Characterization of GNSS Threats
(making the invisible utility… visible)

Greg Wolff
- Office: (303) 539-4904
- Email: greg.wolff@microchip.com

Overview

- Threats to GNSS and our Critical Infrastructure
- Applying a secure firewall approach to protect against GNSS threats
- Visibility of GNSS threats
- Summary

The Biggest Insider Threat: GNSS Receivers

- **Insider threats aren't always people, they can be "things" as well**
  - Chelsea Manning (2010): Leaked ~750,000 documents to WikiLeaks
  - Edward Snowden (2013): Leaked information on global surveillance programs run by the NSA
  - Stuxnet (2010): Infected PLC devices were used in and ultimately destroyed Iranian centrifuges

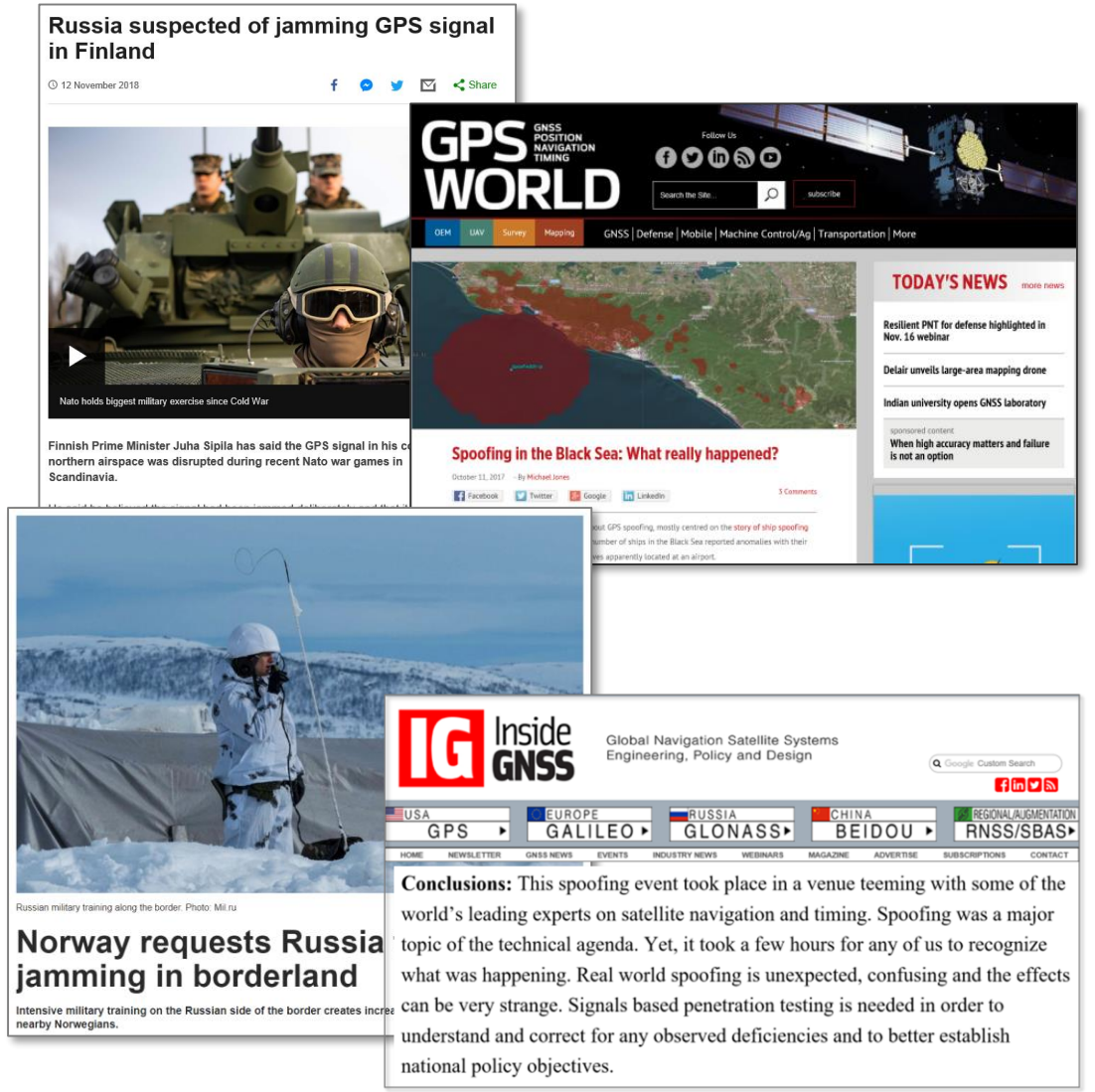
- **GNSS receivers have become trusted insiders**
  - The Positioning, Navigation, and Timing (PNT) solution provided by GPS is "blindly" trusted by many systems
  - GNSS receivers are essential to 11 of the 18 Critical Infrastructure and Key Resource (CIKR) sectors

