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

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.

MICROCHIP

GPS disruptions in recent NATO war games

Russia suspected of jamming GPS signal in Finland

12 November 2018 Share

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.

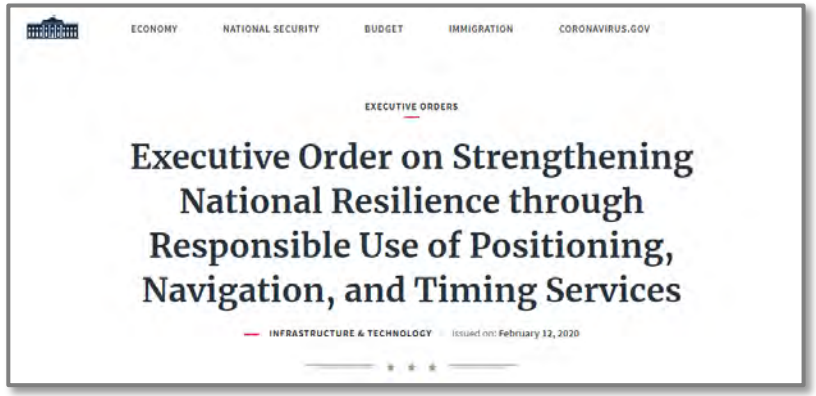
"It is possible that Russia has been the disrupting party in this. Russia is known to possess such capabilities."

MICROCHIP

Presidential Executive Order

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

Microchip Solution



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

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

MICROCHIP

Cybersecurity and Infrastructure Security Agency

CISA
CYBER+INFRASTRUCTURE

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
• 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	• Distribute Electricity • Maintain Supply Chains • Trans • Trans Pass • Pass • Trans Pass • Trans Pass • Transport Materials by Pipeline • Transport Passengers by Mass Transit	• 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	• Exploration and Extraction Of Fuels ning and g Fuels Electricity ture Equipment and Provide ral Products and and Provide nd Animal Food and Services • 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"

MICROCHIP

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

CISA
CYBER+INFRASTRUCTURE

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

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

MICROCHIP

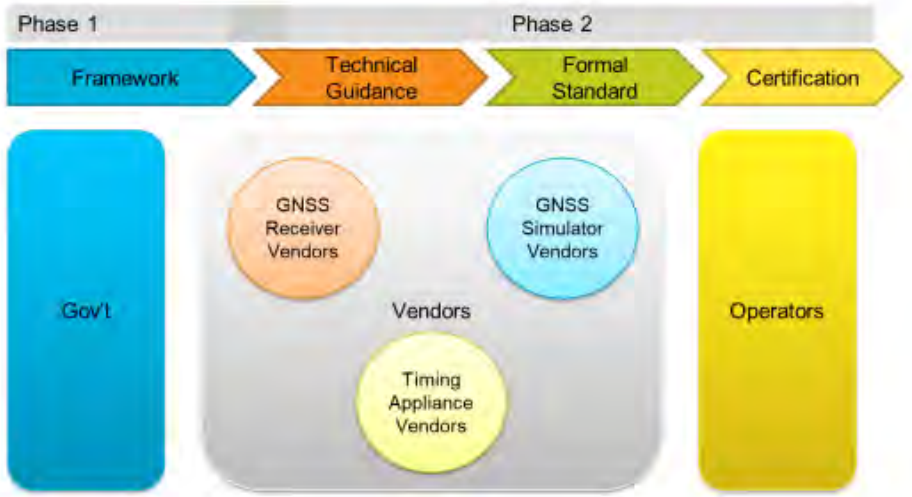
Resilient PNT Conformance Working Group

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
Homeland Security Systems Engineering & Development Institute

