

Welcome to Tech Tuesday

Presented by **Microchip**, Frequency and Time Systems

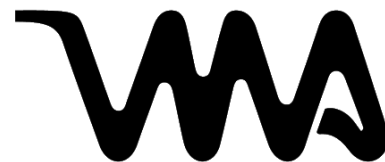
Moderated By:



Ryan Christian

480-577-7172

ryanc@vicmyers.com



VIC MYERS ASSOCIATES

Presented By:



Greg Wolff

303-956-9388

Greg.Wolff@microchip.com



MICROCHIP

Frequency and Time Systems

GPS resiliency using a GNSS Firewall



A Leading Provider of Smart, Connected and Secure Embedded Control Solutions



SMART | CONNECTED | SECURE

Agenda

- **Update on PNT (Position, Navigation and Time) industry initiatives and trends for Critical Infrastructure**
- **BlueSky GNSS Firewall Product Overview**
- **Monitoring GNSS Observables**
 - BlueSky Information Charts
 - BlueSky Performance Monitoring
- **Summary**

Spoofing and Jamming in Norwegian Sea



Russian military training along the border. Photo: Mil.ru

Norway requests Russia to halt GPS jamming in borderland

Intensive military training on the Russian side of the border creates increasing communications troubles for nearby Norwegians.



GPS disruptions in recent NATO war games

Russia suspected of jamming GPS signal in Finland

© 12 November 2018

f t Share



Nato holds biggest military exercise since Cold War

Finnish Prime Minister Juha Sipila has said the GPS signal in his country's northern airspace was disrupted during recent Nato war games in Scandinavia.

He said he believed the signal had been jammed deliberately and that it was possible Russia was to blame because it had the means to do so.

Finland is not a Nato member but joined the war games which began last month.

Norway also reported GPS problems during the exercises near Russia's north-western borders.

How serious was the disruption?

The Finnish region of Lapland and northern parts of Norway close to the Russian border were affected, with the Norwegian regional airline Widerøe confirming its pilots had experienced GPS disruption, Germany's DW news site reports.

However, the airline pointed out that pilots aboard civilian aircraft had other options when a GPS signal failed.

"This is not a joke, it threatened the air security of ordinary people," said Mr Sipila, who is himself an experienced pilot.

"It is possible that Russia has been the disrupting party in this. Russia is known to possess such capabilities."

Presidential Executive Order

IG Inside GNSS Global Navigation Satellite Systems Engineering, Policy, and Design

GPS Galileo GLONASS

Home Applications Columnists Insider Subscribe Become an Advertiser

Washington View: Progress Logged on Strengthening and Backing Up PNT

April 2, 2020 By Dee Ann Davis

After years of delay, we see movement toward a back-up service for PNT and ensuring that critical infrastructure owners and operators take steps to limit vulnerabilities.

<https://insidegnss.com/progress-logged-on-strengthening-and-backing-up-pnt/>

Microchip technology inc. 157,068 followers

We are positioned to support the Executive Order with the new BlueSky™ GNSS Firewall. The BlueSky GNSS Firewall protects already deployed GPS systems by providing a cost-effective overlay solution installed between existing GNSS receivers and antennas.

BlueSky™ GNSS Firewall Meets the Presidential Executive Order For Responsible Use of PNT Services

Like Comment Share

Microchip Solution

ECONOMY NATIONAL SECURITY BUDGET IMMIGRATION CORONAVIRUS.GOV

EXECUTIVE ORDERS

Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services

INFRASTRUCTURE & TECHNOLOGY Issued on: February 12, 2020

<https://www.whitehouse.gov/presidential-actions/executive-order-strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/>

Official website of the Department of Homeland Security

Homeland Security

News In Focus How Do It? Get Involved About DHS

DHS Statement on the President's Executive Order to Strengthen National Resilience through Responsible Use of Positioning, Navigation & Timing

Release Date: February 12, 2020

<https://www.dhs.gov/news/2020/02/12/dhs-statement-president-s-executive-order-strengthen-national-resilience-through>

Cybersecurity and Infrastructure Security Agency



The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to defend critical infrastructure against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow.

**CISA is part of
Department of Homeland Security (DHS)**

NATIONAL CRITICAL FUNCTIONS

AN EVOLVED LENS FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Over the past six months, the Cybersecurity and Infrastructure Security Agency (CISA) has engaged in a far-reaching effort in partnership with the Sector Coordinating Councils, the SLTT Government Coordinating Council, and associated Sector Specific Agencies, as well as other partners to identify and validate a set of National Critical Functions.

National Critical Functions are defined as:

The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

National Critical Functions Set			
CONNECT	DISTRIBUTE	MANAGE	SUPPLY
<ul style="list-style-type: none"> Operate Core Network Provide Cable Access Network Services Provide Internet Based Content, Information, and Communication Services Provide Internet Routing, Access, and Connection Services Provide Positioning, Navigation, and Timing Services Provide Radio Broadcast Access Network Services Provide Satellite Access Network Services Provide Wireless Access Network Services Provide Wireline Access Network Services 	<ul style="list-style-type: none"> Distribute Electricity Maintain Supply Chains Transport Passengers Transport Passengers Transport Passengers Transport Passengers Transport Materials by Pipeline Transport Passengers by Mass Transit 	<ul style="list-style-type: none"> Conduct Elections Develop and Maintain Perform Cyber Incident Management Capabilities Prepare for and Manage Emergencies Preserve Constitutional Rights Protect Sensitive Information Provide and Maintain Infrastructure Provide Capital Markets and Investment Activities Provide Consumer and Commercial Banking Services 	<ul style="list-style-type: none"> Exploration and Extraction Of Fuels Produce Chemicals Provide Metals and Materials Provide Housing Provide Information Technology Products and Services Provide Materiel and Operational Support to Defense Research and Development Supply Water

Position, Navigation, and Timing Services is a “Critical Function”

Why should you be concerned?

Until recently, GPS devices were viewed simply as radio receivers. However, they are actually computers with similar security risks. Threats include denial-of-service attacks (jamming) and the introduction of bad data into the system (spoofing). The advent of software-defined radios has increased the ease and lowered the cost with which these types of attacks can be launched. Efforts should be made to ensure accurate and resilient timing for your GPS device.



TIME – THE INVISIBLE UTILITY



UNCLASSIFIED

Recent and Upcoming DHS PNT

- Information Sheets “Are you Managing your Time?”
- Development of best practices for testing your timing architecture
- Conformance Standards**
- Multi-GNSS vulnerabilities and opportunities
- Support to National Defense Authorization Acts
 - FY 17
 - FY 18
- Support to Department of Transportation for the National Timing Security and Resilience Act
- Update Best Practices

TIME – THE INVISIBLE UTILITY

WHY IS TIME IMPORTANT?

SECTORS AND INDUSTRIES DEPENDENT ON TIME

Transportation	Health	Energy	Finance	Security	IT
Aviation	Medical	Electricity	Banking	Law Enforcement	Cloud Services
Maritime	Pharmaceuticals	Nuclear	Insurance	Regulatory	Mobile
Automotive	Biotechnology	Oil & Gas	Real Estate	Telecommunications	IoT
Space	Healthcare	Power Generation	Commodities	Government	Smart Devices
Manufacturing	Pharmaceuticals	Water	Investment	Defense	Wearable
Supply Chain	Pharmaceuticals	Smart Grid	Commodities	Government	Smart Home

WHY SHOULD YOU BE CONCERNED ABOUT TIME NOW?

