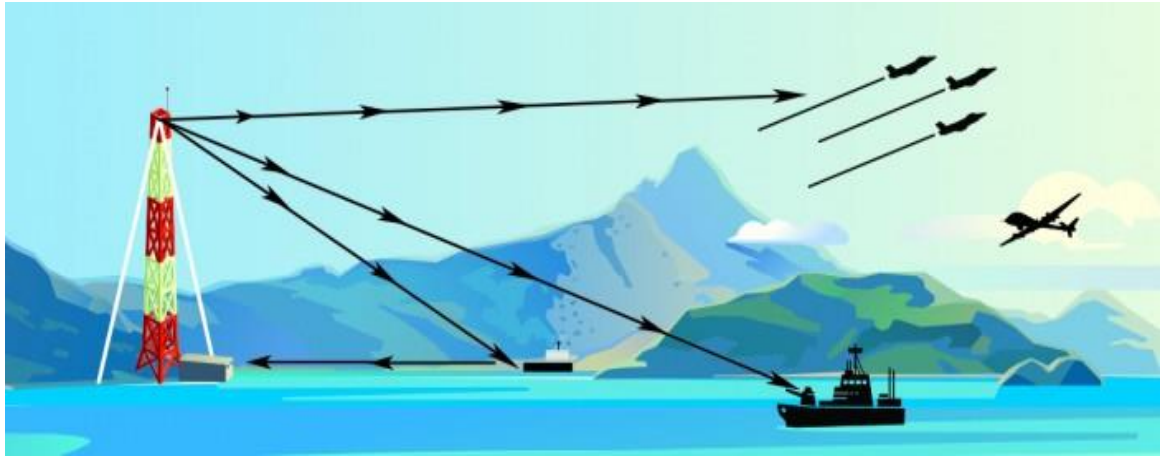


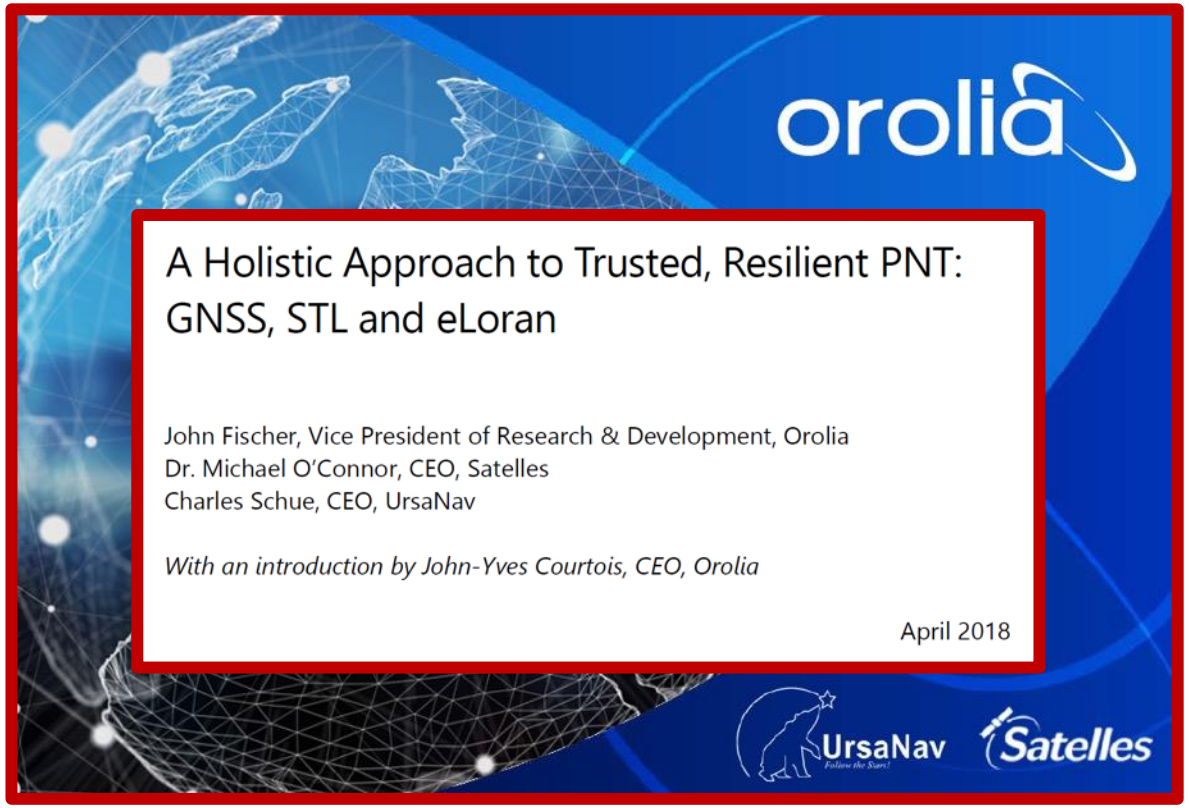
STL – SATELLITE TIME AND LOCATION SIGNAL