MICROCHIP

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***

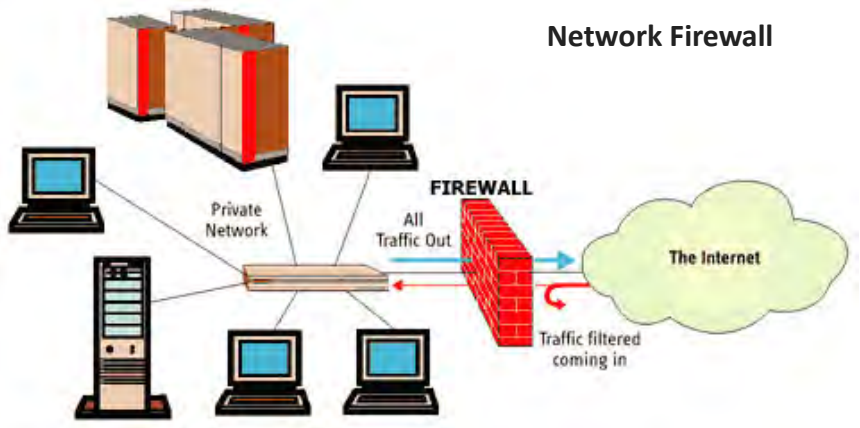
Civilian GPS Receivers

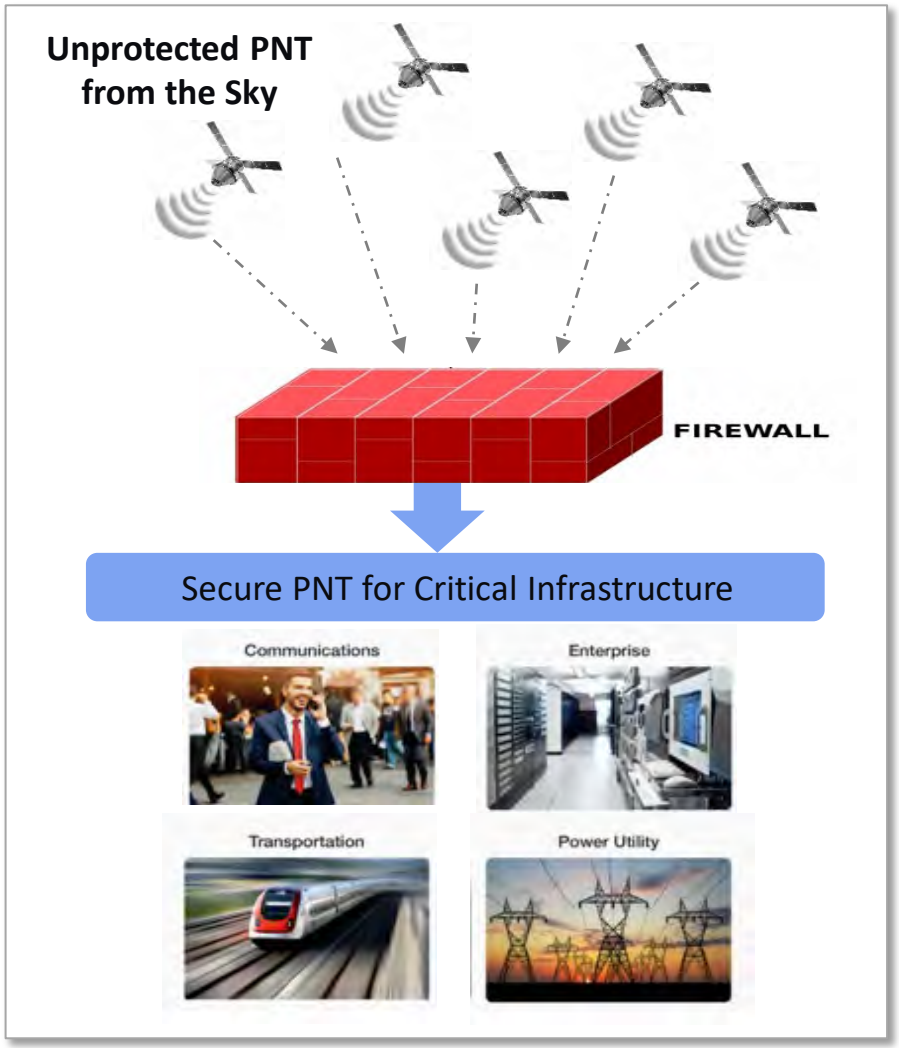
- **Military GPS receiver**
  - Selective Availability Anti-Spoofing Module (SAASM) receivers utilize L1 and the encrypted L2 signal for GPS tracking
  - Provide better anti-jam performance and better protection against more advanced GPS attacks
  - ***Not available for commercial applications***

