orolia

Resilient Timing for Enterprise

Pritam Kandel
Applications Engineer/Product Specialist

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

WHY RESILIENT TIMING ?
LAYERS APPROACH TO RESILIENCY

- Avoid any single points of failure
- Set of technologies and standards at each layer can help effectively solve the resiliency problem
- Peel failure problems with layer approach

1. **Reference**
   - *GNSS Vulnerabilities (Jamming, Spoofing)*
   - *Weak signal (geographic, urban)*
   - *Quality of internal clock (Oscillator)*
2. **Distribution** (networks of systems)
   - *Very dependent on network topology*
   - *Distribution protocol ? PTP or NTP or WR, something else*
   - *Time distribution devices (switch, router, server, hypervisor, or dedicated hardware)*
3. **Client Systems**
   - *Single time server source*
   - *Other OS level failures (not in scope for this presentation)*

Mitigate the point of failure with layers approach

- **Time Reference**
  - Multiple Reference: GNSS not just the GPS
  - Signal Protection: Spoofing and Jamming
  - Alternative Signal: STL, eLORAN, National Labs
- **Time Distribution**
  - Distribution Protocol: NTP, PTP, WR, PPS
  - Used dedicated Time Servers for Distribution
- **Client Systems**
  - NTP Clients – Multiple NTP Servers (> 3)
  - PTP Slaves – Multiple GMs, and so on

Monitoring System

- Compliance (FINRA/MIFID2, PCI etc.)
- SNMP, RestAPI, Syslog..

PREVIOUS NEXT

REFERENCE RESILIENCY

When you are victim of loss GNSS signal , all you know is GPS is gone (not why)
*If **Spoofed** you may not even know it is happening !*

CHALLENGES

GNSS Signal is very weak (-161.5 dBW)

- 20,000 km above the earth
- Difficulty working indoors
- Highly susceptible to jamming and spoofing
- Very inexpensive and easy option to interfere
- More terrestrial than aerial interference (low elevation)

Case Study – Customer's major datacenter facility, experiencing issues with its GNSS signal reception. The GNSS signal was lost almost daily and frequently

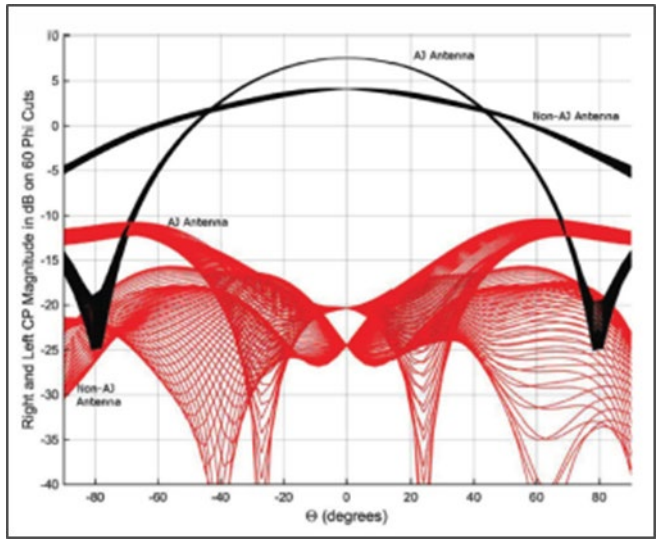
- Service provider using our time server in their large datacenter
- Intermittent loss of GNSS reception, almost daily and frequently for unknown reasons
- Testing showed the issue was not coming from system components
- Test period with a standard Antenna and 8230AJ Antenna on 2 separate time servers

