Leveraging Traditional GNSS Time Servers for Resiliency and Interoperability in Complementary PNT (cPNT) Systems

Francisco Girela – Sales Engineering Lead – Francisco.Girela@nav-timing-safrangroup.com

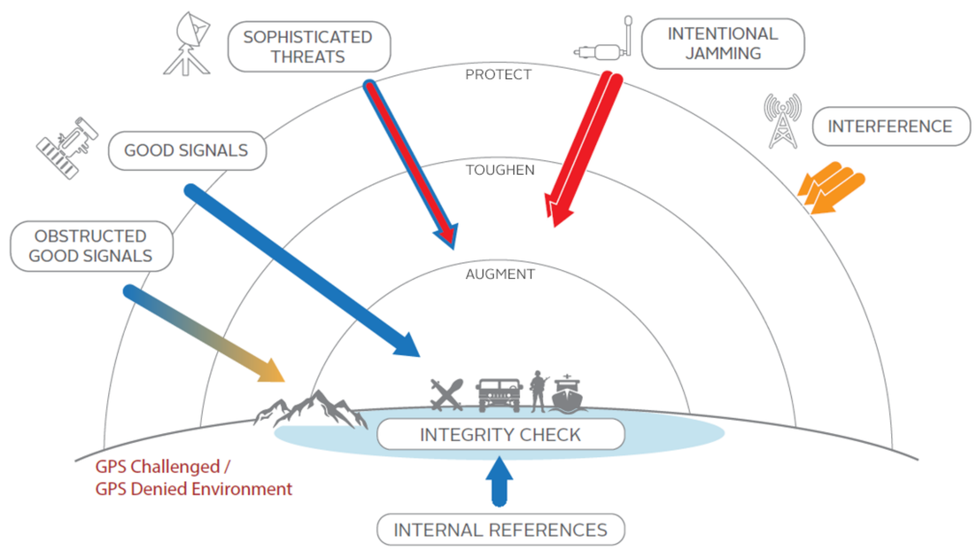
GNSS can and will fail

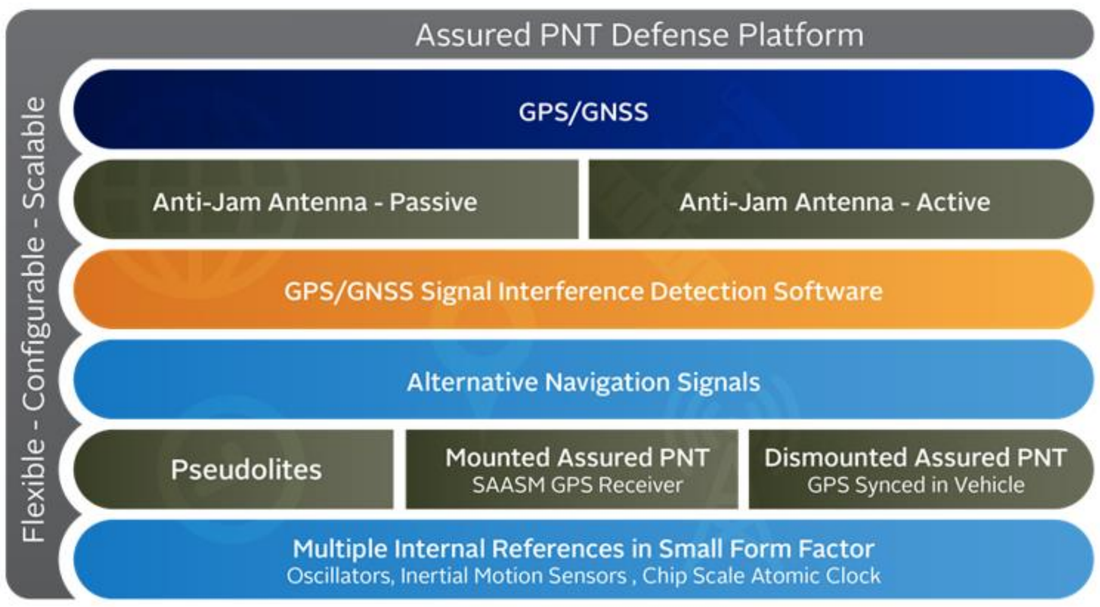
Today, much of our Positioning, Navigation, and Timing (PNT) needs are met by GPS. Precision time signals sent through GPS synchronize cellphone calls, time-stamp financial transactions, and support safe travel by aircraft, ship, train and car.