Military GPS Receiver

Firewall concept

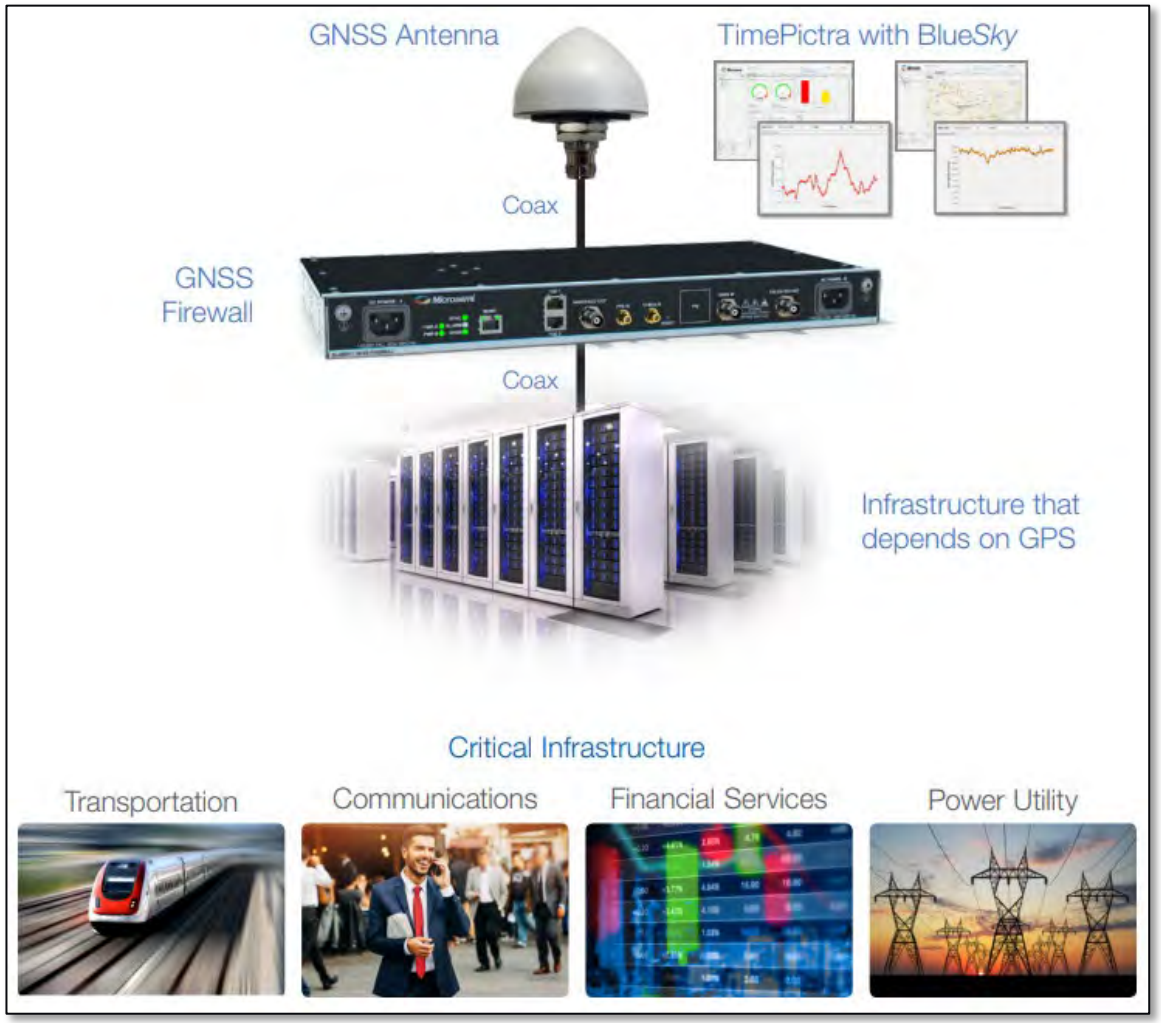
Physical Firewall at Electrical Substation





MICROCHIP

Secure Firewall Overlay



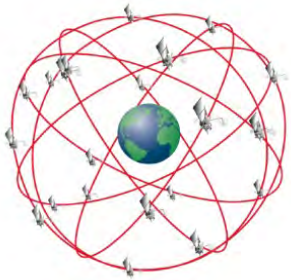
- Protects against GNSS spoofing and jamming
- Simple connection between GNSS antenna and GPS system
- Optional internal MAC for holdover
- 1PPS and 10 MHz timing reference inputs for extended holdover (connection to external cesium reference)
- Redundant AC or DC power options
- “BlueSky Performance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

BlueSky GNSS Firewall (Hardened vs. Validated)

Optional
(inside)

or

Live Sky



Reception/Anomaly Detection

Hardened
Output (GPS format)

Validated
Output (**all bands**)

Holdover

MICROCHIP

Support for Galileo

Optional
(inside)

or

Live Sky

GALILEO and NAVSTAR GPS

Reception/Anomaly Detection

GPS TIME

or

GALILEO TIME

Hardened Output (**GPS format**)

Validated Output (**all bands**)