WHAT CAN YOU DO TO UNDERSTAND AND IMPROVE YOUR "TIME HYGIENE"?

https://www.us-cert.gov/sites/default/files/documents/Technical-Level_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf

https://www.us-cert.gov/sites/default/files/documents/Corporate_Leadership_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf

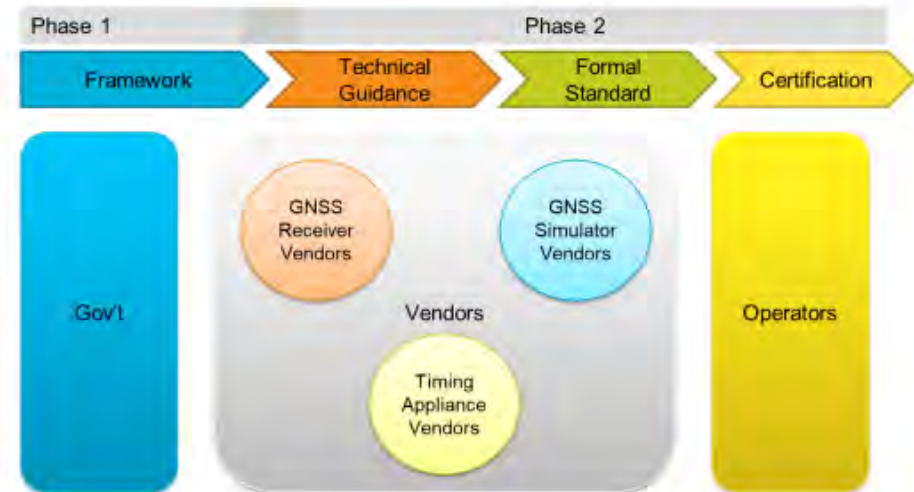
Resilient PNT Conformance Working Group

Introduction:

The Resilient PNT Conformance Framework Working Group (CFWG) is established by the Department of Homeland Security to ensure resilient GNSS-derived timing sources for critical infrastructure.

Objectives:

- Develop an integrated conformance framework for describing resilient PNT systems
- Create meaningful, actionable, and verifiable guidelines for ensuring resilient PNT with a focusing on GNSS dependent timing devices
- Transition to industry application and industry-supported body for adoption and sustainment
- Enable improved risk management and decision making by CI operators when acquiring PNT equipment
- Enable vendors to differentiate products



GNSS – Global Navigation Satellite System

HSSEDI is a trademark of the U.S. Department of Homeland Security (DHS).
The HSSEDI FFRDC is managed and operated by The MITRE Corporation for DHS.

Approved for public release; Distribution unlimited.

Case Number 19-0934 / DHS Reference Number 17-J-00100-05 9/16/19

©2019 The MITRE Corporation. All rights reserved.

HSSEDI
Homeland Security Systems Engineering & Development Institute™

BlueSky GNSS Firewall

Product Overview

Current GPS Receivers

- **Civilian GPS receiver**

- Commercial GPS receivers utilize L1 signal for tracking
- Varying levels of multi-constellation support and limited security features
- **Civilian GPS receivers make-up the majority of GPS receivers used by Critical Infrastructure**

- **Military GPS receiver**

- Selective Availability Anti-Spoofing Module (SAASM) receivers utilize L1 and the encrypted L2 signal for GPS tracking
- Provide better anti-jam performance and better protection against more advanced GPS attacks
- **Not available for commercial applications**