- **New signal available today**
  - Broadcast on the Iridium sats
- **>30 dB stronger than GPS**
  - Higher jamming and interference resistance
  - Operates indoors
- **Encrypted signal**
  - Inherently anti-spoof
  - Subscription based service
  - Available for civilian use

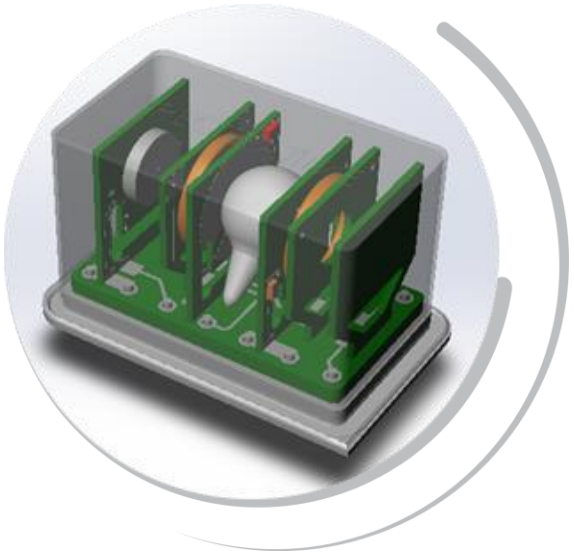
eLORAN

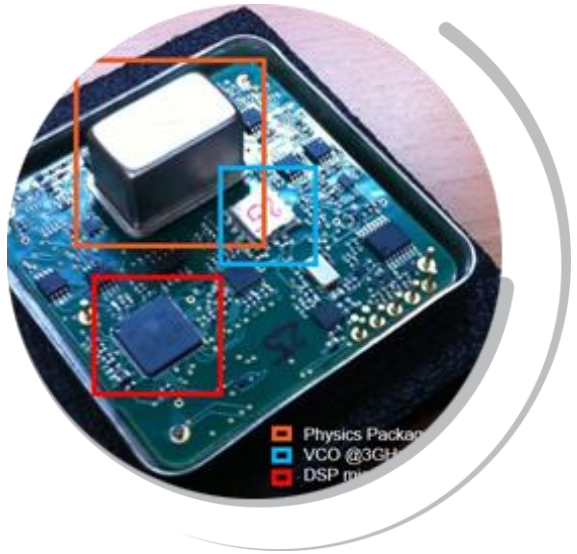
Royal Netherlands Air Force
Have Quick Timing System (HQTS)
eLORAN + GNSS