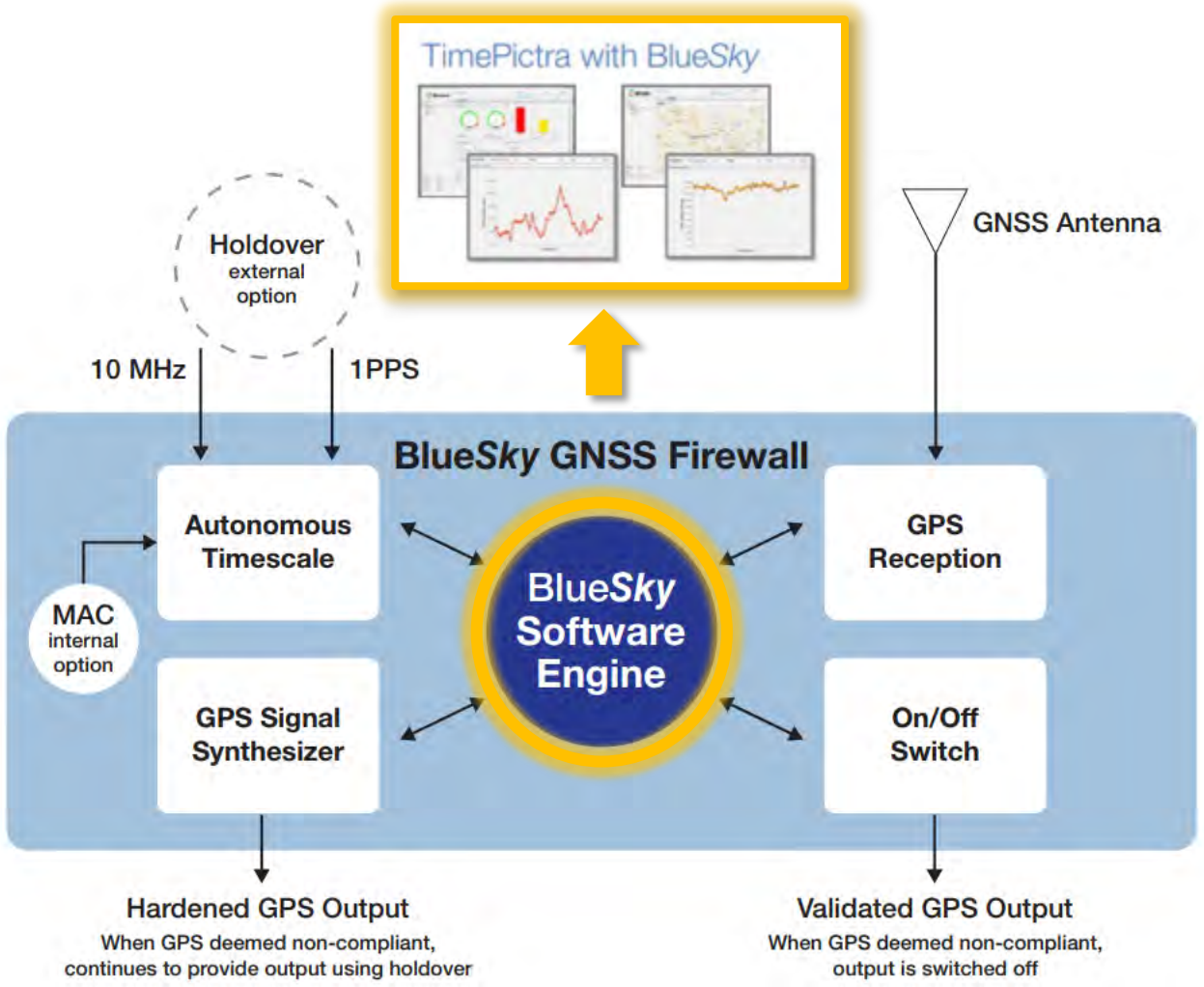
Holdover

MICROCHIP

Blue*Sky* 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

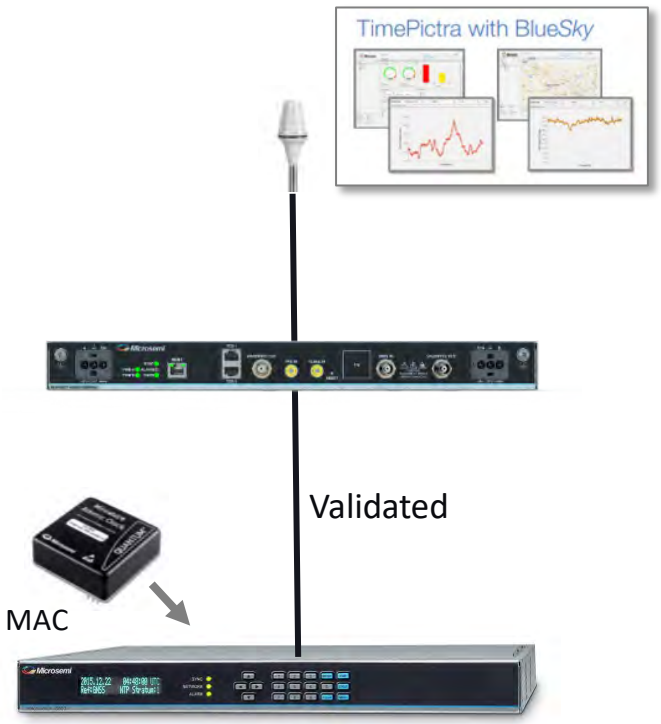
- **BlueSky Performance Monitoring (integrated as part of TimePictra)**
  - Enables management of multiple firewalls from a centralized location
  - Provides situational awareness of your entire GNSS infrastructure (BlueSky Performance Monitoring)