Industry must "open its eyes" to the potential impact of GNSS attacks and actively participate in the defense of the services they provide

GNSS Enables our Critical Infrastructure

- **Positioning, Navigation, and Timing (PNT) is not identified as a Critical Infrastructure and Key Resource (CIKR) sector but a majority of CIKR sectors depend upon it**
  - In the case of GPS, there is no obligation for continued availability or performance of the GPS system
  - The occurrences of PNT disruption are increasingly frequent and occur globally

- **Continued availability of PNT service is in the economic and strategic interests of everyone**
  - Enables other services to continue to add more value and at a lower cost point (good use of taxpayer dollars)

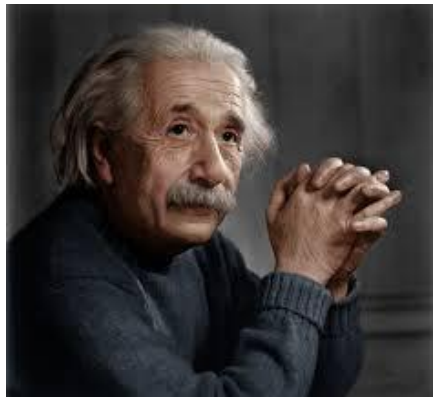


Signal-in-Space Threat

- **Signal in space threats are generally categorized based on the failure mode they induce in a GNSS receiver**
  - **Jamming**: Partial or complete loss of ability to receive GNSS signals
  - **Spoofing**: Tricking a GNSS receiver into receiving illegitimate signals

- **Multi GNSS systems are available for use but they provide minimal protection against signal-in-space threats**
  - Use of multi-constellation can help in detecting errors in the space and ground segments of GNSS but these errors are few and far between
  - GNSS constellations are relatively close in frequency so jamming events often impact all the constellations
  - It is only slightly more difficult to spoof multiple GNSS systems than it is to spoof a single GNSS system

System	GPS	GLONASS	BeiDou	Galileo	IRNSS
Owner	United States	Russian Federation	China	European Union	India
Coding	CDMA	FDMA	CDMA	CDMA	CDMA
Number of satellites	31 (at least 24 by design)[8]	28 (at least 24 by design) including:[9] 24 operational 2 under check by the satellite prime contractor 2 in flight tests phase	5 geostationary orbit (GEO) satellites, 30 medium Earth orbit (MEO) satellites	8 test bed satellites in orbit, 22 operational satellites budgeted	3 geostationary orbit (GEO) satellites, 4 geosynchronous orbit satellites
Frequency	1.57542 GHz (L1 signal) 1.2276 GHz (L2 signal)	Around 1.602 GHz (SP) Around 1.246 GHz (SP)	1.561098 GHz (B 1) 1.589742 GHz (B 1-2) 1.20714 GHz (B2) 1.26852 GHz (B3)	1.164–1.215 GHz (E5a and E5b) 1.260–1.300 GHz (E6) 1.559–1.592 GHz (E2-L1-E11)	1.17645 GHz (L5) 2.492028 GHz (S1)
Status	Operational	Operational	15 satellites operational, 20 additional satellites planned	In preparation	4 satellites launched, 3 additional satellites planned to be launched by Early 2016



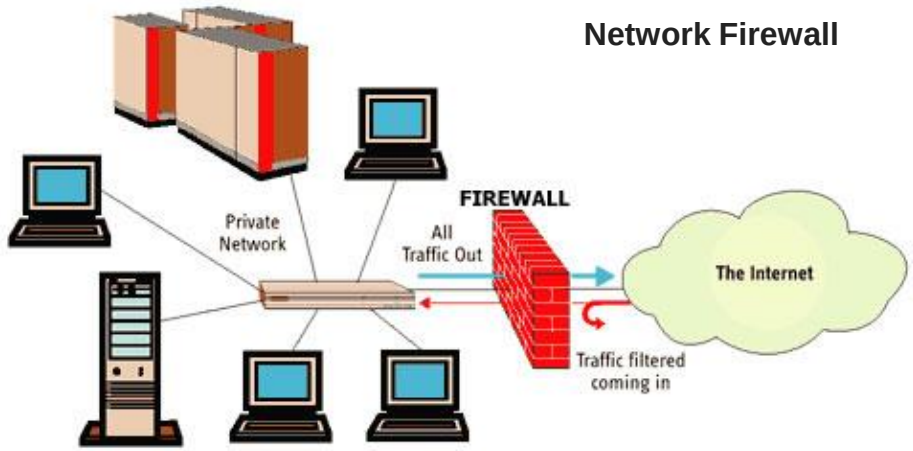
We cannot solve our problems with the same thinking that we used when we created them.