Civilian GPS Receivers



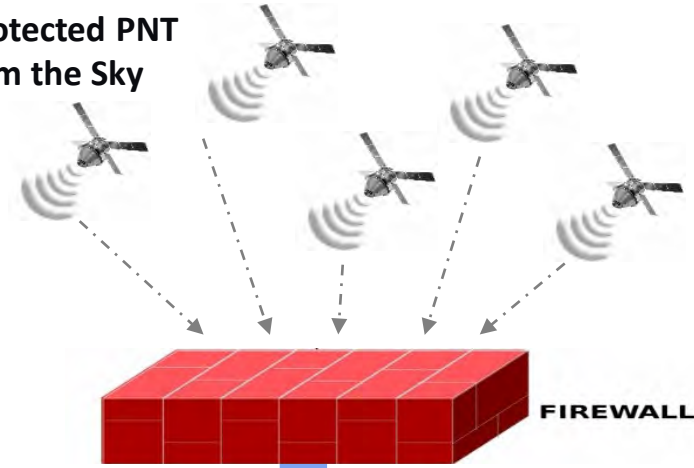
Military GPS Receiver

Firewall concept

Physical Firewall at Electrical Substation



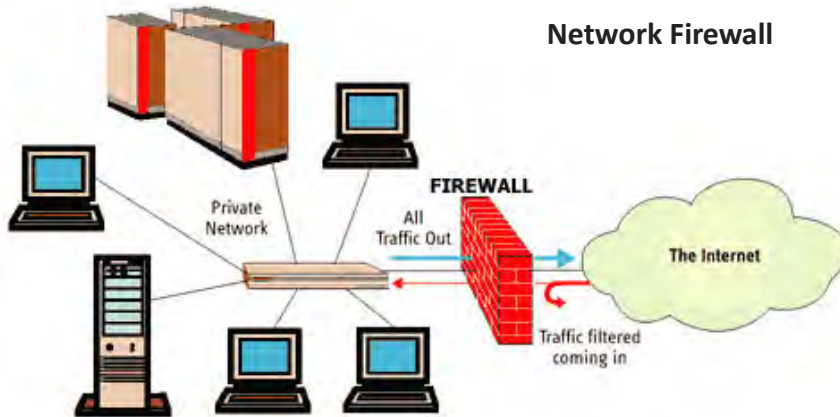
Unprotected PNT from the Sky



Secure PNT for Critical Infrastructure



Network Firewall

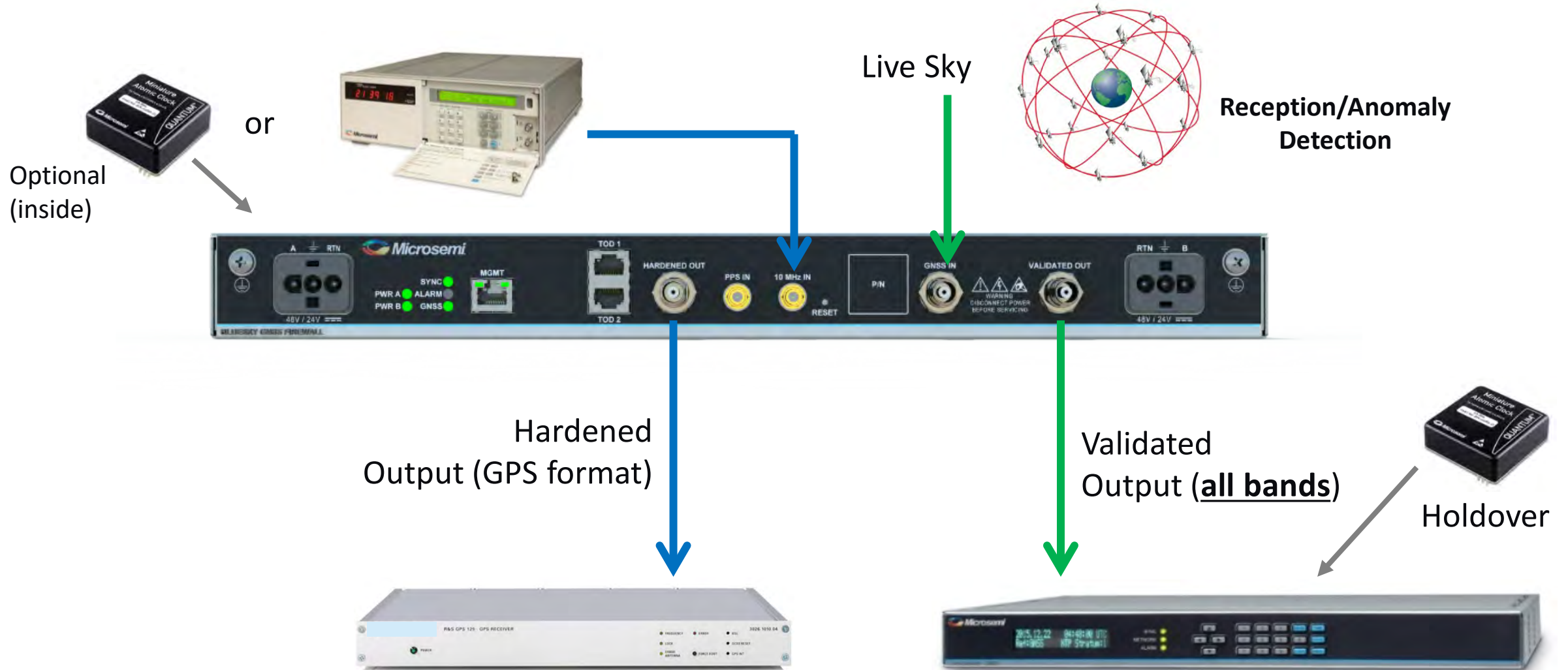


Secure Firewall Overlay

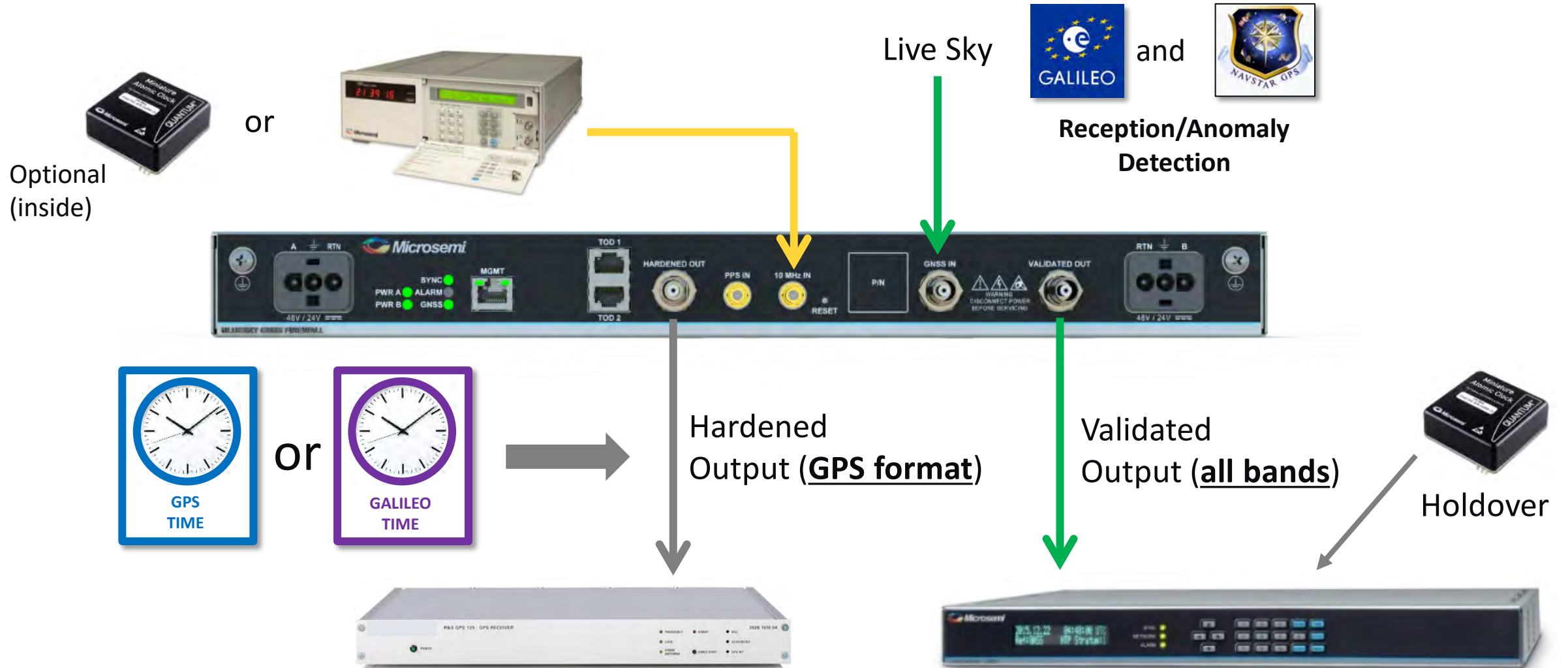


- **Protects against GNSS spoofing and jamming**
- **Simple connection between GNSS antenna and GPS system**
- **Optional internal MAC for holdover**
- **1PPS and 10 MHz timing reference inputs for extended holdover (connection to external cesium reference)**
- **Redundant AC or DC power options**