MICROCHIP

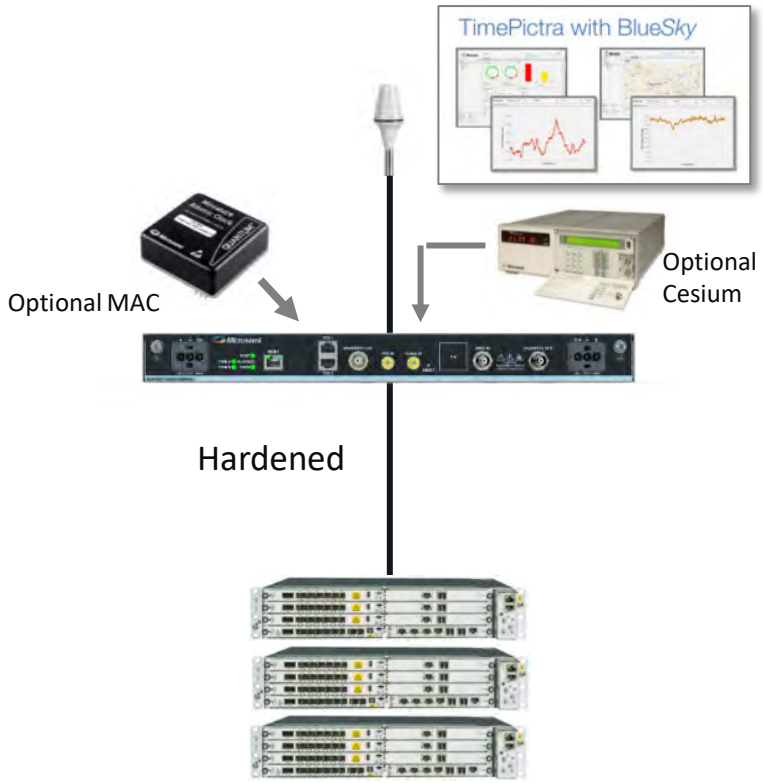
BlueSky GNSS Firewall Deployment models

Firewall using Validated Output



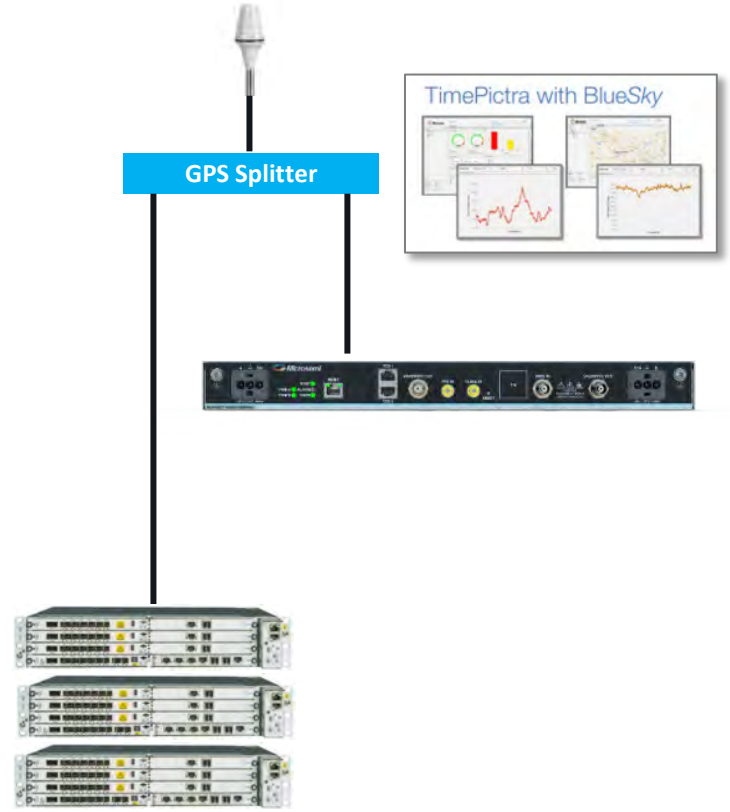
SyncServer S600/S650

Firewall using Hardened Output



Equipment requiring GPS/L1 signal

Firewall deployed for monitoring only



Equipment requiring GPS/L1 signal

MICROCHIP

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