- Albert Einstein

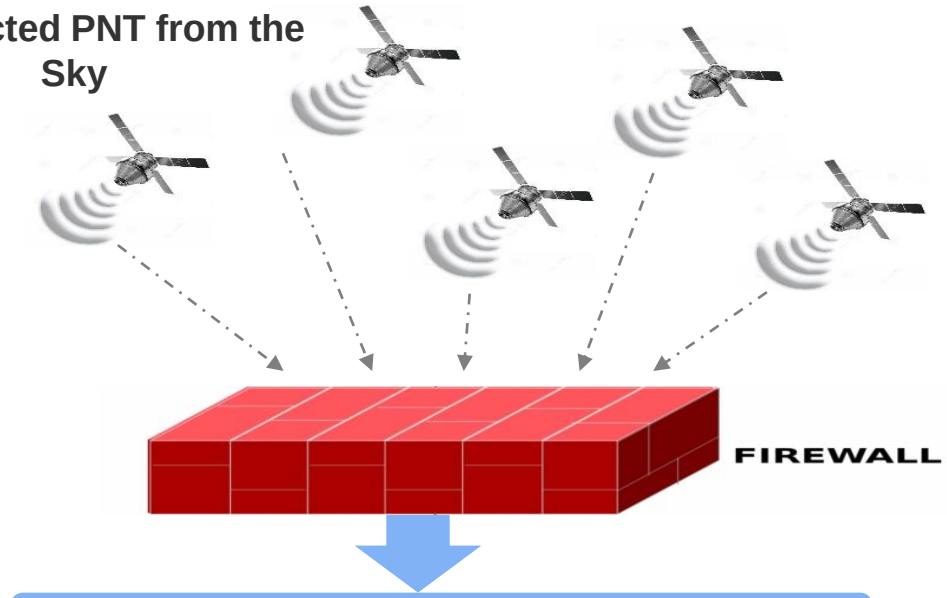
Firewall security for signals in space

Physical Firewall at Electrical Substation

Network Firewall



Unprotected PNT from the Sky



Secure PNT for Critical Infrastructure

GNSS Firewall: Verifying the Integrity of GNSS Signals

- **There are large deployments of GNSS receivers within our critical infrastructure that do little to verify the integrity of GNSS signals**
- **GNSS firewall protects GNSS receivers that would otherwise be vulnerable**
  - Uses multiple detectors to identify waveform, data, and solution anomalies in the GNSS signal
- **GNSS firewall assumes that threats will evolve over time**
  - Detector algorithms are updated analogously to virus scanning software

GNSS Anomalies

Power received on Earth from a satellite, -160 dBm,
This is as “bright” as a flashlight in Los Angeles when viewed in New York City, approx. 5000 km away

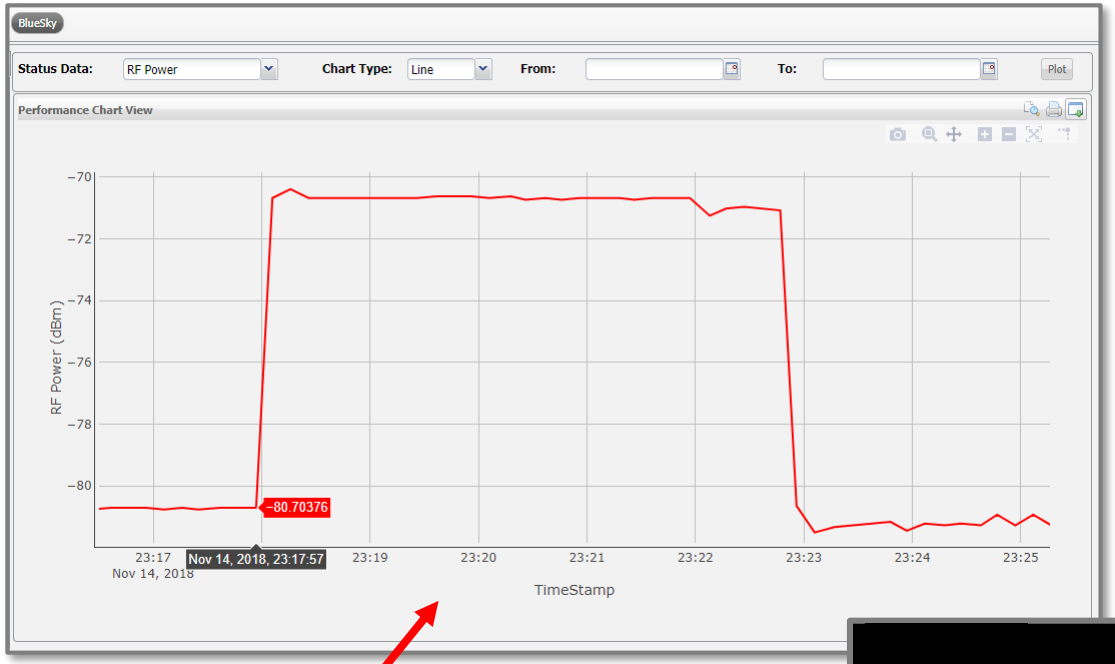
Satellites powered by solar panels and there are 12,000 miles between satellites and receiver