MINI RUBIDIUM ATOMIC CLOCK

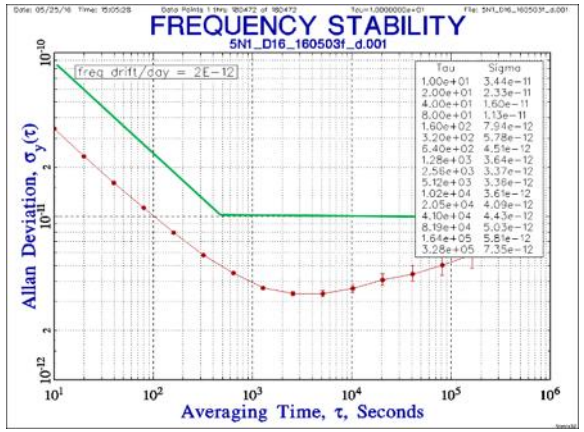




Higher stability performance than CSAC

- Same size and weight
- <500 mW power

- Short-term ADEV = **1E-10 @1sec**
- Frequency drift = **2E-12/day** (specification < +/- 1E-11/day)



PROTECTING GPS

PROTECTION BY MAKING RECEIVERS SMARTER

orolia

The Global Leader in Resilient PNT

GNSS Vulnerability Test System

Challenge

Hardening GPS/GNSS receiver applications against the threat of spoofing

Solution

Orolia GPS/GNSS simulation system with easy control of "real" versus "faked" signals

Results

Full understanding of how a system reacts in a spoofing situation and the effectiveness of mitigation techniques or countermeasures

"Understanding the reaction of GPS-based navigation in various spoofing scenarios is the key to hardening the system against spoofing attacks."

The threats to GPS-based navigation systems are ever-increasing. The risk of intentional disruption of GPS signals is moving from simple jamming to a much higher-level of sophistication. Spoofing — an attempt to deceive by broadcasting false GPS signals — can be devastating, leading to loss of assets or, worse, lives. Although testing the sensitivity to jamming is basic functionality of GPS simulators, measuring the effects of various spoofing scenarios requires a high degree of complexity. Orolia is at the forefront of testing the vulnerabilities of GPS-based navigation and now offers its capability as a GNSS Vulnerability Test System.

Through the integration and synchronization of two Orolia GNSS RF generators, the user has full control of the critical parameters to test the susceptibility to spoofed signals, compared to simulated 'live sky', with varying degrees of the alignment of time, position and RF power. And these tests can be performed under varying motion trajectories, either assuming the spoofer can anticipate the motion or not, and any other condition.

Testing vulnerabilities to any navigation application with a GPS/GNSS simulation system is simply the best way to understand risks and for designing and evaluating countermeasures. For more information about Orolia's work in evaluating the effect of GPS spoofing attacks, see our technical paper, Testing GNSS Receivers to Harden Against Spoofing Attacks.

Orolia's GNSS Vulnerability Test System consists of two simulators, a time and frequency synchronization unit, RF connectors, and PC control system. It comes with training and start-up assistance as well as a service plan so you get the most out of your testing program.

www.orolia.com
www.spectracom.com
The industry-leading Spectracom products you depend on are now brought to you by Orolia, the global leader in Resilient Positioning, Navigation and Timing Solutions.

21 September - GNSS-Vulnerability-Test (B)
Specifications subject to change or improvement without notice
© 2016-2018 Orolia