- **“BlueSky Performance Monitoring” integrated within TimePictra**

BlueSky GNSS Firewall (Hardened vs. Validated)

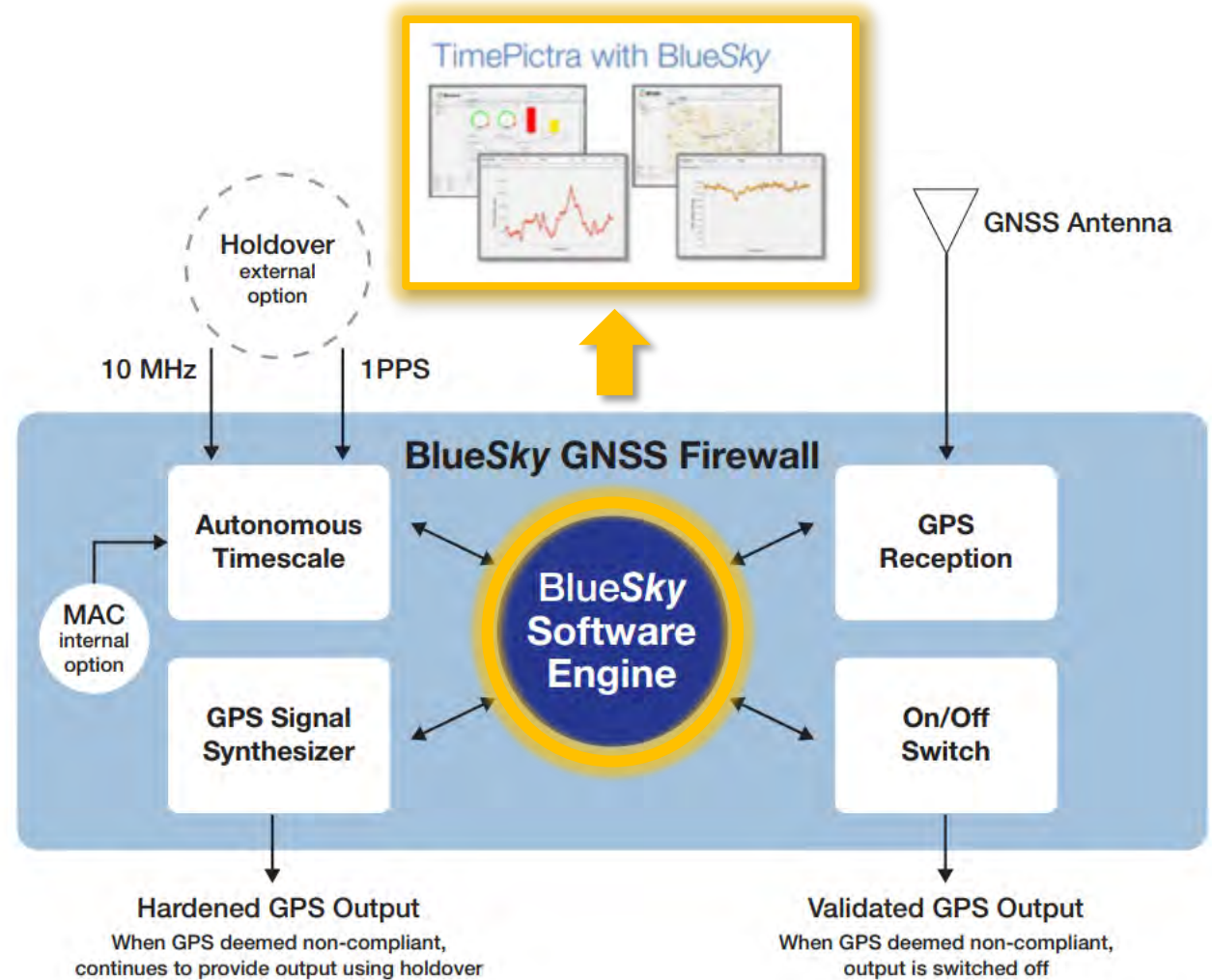


Support for Galileo



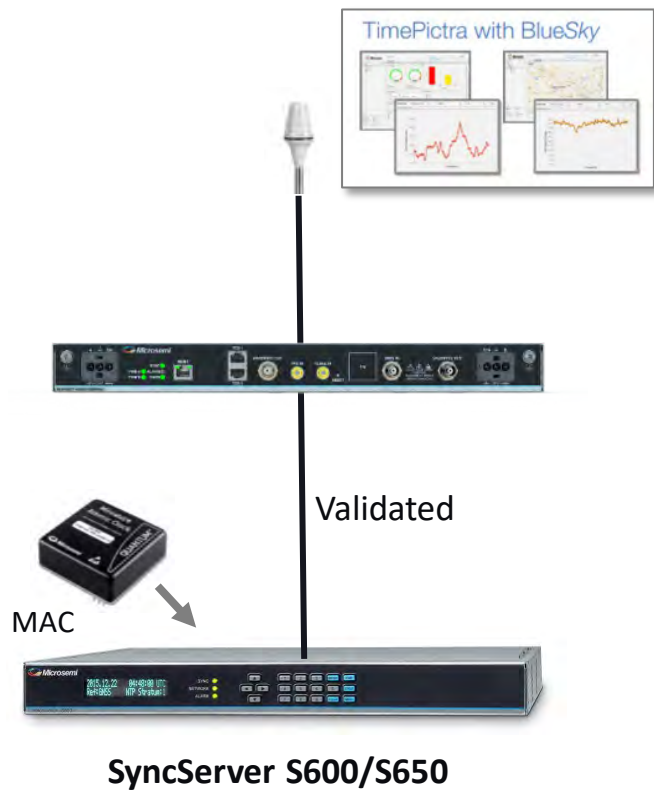
BlueSky Software

- **BlueSky software engine manages internal elements of the GNSS firewall**
 - Contains algorithms to aggregate and interpret the data from anomaly detectors
 - Makes informed decisions on the validity of Live Sky input and takes action to protect downstream GNSS systems
- **BlueSky Performance Monitoring (integrated as part of TimePictra)**
 - Enables management of multiple firewalls from a centralized location
 - Provides situational awareness of your entire GNSS infrastructure (BlueSky Performance Monitoring)