1. Satellite Error
2. Environmental Effects
3. Weather Anomolies
4. Multipath Interference
5. Jamming
6. Spoofing
7. Cyber Attack

Sample of GNSS metrics

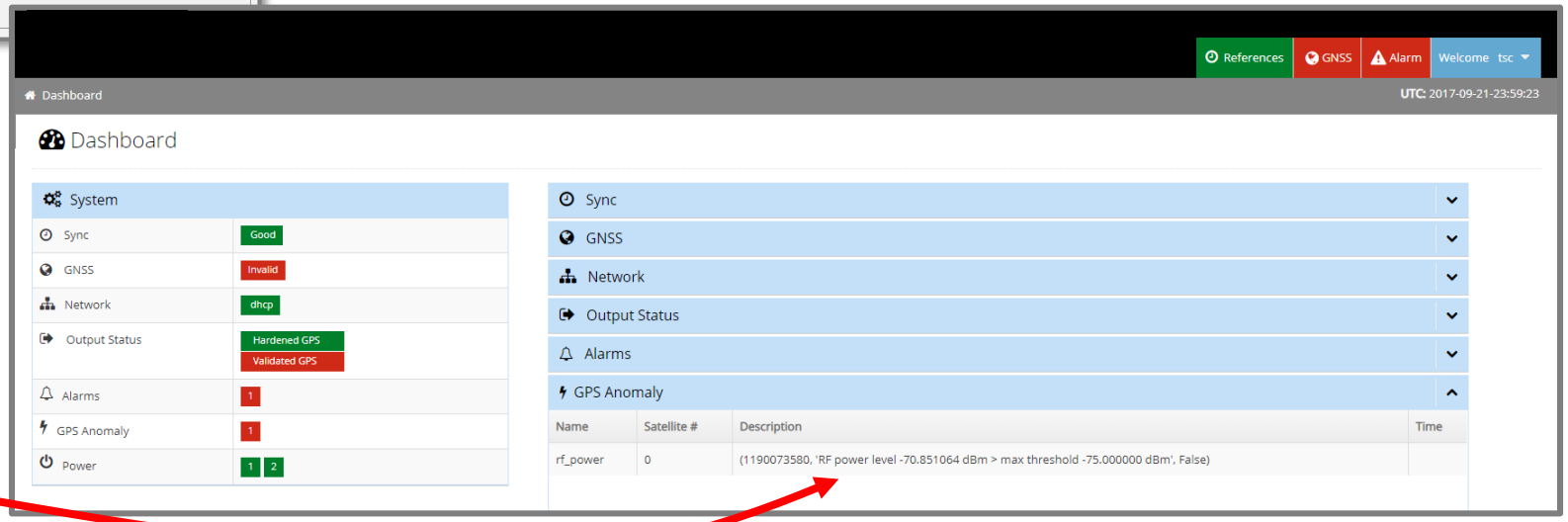
Metric	Characteristic of Signal Anomaly
Tracked Satellite Count	Are the expected number of satellites in view?
GPS Position Delta	Is the position data coming from the sky moving too much relative to surveyed antenna position?
Phase Time Deviation	Is the sky received “time” moving? (suddenly, gradually, etc?)
GPS Signal Average	Is the GNSS signal strength of the visible satellites in the expected range?
RF Power	Is the RF power level within expected threshold?