Lab Testing

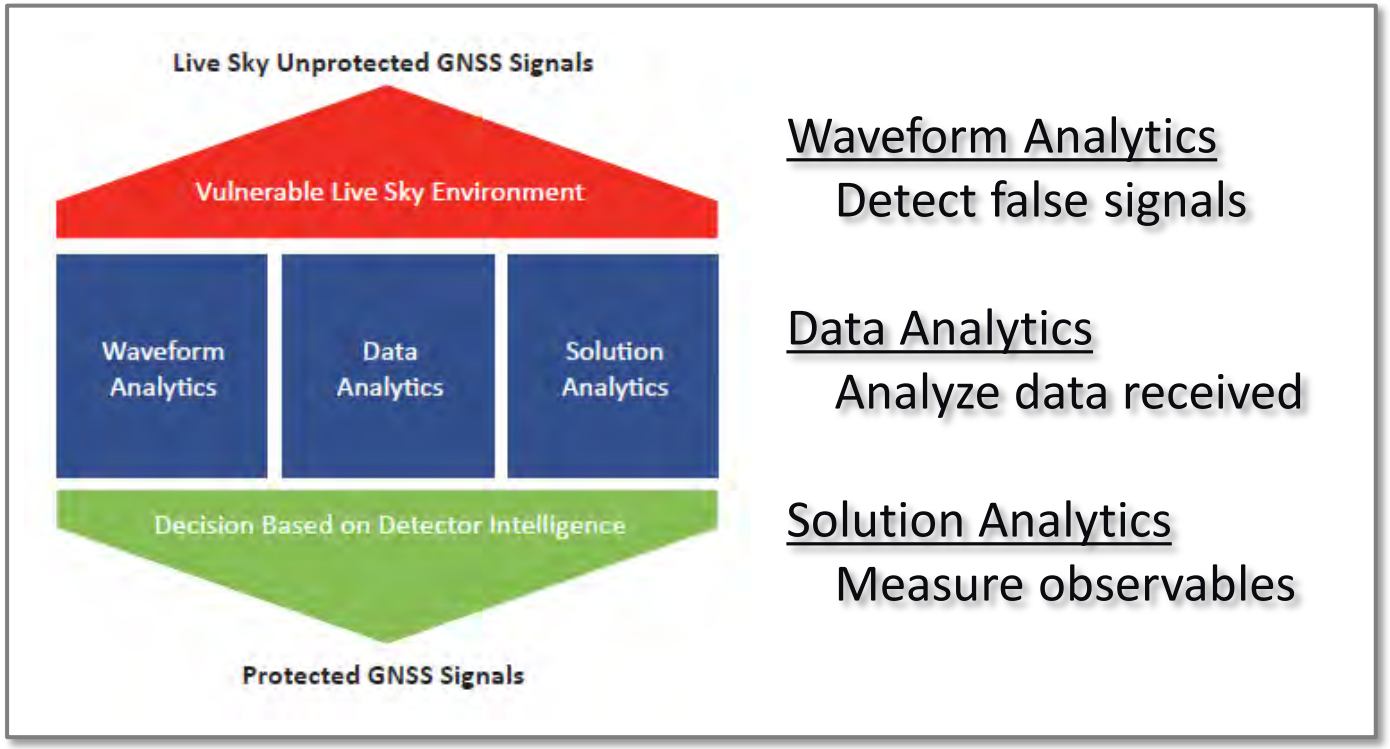
VS

Live Sky Testing

MICROCHIP

BlueSky GNSS Firewall Software Release 2.0

Improved Protection and Threshold Settings

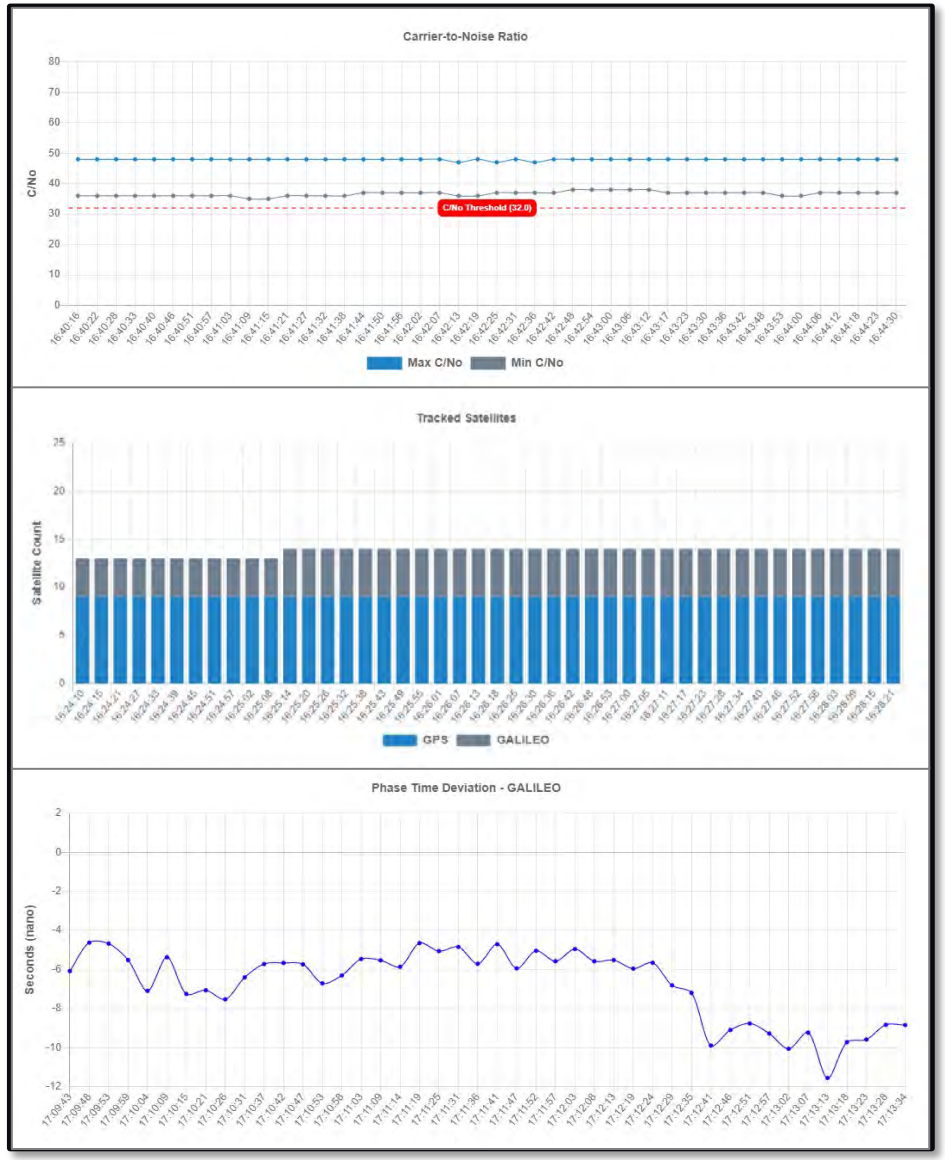


Waveform Analytics
Detect false signals

Data Analytics
Analyze data received

Solution Analytics
Measure observables

BlueSky Information Charts



MICROCHIP