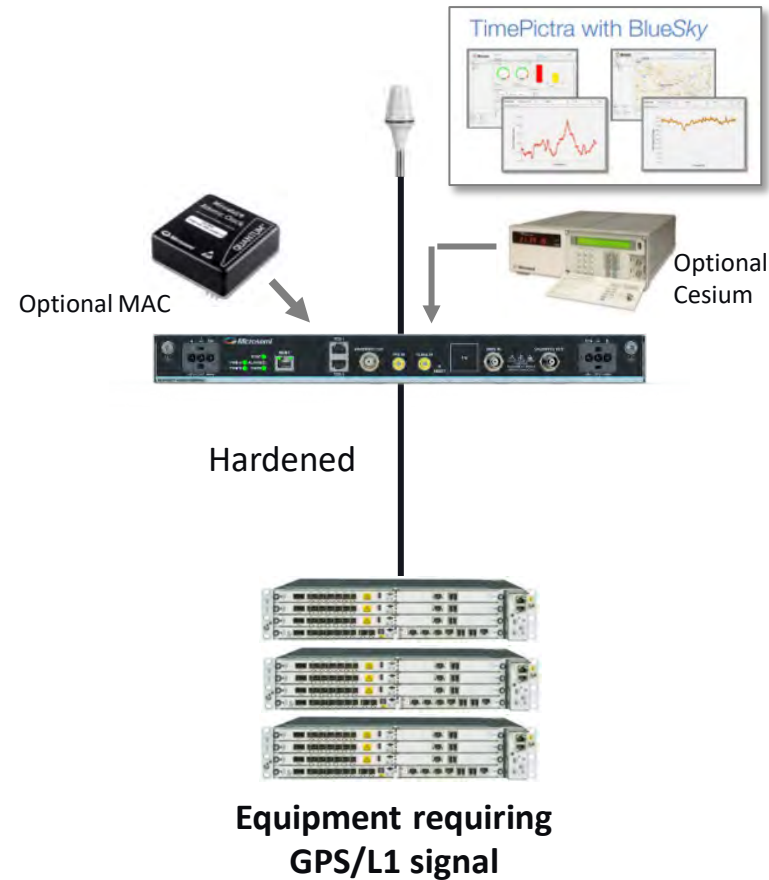


BlueSky GNSS Firewall Deployment models

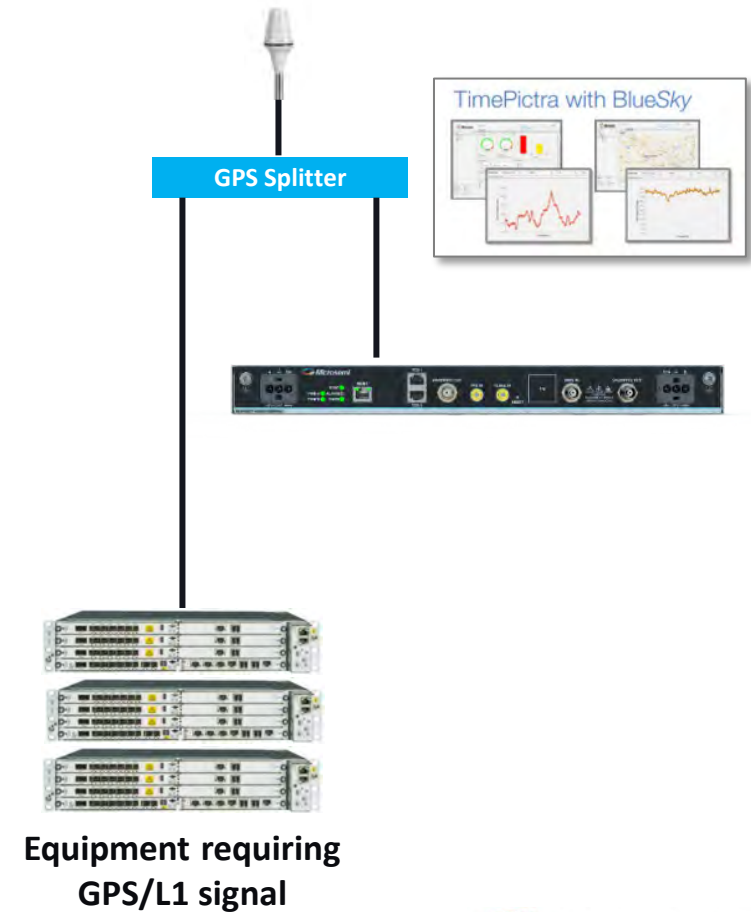
Firewall using Validated Output



Firewall using Hardened Output



Firewall deployed for monitoring only



Monitoring GNSS Observables

BlueSky Information Charts and
BlueSky Performance Monitoring

Causes of GNSS Anomalies

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

12,000 miles between satellites and receiver



Sample of GNSS observables

Metric	Characteristic of Signal Anomaly
Tracked Satellite Count	Are the expected number of satellites in view?
Position Dispersion	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?)
Carrier-to-Noise	Is the GNSS signal strength of the visible satellites in the expected range?
Satellites in view	Are individual satellites at the expected location?
RF Power	Is the RF power level within expected threshold?

QUESTION: HOW DO YOU KNOW IT WORKS?

ANSWER: GET-CI -> GPS Equipment Testing for Critical Infrastructure

- GET-CI is hosted by the U.S Department of Homeland Security (DHS) Science and Technology Directorate (S&T)
- Opportunity to evaluate equipment in unique live-sky signal environments that are only possible to create under controlled conditions authorized by the U.S. Government
- Purpose of event is to provide manufacturers of commercial GPS receivers used in critical infrastructure the opportunity to perform equipment evaluations in a rarely available live-sky spoofing environment.