RF Power Detection

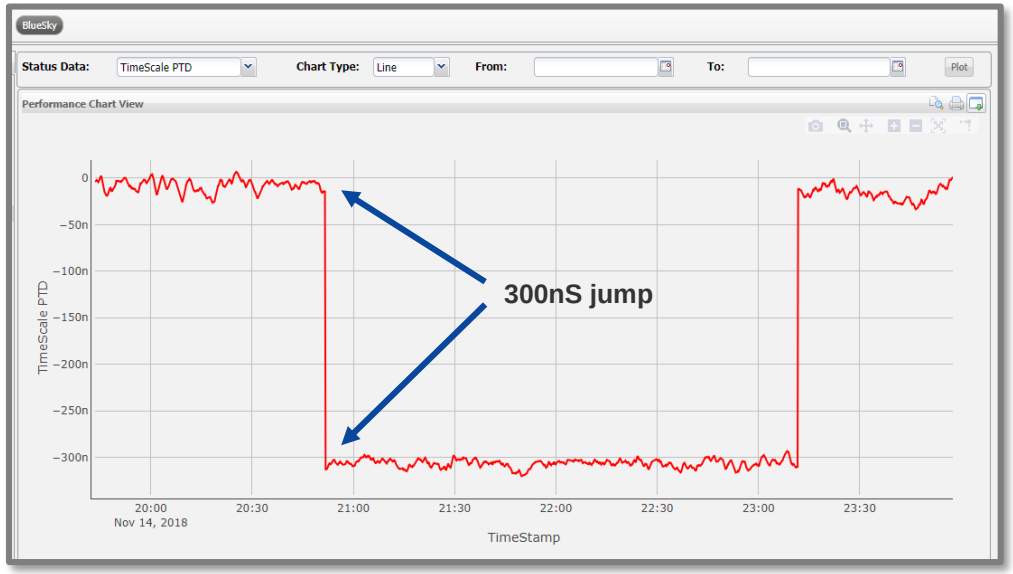


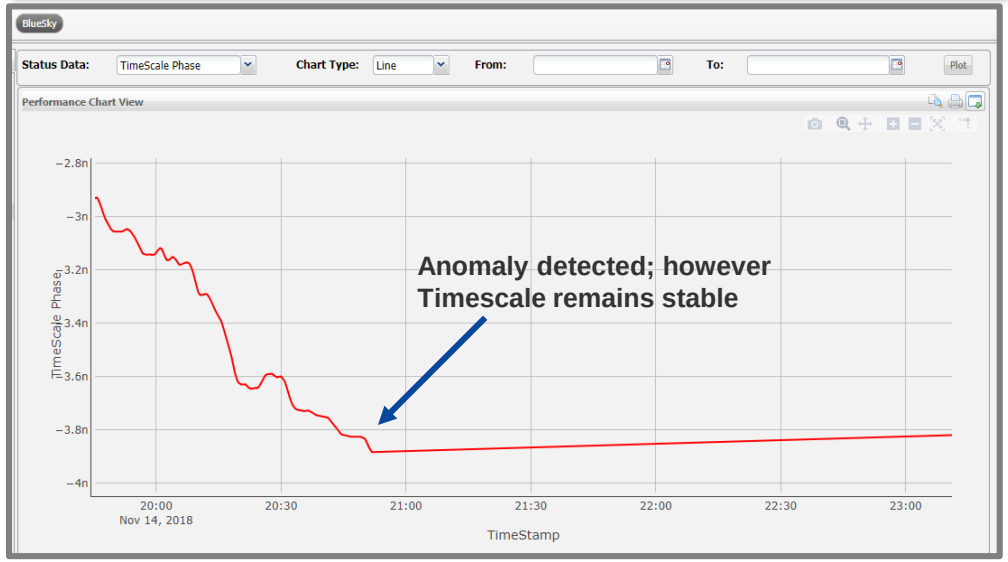
- GPS RF Power level operates at a very low signal level
- Typically, when connected to antenna, signal is in the 60db to 90db range
- Small power shifts, just enough to take over the reception of the receiver

- Time based performance monitoring shows characteristics of knock-off signal
- Dashboard views are also convenient for seeing alarm condition