BlueSky GNSS Firewall, Software Release 2.0.1

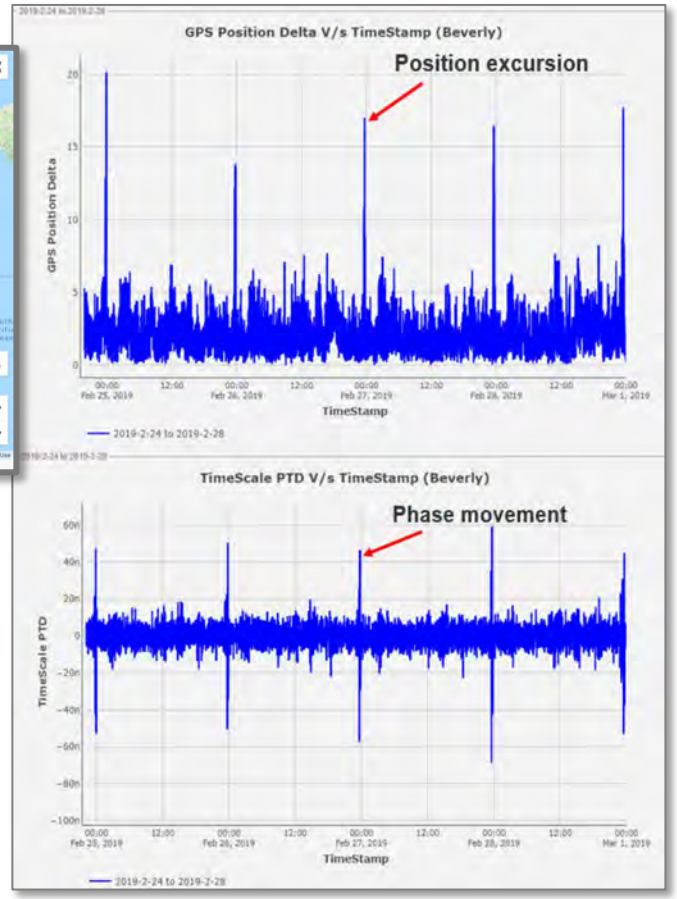
NEW

Local Charting

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

Release 2.0.1

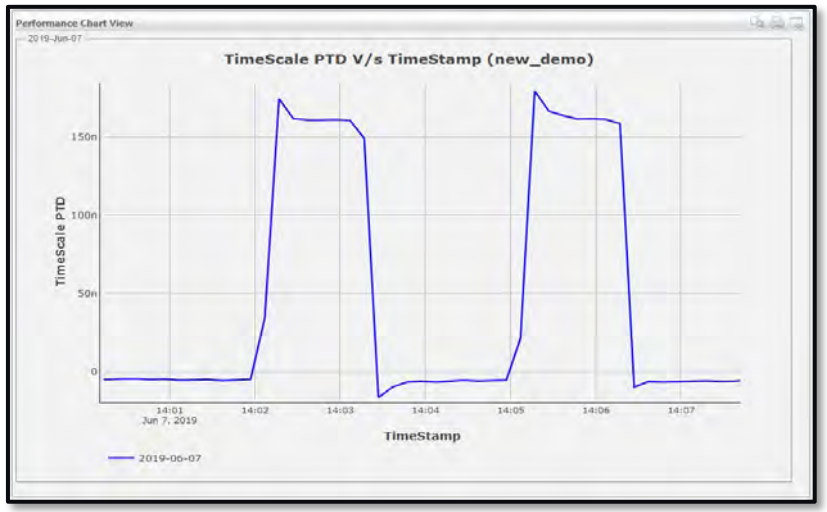
TimePictra with BlueSky Performance Monitoring



- 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)

MICROCHIP

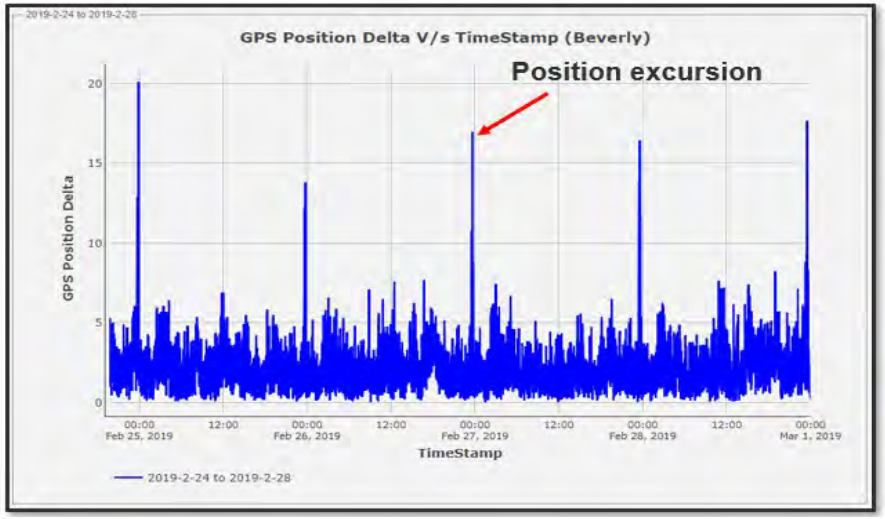
BlueSky Performance Monitoring - overview