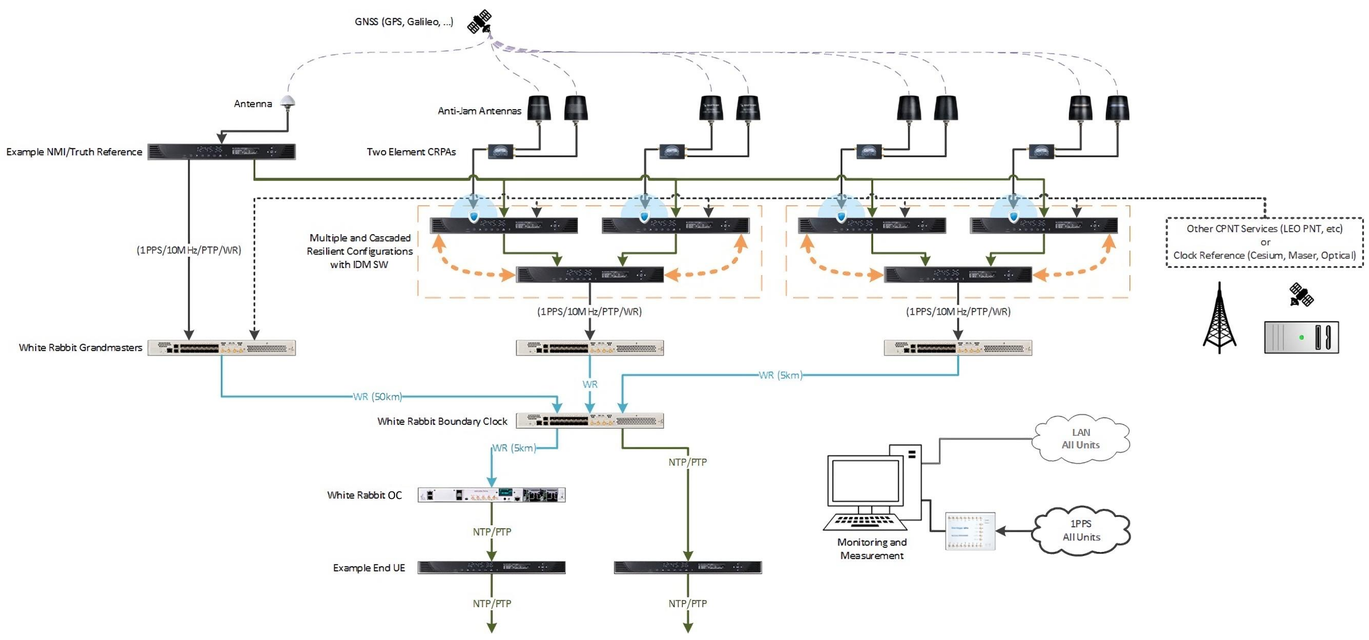
GNSS layer: Support multiple frequencies and constellations has vastly improved the diversity of available sources.

Antenna layer: anti-jamming antennas with smaller observation angle prevent attacks. Anti-jamming devices that combine the signals from multiple antennas can provide an extra level of security in this layer.

Signal interference detection layer: Alert and notify the user of a GNSS-based PNT system about the presence of a threat. GNSS receivers are increasingly equipped with anti-jamming/spoofing features.







GNSS vulnerabilities

Jamming: Intentional interference by means of a radio-frequency signal.

Interferences: Natural causes such as atmospheric phenomena.

Spoofing: Broadcasting false signals with the intent of deceiving a GNSS receiver.

Alternative PNT references layer: Position, Navigation, and Timing (PNT) independently from GNSS.

Pseudolites and Assured PNT layer: Defense-oriented, including CRPA antennas, encrypted technologies as Selective Availability Anti-spoofing Module (SAASM) or M-Code and some other ground-based systems for military applications.

Internal References layer: Holdover solutions, such as oscillators for timing or gyroscopes, altimeters and accelerometers for Inertial Navigation Systems. Chip-sized atomic clocks, make it possible to embed such timepieces in GPS devices which can go for days or weeks without connecting to GPS.

Redundant, hardened generation and timing distribution: Combine hardened GNSS references with Complementary PNT sources and redundant time distribution.

- **High availability**
  Fully redundant configurations, with back-up sources, Wide Area time distribution and local Holdover.
- **Improved reliability**
  Combination of anti-jamming and anti-spoofing hardware, timing outputs isolation from live references, and error-bounded failover combined with real-time metrics of all sources and end nodes.
- **Standard-based distributed solution**
  Prevention of local attacks, blackouts, Acts of God or compromised locations with distributed interoperable time distribution and generation in multiple locations.

Ground-truth network to monitor the timing distribution: Monitor heterogeneous timing distribution networks based on NTP, IEEE 1588 (PTPv2) or analog signals.

- **High accuracy visibility**
  Sub-nanosecond accuracy and hardware timestamping allow high accuracy monitoring.
- **Real-time metrics**
  Inserting distributed probes at strategic points allows measuring the timing performance of the timing distribution network in real-time.
- **Latency monitoring**
  Time of Flight based measurements for latency monitoring, preventing fiber tampering and providing additional information on bottlenecks, malfunctioning or suspicious activity.

SAFRAN