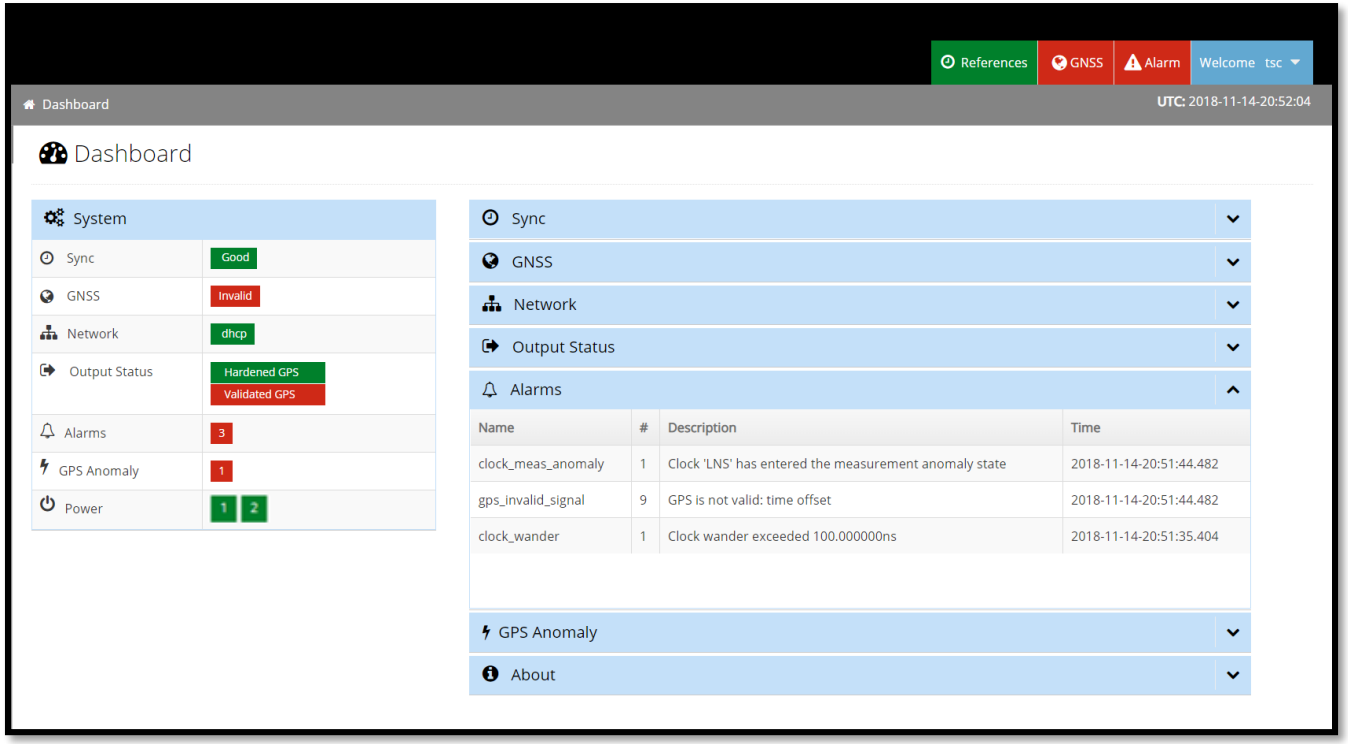


Time Jump Anomaly





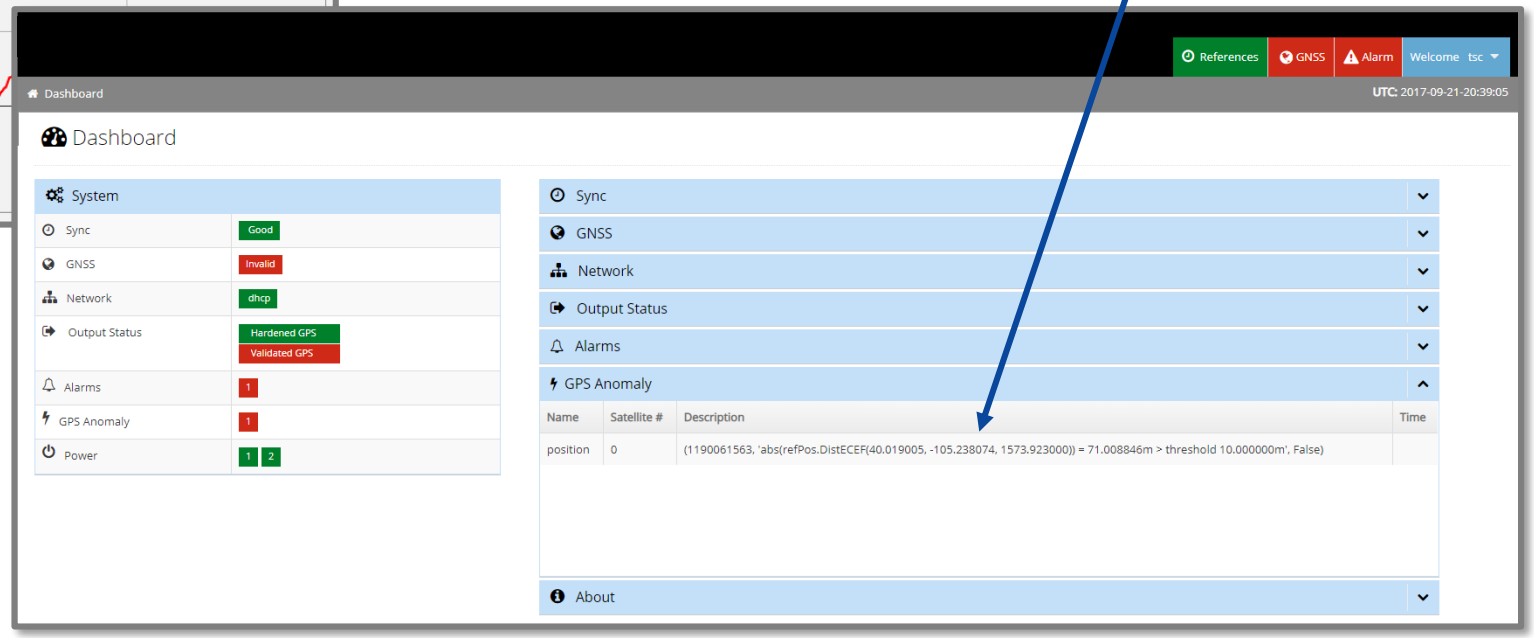
- Timing anomalies can be both sudden jumps in time or more gradual time shifts
- Autonomous timescale algorithms are used to detect time offsets (sudden, gradual, etc.)
- When detected, GPS synthesizer technology driven by the timescale, can maintain operation



