WE ARE RELIANT ON PNT FOR CRITICAL APPLICATIONS

Our Defense
  Situational awareness
  Precision Weapons
  Guidance
  Navigation
  RADAR Systems
  Range Timing
  SATCOM
  Instrumentation
  ...

Our Critical Infrastructure
  Power Grids
  Financial Markets
  Emergency Services
  Industrial Control
  Telecom
  Precision Agriculture
  Supply Chains
  ...

A Layered Approach to Resilient PNT
GPS/GNSS VULNERABILITIES

Unintentional Threats
• System errors
• Unwanted RF Transmissions
• Natural phenomena

Intentional Threats
• Jamming
• Spoofing
RESILIENT PNT FOR CRITICAL APPLICATIONS

A Layered Approach to Resilient PNT

- Sensor & Signal Fusion
- Threat Generation & Characterization
- Encryption
- Performance Testing & Certification
- Clocks
- IMUs
- PNT Sensors
- NTP/PTP Cybersecurity
- Network Timing
- LEO
- GNSS
- IDM
A Layered Approach to Resilient PNT

Signals containing PNT reference info
Prevent bad signals from entering system
Clean interference from signals
Detect residual interference
Leverage internal PNT information
Detect (residual) anomalies/failures
Prevent cyber attacks through the system
Supporting technologies
EXTERNAL REFERENCES

GNSS is the most widely used primary external reference, with its known vulnerabilities

Other external references are available today as alternatives or layered with GNSS

LEO Constellations
• STL (Iridium), XONA
• Stronger signals, Encryption available

Network Timing
• NTP, PTP, White Rabbit
• Network security needs to be considered

Terrestrial Wireless Infrastructure, Signals of Opportunity
• 5G, NextNav, Locata, TV, Radio
• Emerging standards/technology, Specialized hardware required
Horizon Blocking and Controlled Radiation Pattern Antennas (CRPA) are the first defense in combatting GPS/GNSS jamming and spoofing

- Solutions range from affordable (~$1K) to very expensive (~$50K) and are available today
- Fixed or controlled patterns filter signals from potential interference sources
- Can provide 20-50 dB of jamming protection

- The most effective means of Anti-Jam (AJ) protection is preventing the energy from being received
IN-LINE PROTECTIONS AND INTERFERENCE DETECTION

Additional protection and detection can be added in path between the antenna and the receiver, and operating within the receiver

Available elements today can filter jamming and interference, detect and reject spoofing
  - Detection of interference is critical for any chance to mitigate that interference

Newer receivers are embedding advanced detection capabilities taking advantage of multi-frequency and multi-GNSS reception

New and upcoming signal/protocol security capabilities
  - Galileo OSNMA (Open Service Navigation Message Authentication)
  - NTS (Network Time Security) for NTP
  - PTP (1588-2019) Authentication TLV

Proprietary and open-source software detection libraries are available for integration
"INTERNAL" PNT REFERENCES AND QUALITY DETECTION

Internal references like Rubidium oscillators and MEMs or FOG IMUs provide for the last PNT fallback if all external references are lost or compromised.

These internal references and other platform “internal” references/sensors can also be used to qualify external references for residual anomalies and failures:

- Solution fusing with coherency checks
- Very stable in short term conditions
- Ground “truths” that don’t rely on external elements, virtually shielding them from external interference
THREAT SIMULATION & PERFORMANCE TESTING

Understanding system operation under different threats, hazards, and disruptions helps determine the vulnerability and effects of that vulnerability

• System Errors
• Jamming
• Spoofing
• Loading
A Layered Approach to Resilient PNT

**Layered Approach**

- Layered solutions exist to retrofit existing systems
- Look for modular capabilities to scale based on risk and requirements
- Upgradeability is important (gradual investment in Resiliency possible)
- Evolving with new threats and new technologies
- Protecting past investments

**Layers of Protection**

- **Cybersecurity**
- **Internal Quality Detection**
- **Internal PNT References**
- **Interference Detection**
- **In-Line Protections**
- **Antennas**
- **External References**
- **Orolia Resilient Timing**

**External References**

**Antennas**

**In-Line Protections**

**Interference Detection**

**Internal PNT References**

**Internal Quality Detection**

**Cybersecurity**

**Simulation & Analysis**
The Global Leader in Resilient PNT

David Sohn
Senior Solution Architect
david.sohn@orolia.com