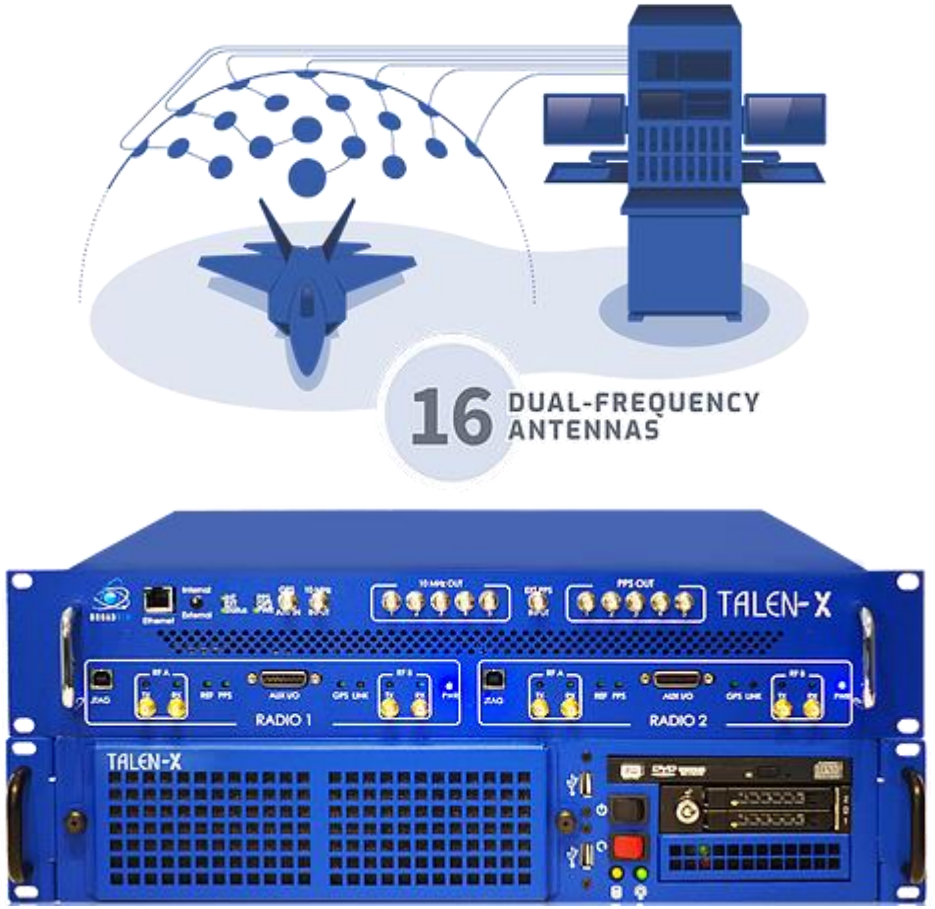
Testing and certification services

- Receiver Certification Testing
- Supported DoT Adjacent Band Compatibility (ABC) initiatives
- Supports US Govt receiver certification efforts

SIMULATION SYSTEMS

- Stress testing with the right scenarios
- Publishing the results

BroadSim Anechoic

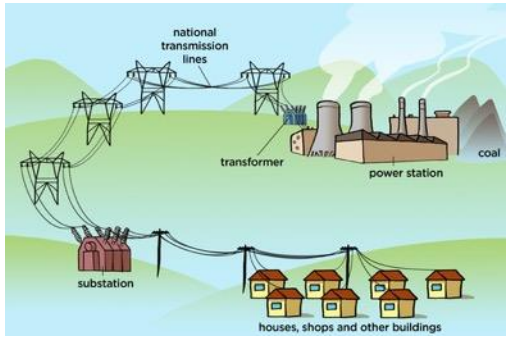


Panacea

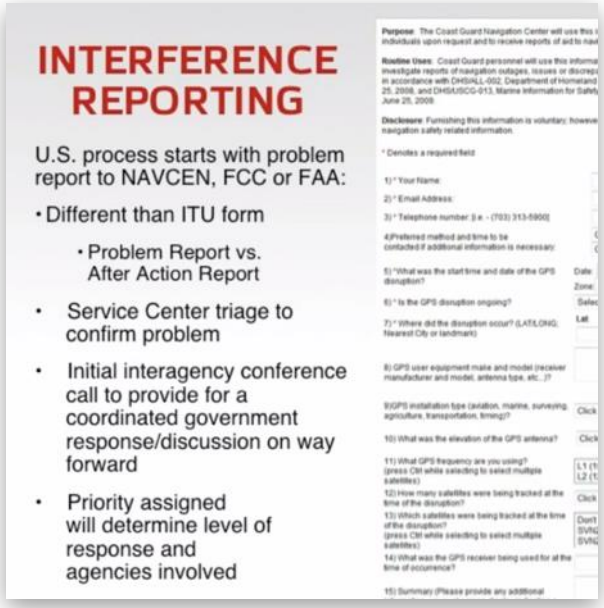
CROWDSOURCED GNSS INTERFERENCE DETECTION SYSTEM

Every GPS receiver connected to the Internet can serve as an interference detector

- Connected Cars
- Cell Towers*
- Smart Power Grid elements
- 911 Call Centers, etc.