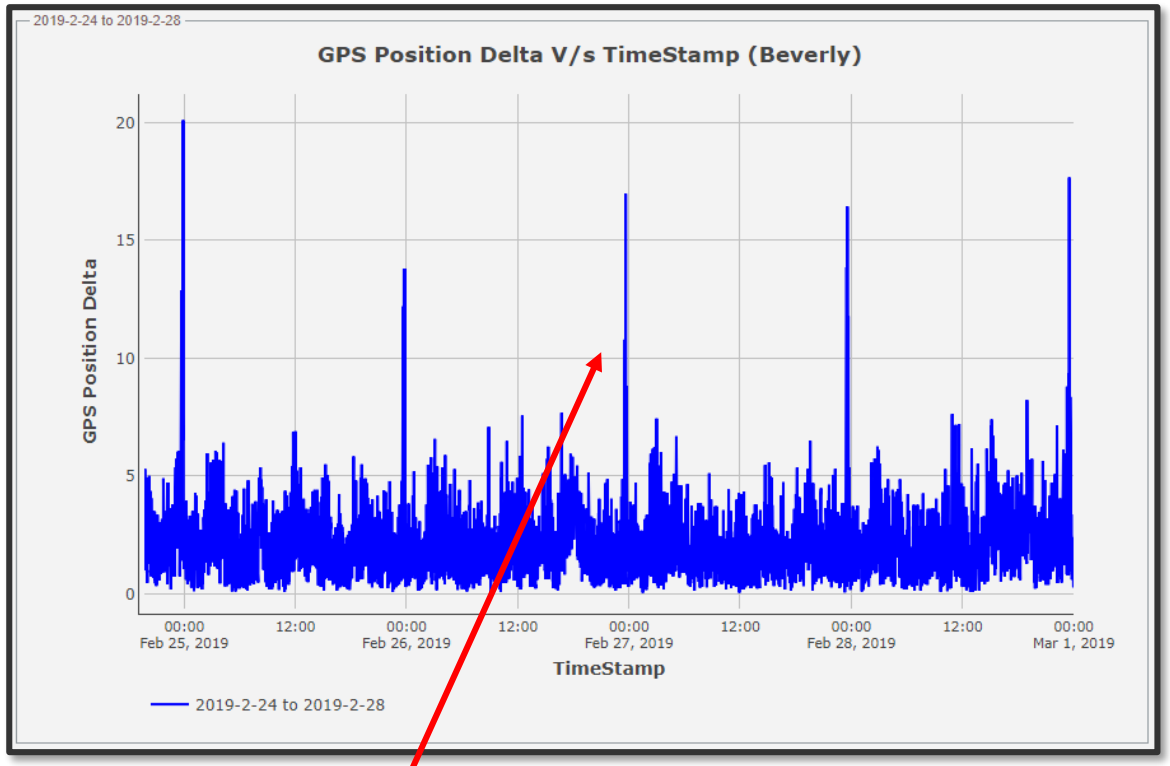
Position Movement Anomaly

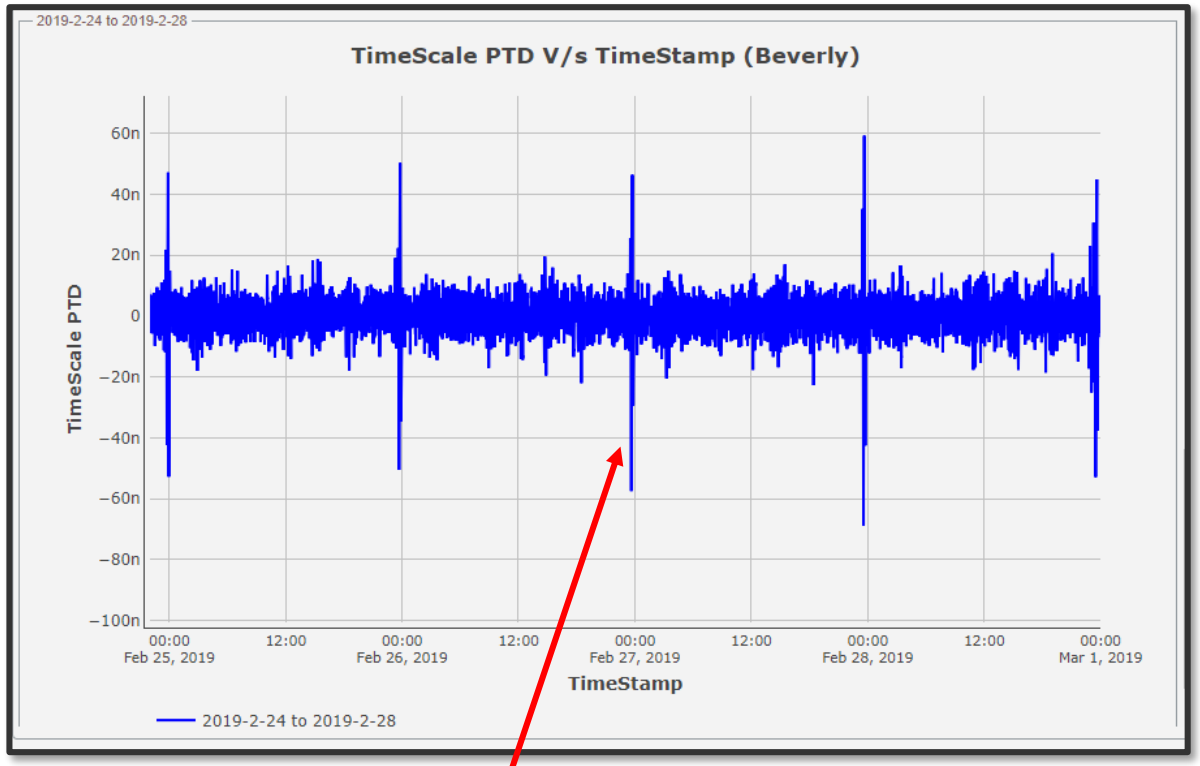
- Anomaly position detector can be set to the desired threshold, for example 10 meters
- Once threshold is crossed, alarm is generated

- Time based performance monitoring provides plot of position movements



Observing multiple anomaly types to detect root cause





Position movement occurring daily

GPS phase movement occurring at same time

Visibility: Reporting GNSS Anomalies

- **Critical Infrastructure providers need to recognize the threat**
  - Many read the news, but have not felt the pain
  - Visibility is a smart first step towards proactively securing GNSS reception… rather than waiting for disaster to strike

- **Ability to quickly recover from anomalous GNSS events is greatly aided by real-time diagnostics and reporting**
  - Most users don't actively monitor the health of GNSS…the "set it and forget it" culture needs to be changed
  - Knowing is half the battle: Situational awareness reduces time spent identifying and localizing the issue

Thank you!

Microsemi, a wholly owned subsidiary of Microchip Technology Inc. (Nasdaq: MCHP), offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions, security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Learn more at www.microsemi.com.

Microsemi Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
email: sales.support@microsemi.com
www.microsemi.com