Lab Testing versus Live-Sky Testing

Live Sky Testing

Lab Testing



VS

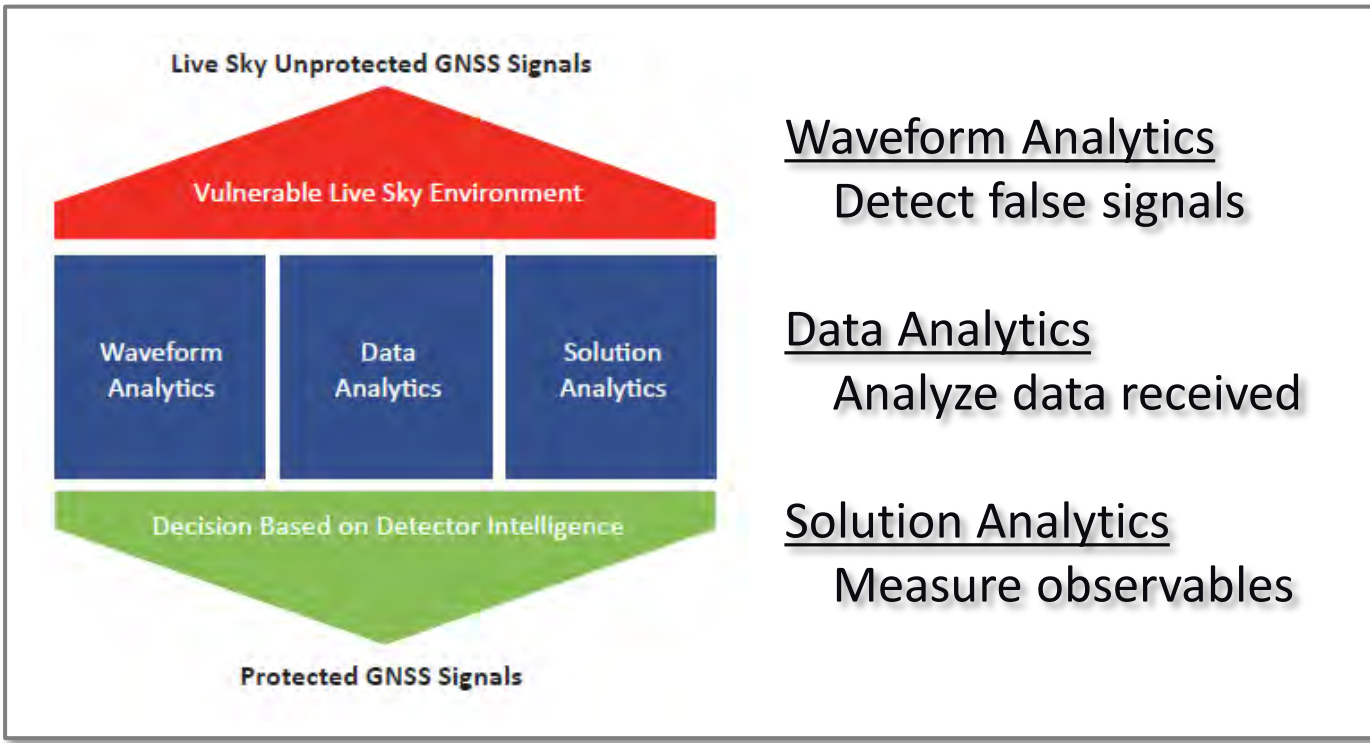


RF constellation simulator system



BlueSky GNSS Firewall Software Release 2.0

Improved Protection and Threshold Settings

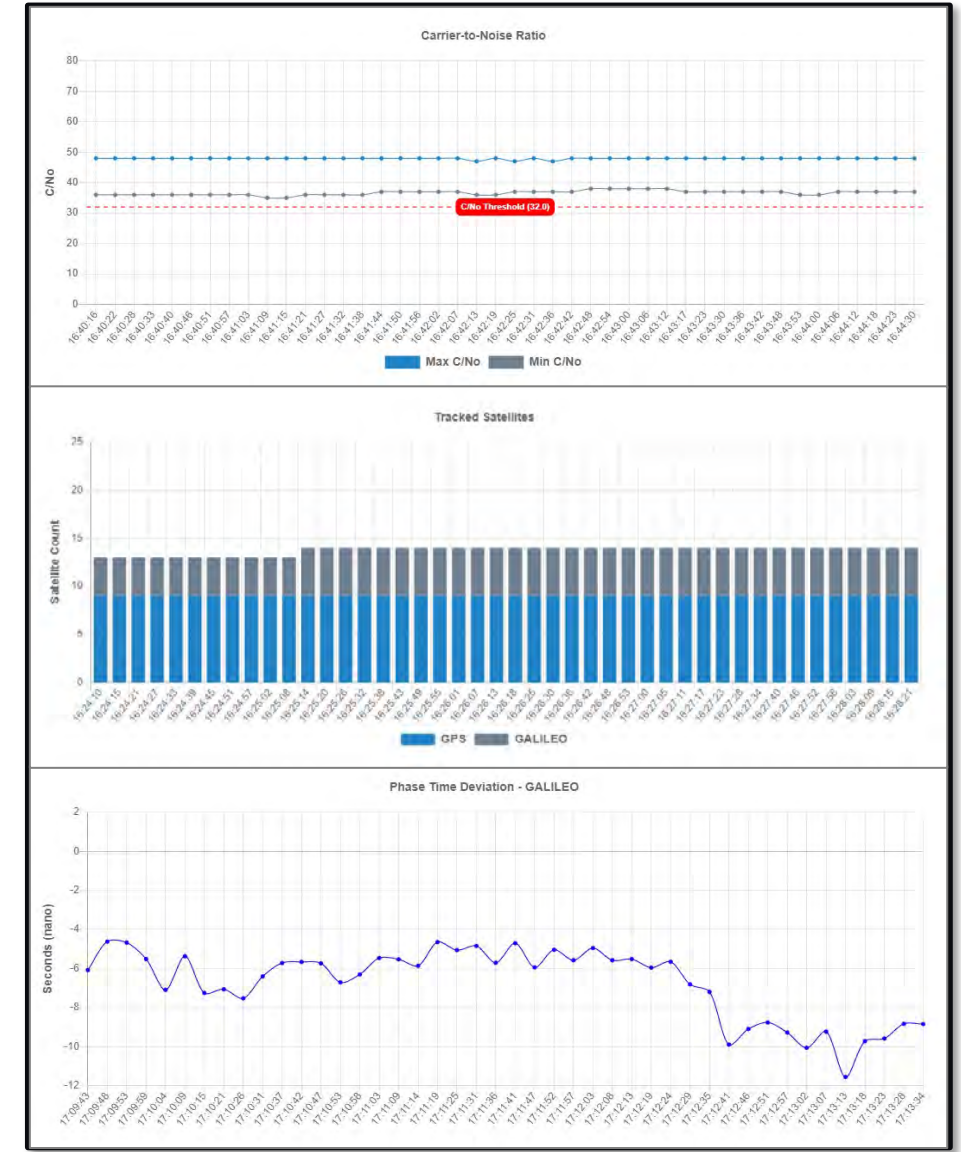


Waveform Analytics
Detect false signals

Data Analytics
Analyze data received

Solution Analytics
Measure observables

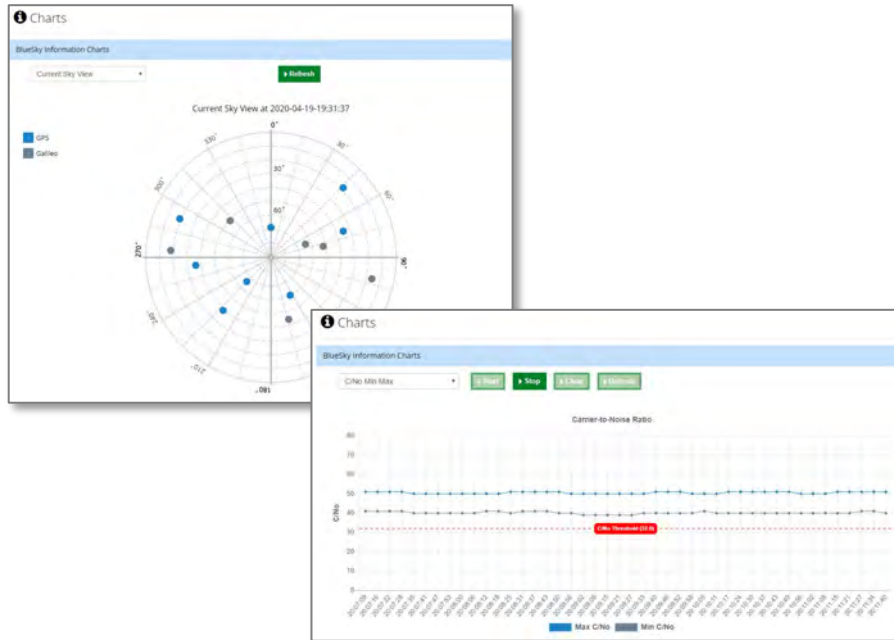
BlueSky Information Charts



BlueSky GNSS Firewall, Software Release 2.0.1



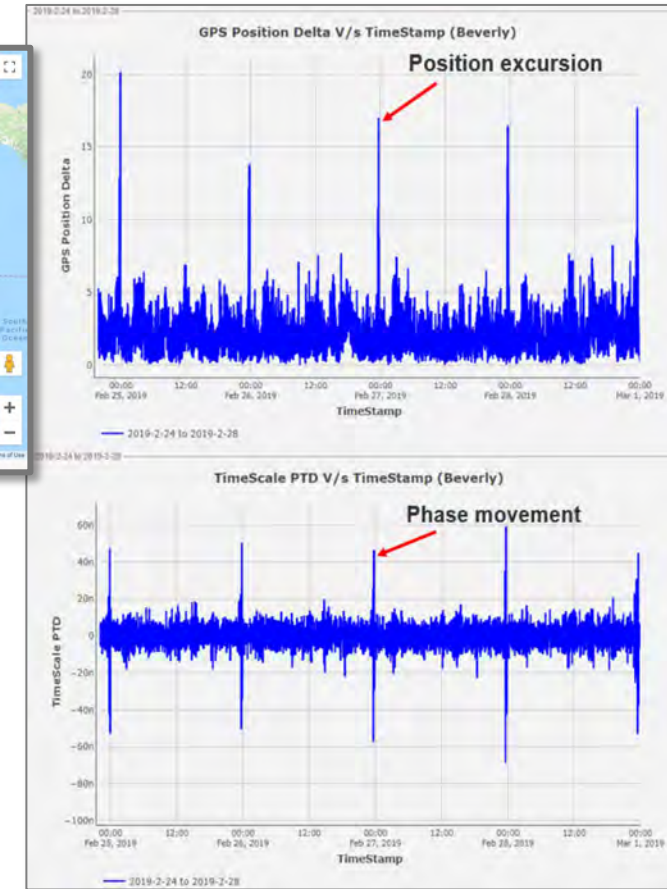
Local Charting



- Charting for quick view of GNSS metrics
- Enhanced threshold settings (CN/o, # of SV's configurable)
- Improved support for SNMP and Alarms

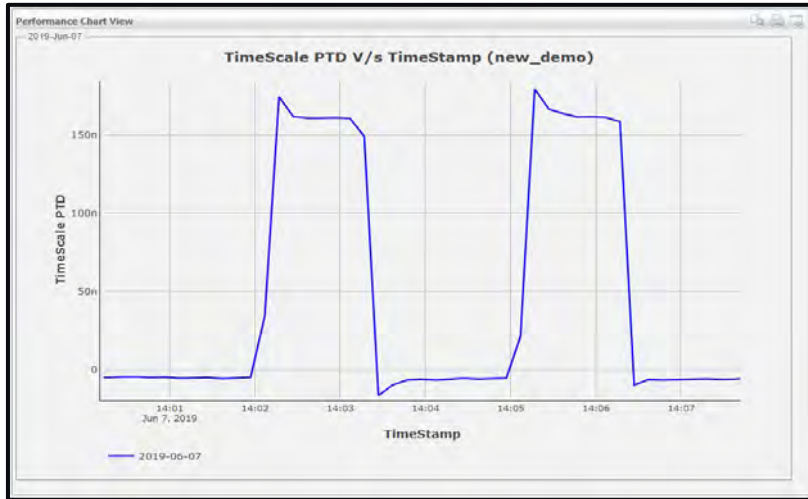


TimePictra with BlueSky Performance Monitoring



- Regional/global deployment view
- Multi-element mgmt. & alarms
- Compare multiple GNSS metrics
- Simultaneously compare observables from different Firewall(s)
- Centralized database of historical GNSS data (weeks, months, years)

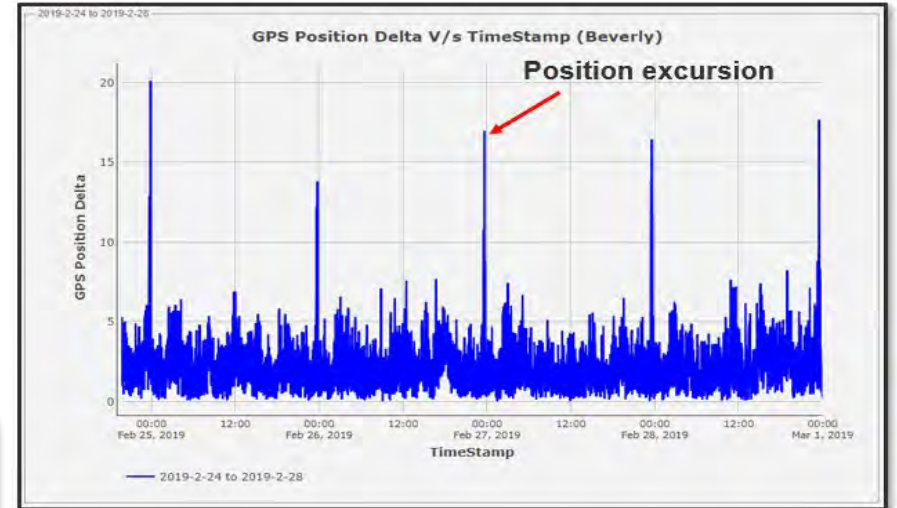
BlueSky Performance Monitoring - overview