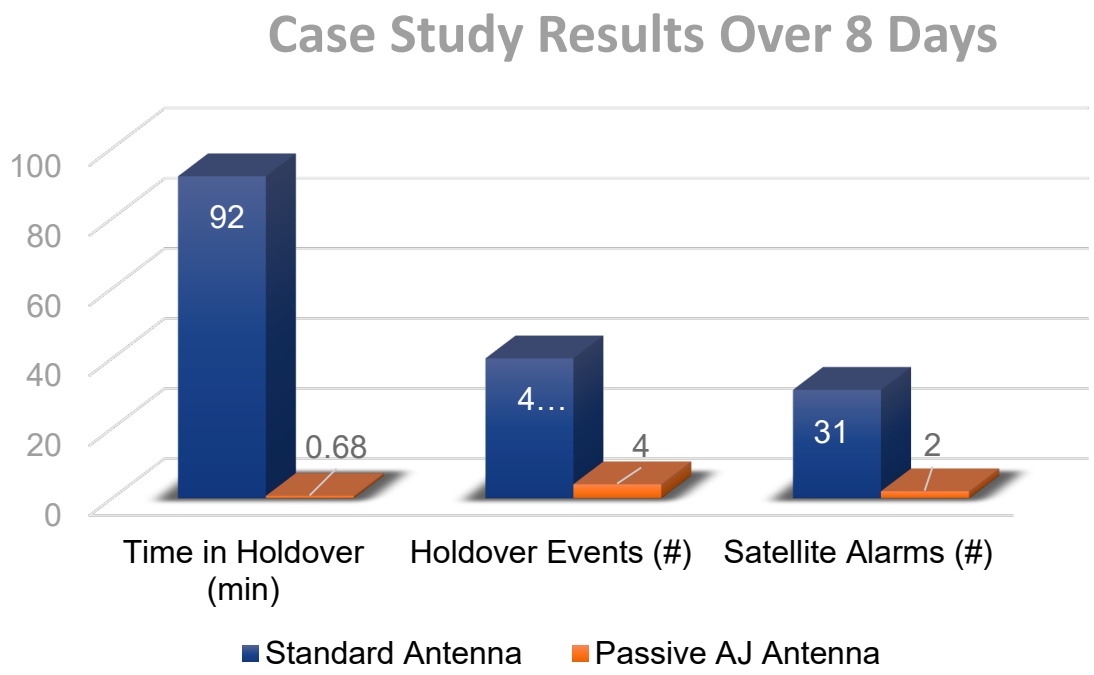
PREVIOUS NEXT

REFERENCE RESILIENCY – ANTI-JAM HORIZON BLOCKING ANTENNA

SOLUTION

- Replacement for standard L1 GNSS antenna
- Horizon blocking antenna technology
- Effective: Signal attenuation at the horizon where most interference comes from
- Low cost and often a drop in replacement for standard antenna (same cable, mount, etc.)
- Suitable for timing and stationary application



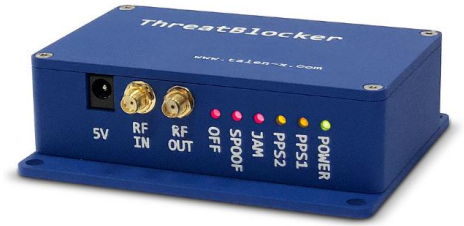


REFERENCE RESILIENCY – SOFTWARE ALGORITHM

SOLUTION

Jamming and spoofing interference detection algorithms

- Over 75 jamming and spoofing detection algorithms working with raw receiver data
- Provides event reporting and data collection
- Can be integrated within customer HW platforms
- Can be Inline GPS jamming and spoofing protection device



REFERENCE RESILIENCY

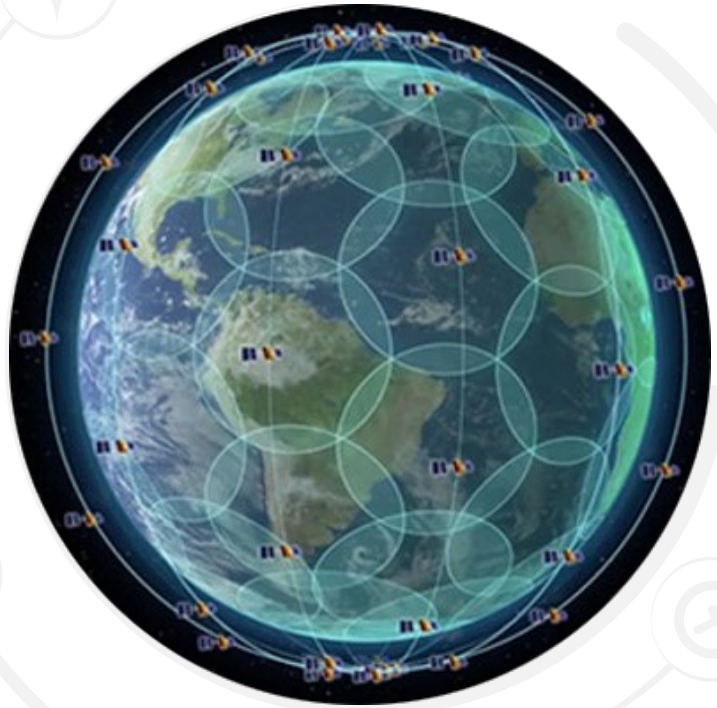
CHALLENGES

Access to GNSS Signal can be limited or not available, especially in the data center environment

Case Study – A major auto manufacturing company ran a critical data center at remote location

- Access to GNSS signal was not available from data center providers
- Unsynchronized systems impact manufacturing processes all around the globe

- Is there any alternative to augment the GNSS signal?