**Cell phones not practical detectors because of battery drain*

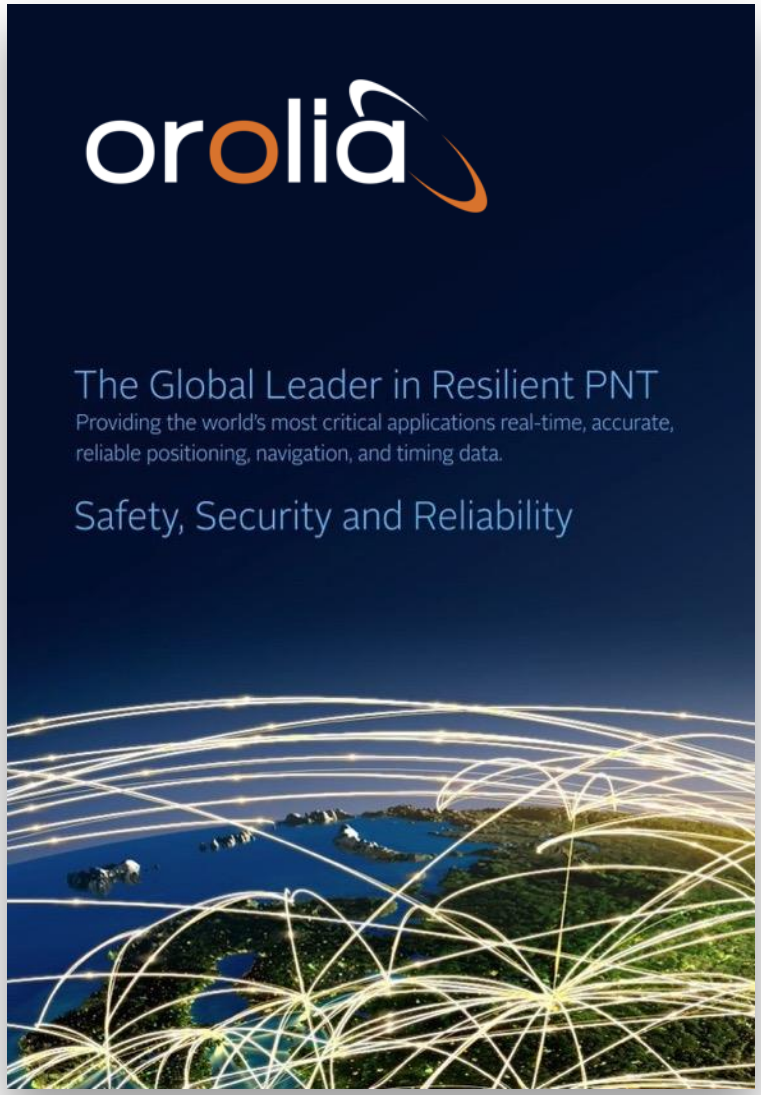


Existing USCG NAVCEN Reporting System

Command and Control Station

- Millions of detectors geographically dispersed
- Positional correlation of multiple reports
- Enforcement
- Response

SUMMARY



Many technologies are available today to Toughen, Augment and Protect GPS

- Public policy can support the adoption of these technologies by:
  - Requiring them in government procurements
    - DHS, DoD, DoT, etc.
  - Establishing standards for GPS receiver performance, analogous to the Risk Management Framework (RMF) in Cybersecurity
  - Establishing a GNSS receiver certification program
  - Establishing a Nationwide Interference Detection and Reporting System
- Private sector alone cannot find the business models to support these initiatives