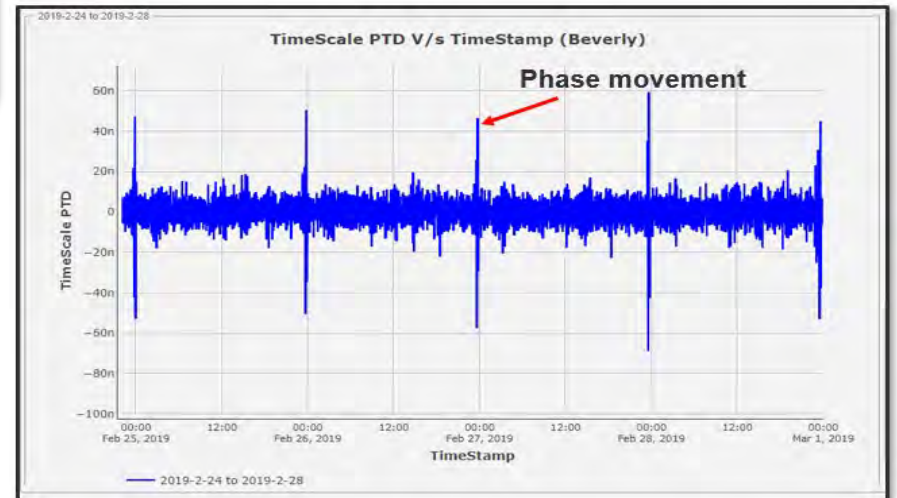
Timing Anomaly



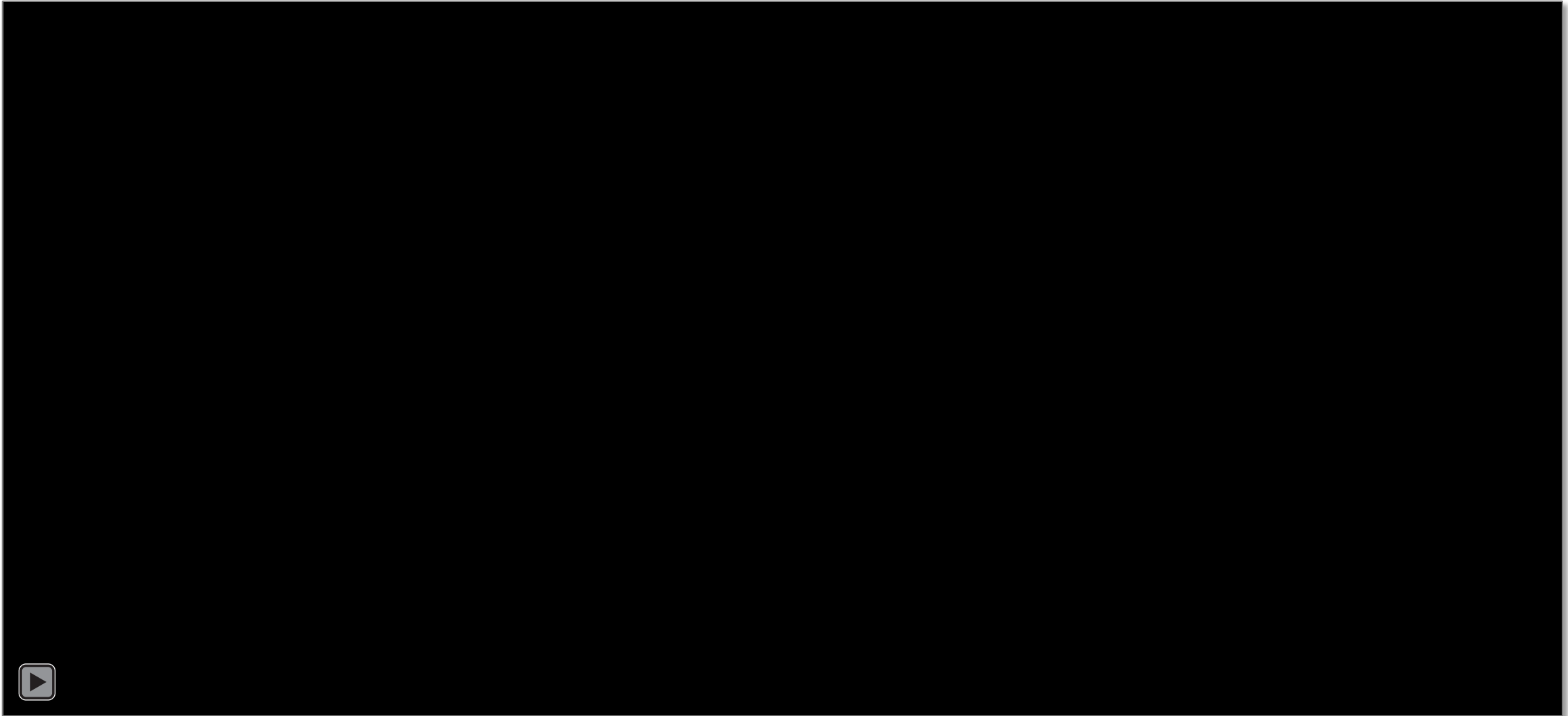
Spoof – Satellite falling out of view



Phase movement & Position Excursion



Time Anomaly



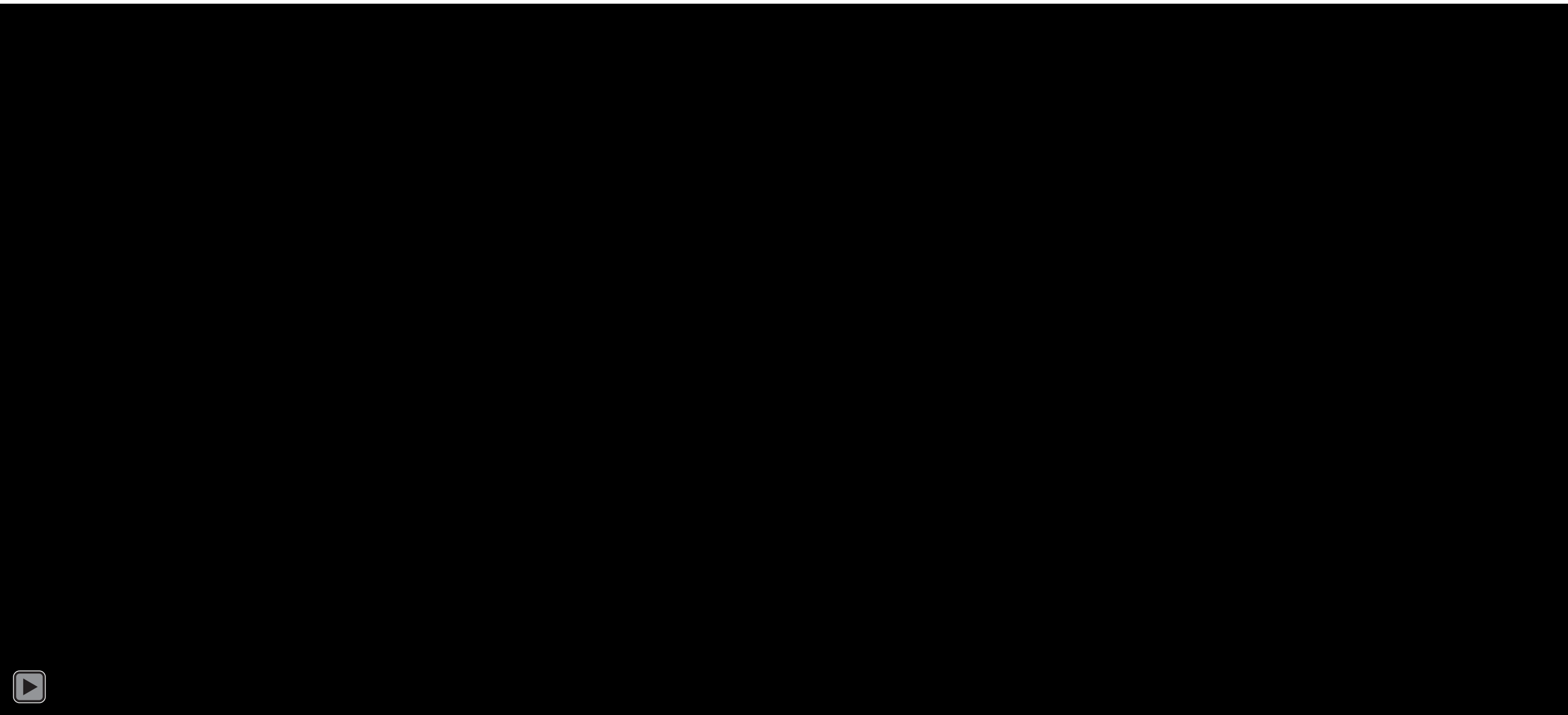
Satellite Drop-off



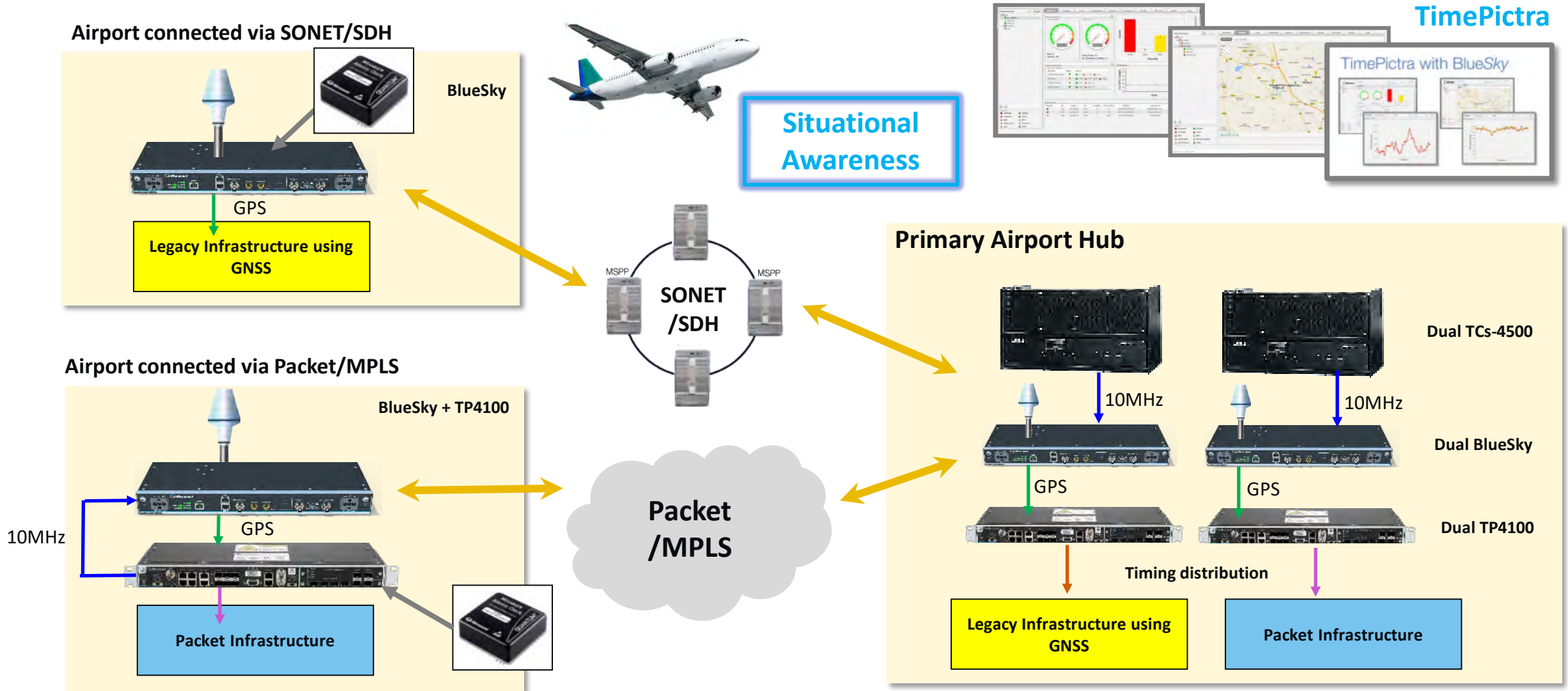
Time Anomaly #2



Position Anomaly



Aviation Timing Architecture



Microchip and Microsemi websites

Home / Synchronization and Timing Systems

Synchronization and Timing Systems

Our portfolio of synchronization and timing systems supports today's precise timing standards, including GPS-based timing, IEEE® 1588 Precision Time Protocol (PTP), Network Time Protocol (NTP), Synchronous Ethernet and DOCSIS® timing. These end-to-end timing solutions are engineered to solve your most difficult network timing challenges. Use the links below to explore our products:

- Carrier-Grade NTP and PTP IEEE 1588 Grandmasters
- Enterprise Network Time Servers
- Modular Synchronization Systems
- Time Scale Systems
- 1U Distribution Amplifiers
- GPS Instruments
- Synchronization Services
- GPS Disciplined Oscillators
- Atomic Clocks, Frequency Standards and References
- GPS and Timing Accessories

Latest Announcements:

BlueSky™ GNSS Firewall – Software Release 2.0

The BlueSky GNSS Firewall is a cost-effective overlay solution that is installed between existing Global Navigation Satellite System (GNSS) antennas and GPS systems. Similar to a network firewall, the BlueSky GNSS Firewall protects already-deployed GPS systems inside the firewall from untrusted, sky-based signals outside the firewall. Software Release 2.0 includes charting and advanced threshold settings of GNSS observables such as satellites-in-view, carrier-to-noise, position dispersion, phase time deviation and Radio Frequency (RF) power level to simplify system turn-up and deployment.

- Protects GPS systems from spoofing and jamming
- Hardened GPS output provides secure signal that is isolated from live-sky interference
- Optional internal Miniature Atomic Clock (MAC) for extended holdover and enhanced detection
- Seamless integration of BlueSky performance monitoring within TimePictra® software suite

[Download Brochure](#)

[Learn More](#)

[Download Software 2.0 Sell Sheet](#)

<https://www.microchip.com/design-centers/synchronization-and-timing-systems>

Home / Products & Services / Timing & Synchronization / Synchronization Systems / GPS Instruments / BlueSky GNSS Firewall

BlueSky GNSS Firewall

[Overview](#) [Key Features](#) [Webinar and Videos](#) [Resources](#) [Ordering Info](#)

Protects GNSS Systems against spoofing and jamming threats

The vulnerability of GNSS systems to various signal incidents is well documented. The rapid proliferation of GNSS systems has embedded these vulnerabilities into critical national infrastructure as well as corporate infrastructures that rely on GNSS-delivered position, navigation and timing (PNT) for daily operations. The widespread deployment of GNSS makes it impractical to replace all fielded GNSS systems in a timely or cost-effective manner.

Microsemi provides a portfolio of technologies, products, and services that enables operators of Critical Infrastructure to construct a secure and robust PNT network that is resilient to GNSS errors as well as errors coming from other sky-based delivery channels such as Galileo, GLONASS, BeiDou, or another. Details of this complete portfolio can be found [here](#).

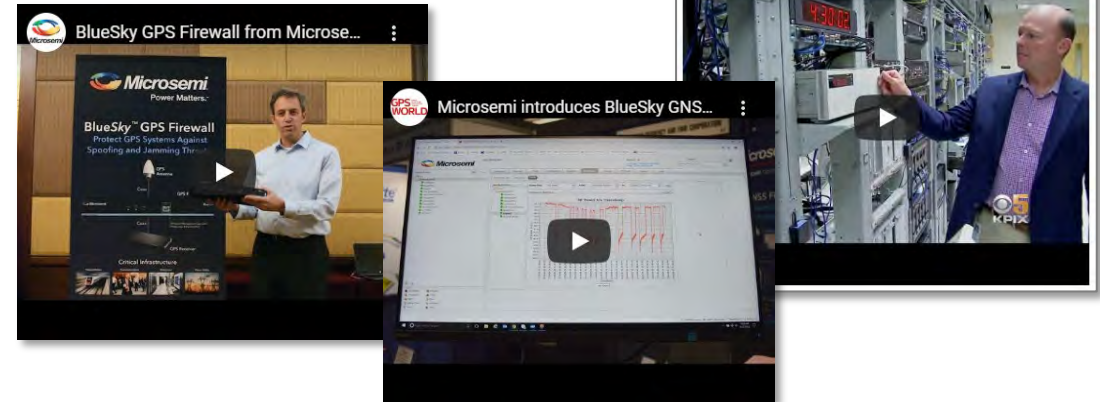
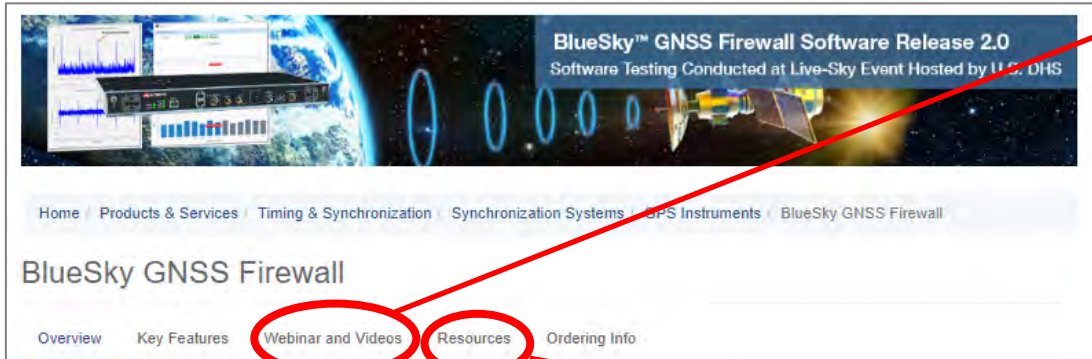
The BlueSky™ GNSS Firewall protects already deployed GNSS systems by providing a cost-effective overlay solution installed between existing GNSS antennas and GNSS systems. Similar to a network firewall, the BlueSky GNSS Firewall protects systems inside the firewall from untrusted sky-based signals outside the firewall.

The new BlueSky GNSS Firewall Software Release 2.0 includes charting and advanced threshold settings of GNSS observables. These improvements are as a result of participation in an industry live-sky testing event hosted by the U.S. Department of Homeland Security (DHS) which included GNSS threat scenarios.

Identifies and Protects GNSS Systems from Spoofing and Jamming

[Download Brochure](#)

<https://www.microsemi.com/product-directory/gps-instruments/4398-bluesky-gps-firewall>



Protects GNSS Systems against spoofing and jamming threats

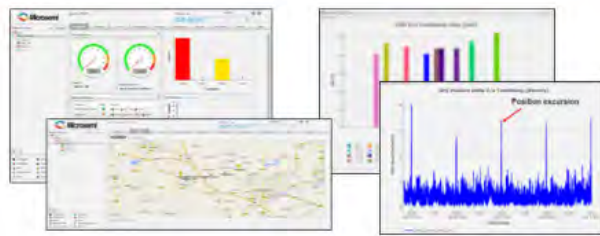
The vulnerability of GNSS systems to various signal incidents is well documented. The rapid proliferation of GNSS systems has embedded these vulnerabilities into critical national infrastructure as well as corporate infrastructures that rely on GNSS-delivered position, navigation and timing (PNT) for daily operations. The widespread deployment of GNSS makes it impractical to replace all fielded GNSS systems in a timely or cost-effective manner.

Microsemi provides a portfolio of technologies, products, and services that enables operators of Critical Infrastructure to construct a secure and robust PNT network that is resilient to GNSS errors as well as errors coming from other sky-based delivery channels such as Galileo, GLONASS, BeiDou, or another. Details of this complete portfolio can be found [here](#).

The BlueSky™ GNSS Firewall protects already deployed GNSS systems by providing a cost-effective overlay solution installed between existing GNSS antennas and GNSS systems. Similar to a network firewall, the BlueSky GNSS Firewall protects systems inside the firewall from untrusted sky-based signals outside the firewall.



The new BlueSky GNSS Firewall Software Release 2.0 includes charting and advanced threshold settings of GNSS observables. These improvements are as a result of participation in an industry live-sky testing event hosted by the U.S. Department of Homeland Security (DHS) which included GNSS threat scenarios.



Identifies and Protects GNSS Systems from Spoofing and Jamming

<https://www.microsemi.com/product-directory/gps-instruments/4398-bluesky-gps-firewall>

Questions?