REFERENCE RESILIENCY – ALTERNATIVE SIGNAL STL

SOLUTION

Monitoring Results Over 8 Days

	Average	Std Dev
GPS	-13ns	9ns
STL	-135ns	78ns

Globally available PNT signal broadcast on the Iridium satellite constellation

- **30 dB stronger signal**
  - Interference resistance
  - Better indoor penetration
- **Encrypted signal**
  - Anti-spoofing capability
- **Unidirectional burst message structure**
  - One way communication from the satellites
  - Does not require continuous signal reception
- **Subscription based service**
  - Available for civilian use

DISTRIBTION RESILIENCY

CHALLENGES

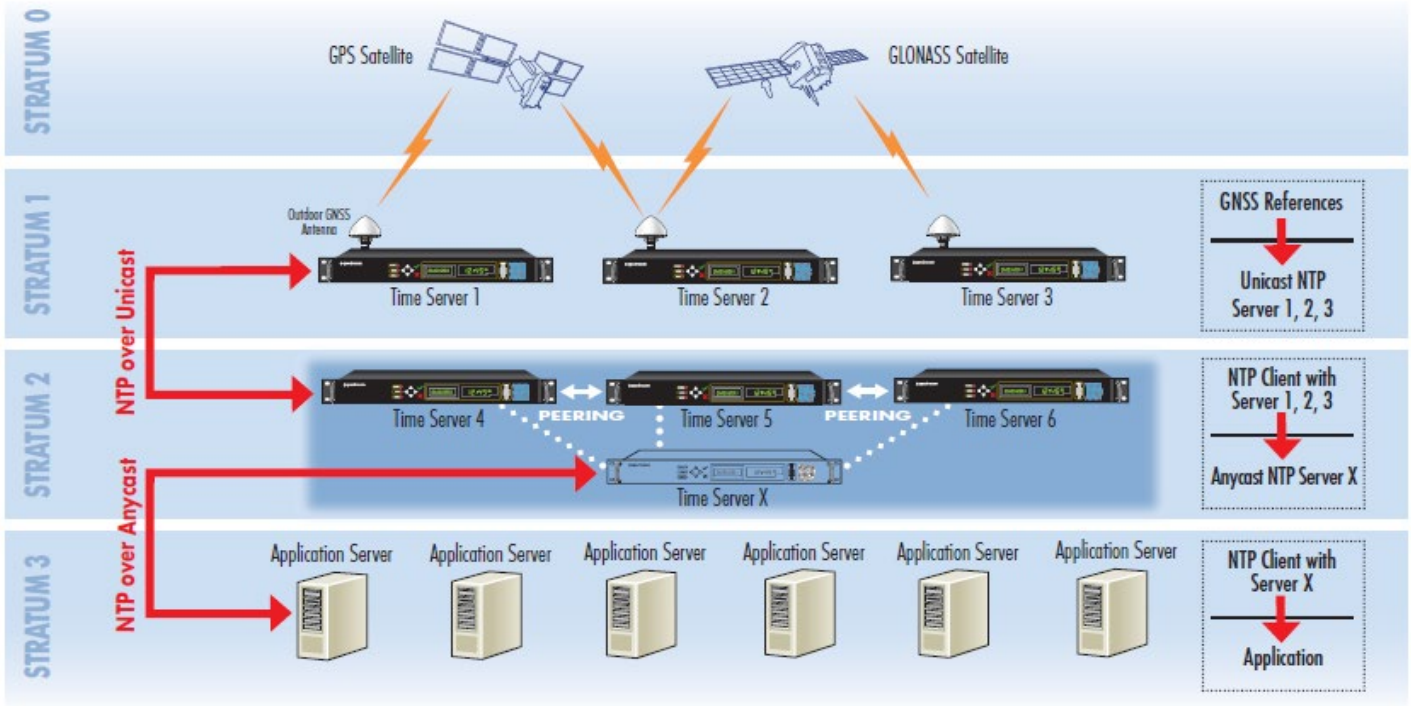
Time distribution infrastructure is equally important for resiliency of timing in the network as it is for time source

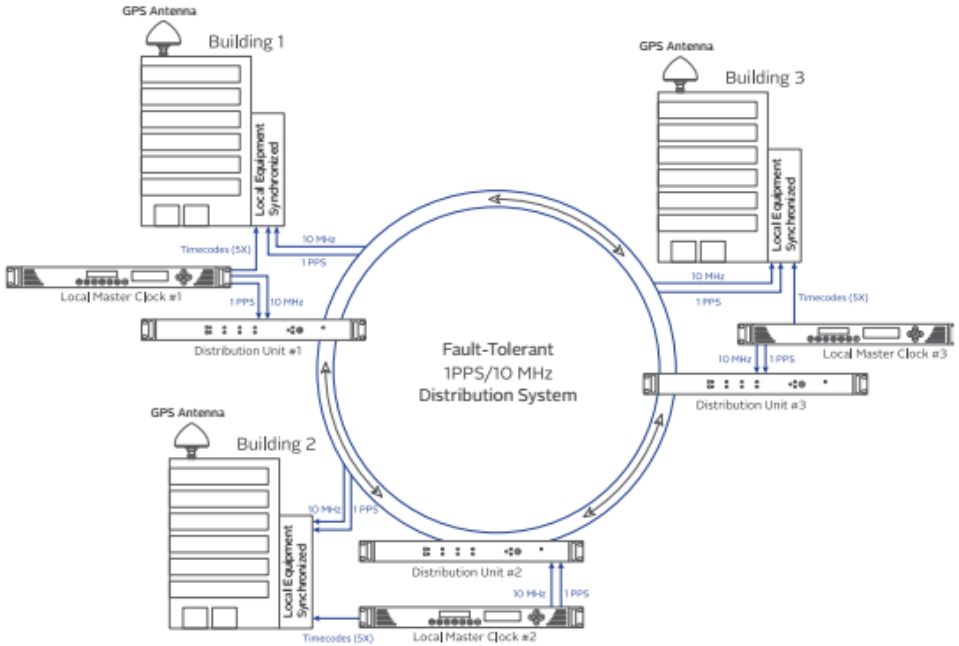
Case Study – Large broadcasting company in the world, including national TV channels with regional programming, national and local radio stations, and an extensive online content

- A much anticipated pay-per-view MMA fight broadcast got delayed
- Issue timing synchronization failed in the infrastructure.
- By the time the broadcast aired, the match ended.
- This resulted with upset customers requested their money back, users cancelling their subscription, which ultimately impacted revenue

DISTRIBTION RESILIENCY – NTP OVER ANYCAST

SOLUTION

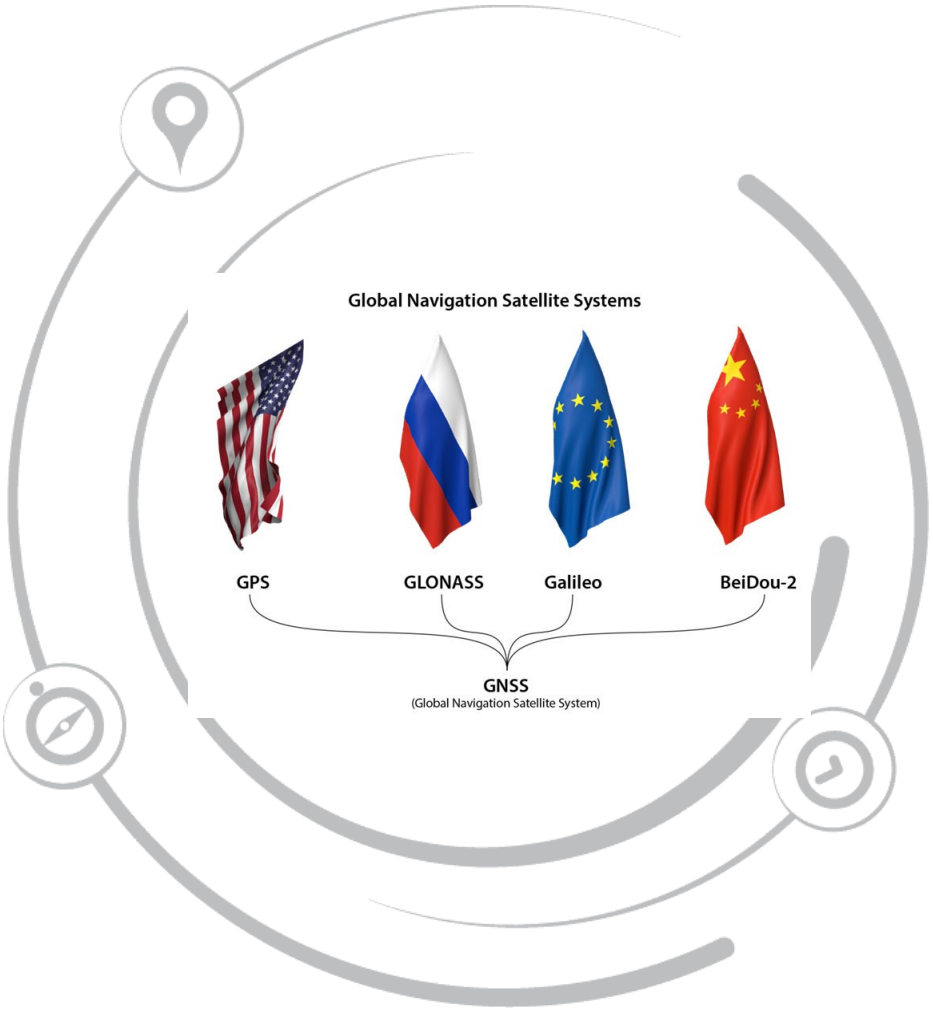




BEST PRACTICES FOR TIME RESILIENCY

REFERENCE

- Use Multiple GNSS Reference
  - GPS, GLONASS, Galileo, Beidou and other regional systems
- Diversify the time reference to multiple servers
  - time1.orolia.com (GPS)
  - time2.orolia.com (GNSS)
  - time3.orolia.com (STL)
- Diversify hardware vendor
- Define holdover budget and pick right quality of oscillator (internal clock)
  - Rb, Cesium, OCXO



BEST PRACTICES FOR TIME RESILIENCY

DISTRIBUTION

- Scope for resiliency extends to the underlying network infrastructure
- Resiliency can be base on underlying network topology and infrastructure
  - SONET, MPLS, Ethernet
  - DC, Campus, Service Provider
- Time traffic [source <-> destination]
  - Low latency switching and Symmetric network path
  - Traffic Engineering, MPLS-TE, VLAN/VXLAN, direct cables etc.
  - Isolate time traffic form the rest – Treat similar to OOB.
- Dedicated hardware for time distributions
  - Time budget (acceptable offset from UTC) nano vs micro vs mili
  - Speed, Bandwidth, Capacity
  - Often used – Network Switches/Routers, NIX Systems, Active Directory

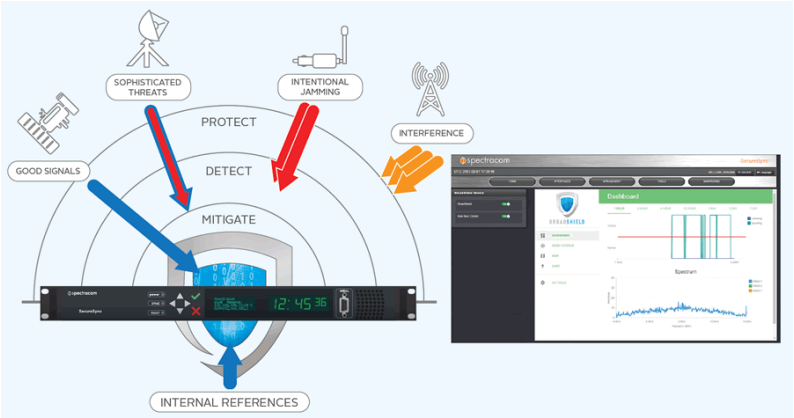
BEST PRACTICES FOR TIME RESILIENCY

CLIENT SYSTEMS

- Multiple time servers
  - NTP Client (at least 3)
- Follow industry best practices for client system redundancy
  - Dual switch uplink
  - Multiple Gateways
  - Path Redundancy

MONITORING

- More than 1 method for monitoring
  - SNMP, Syslog, RestAPI and so on
- Different Requirements
- FINRA/MIFID2
  - Legally you are require to monitor
  - Store logs
  - Time offset accuracy
- PCI or something else



TIME AND LOCATION YOU CAN TRUST™

QUESTIONS ?