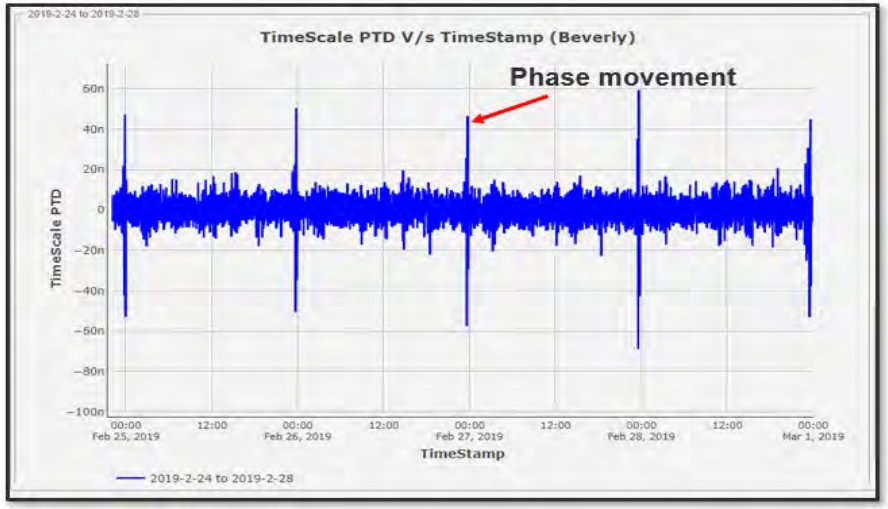


Timing Anomaly

Spoof – Satellite falling out of view

Phase movement & Position Excursion



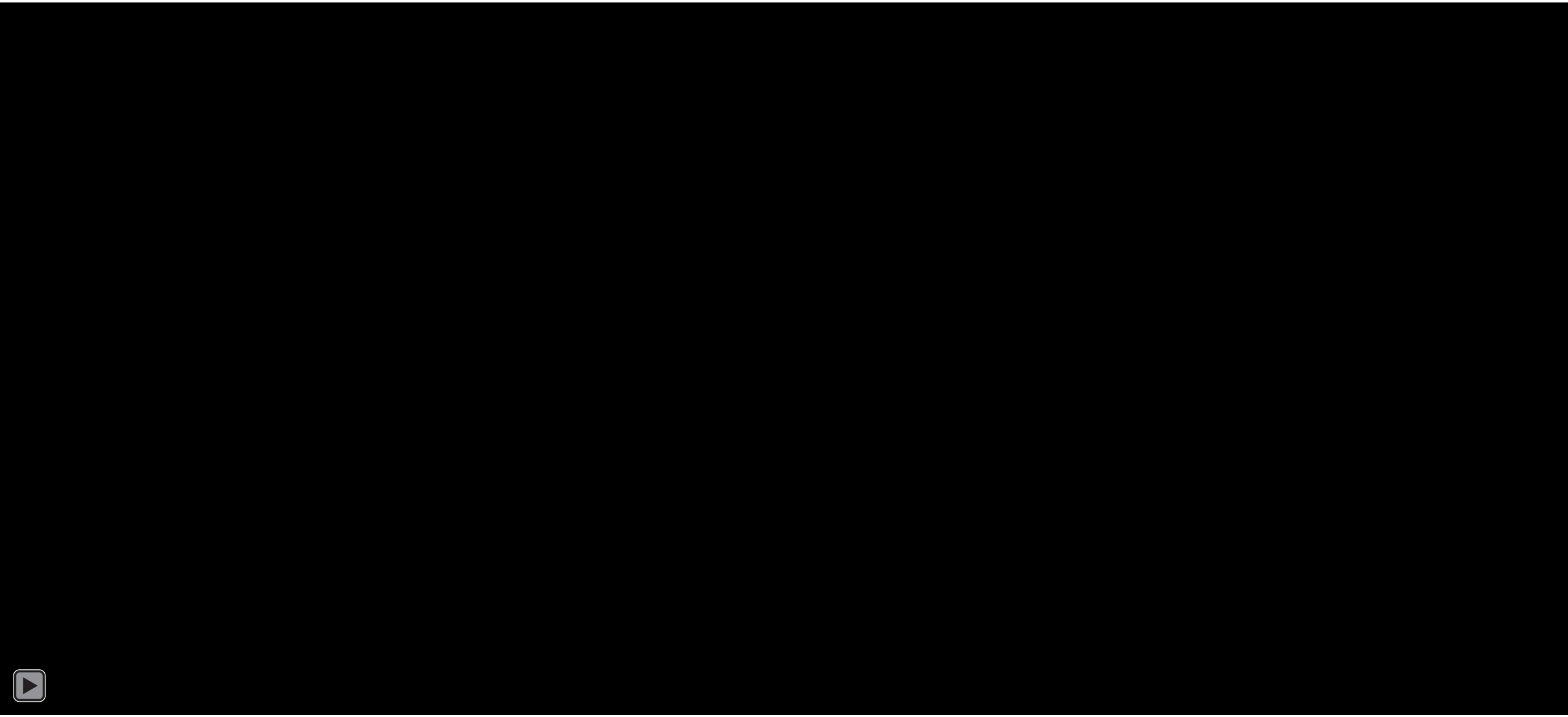


MICROCHIP

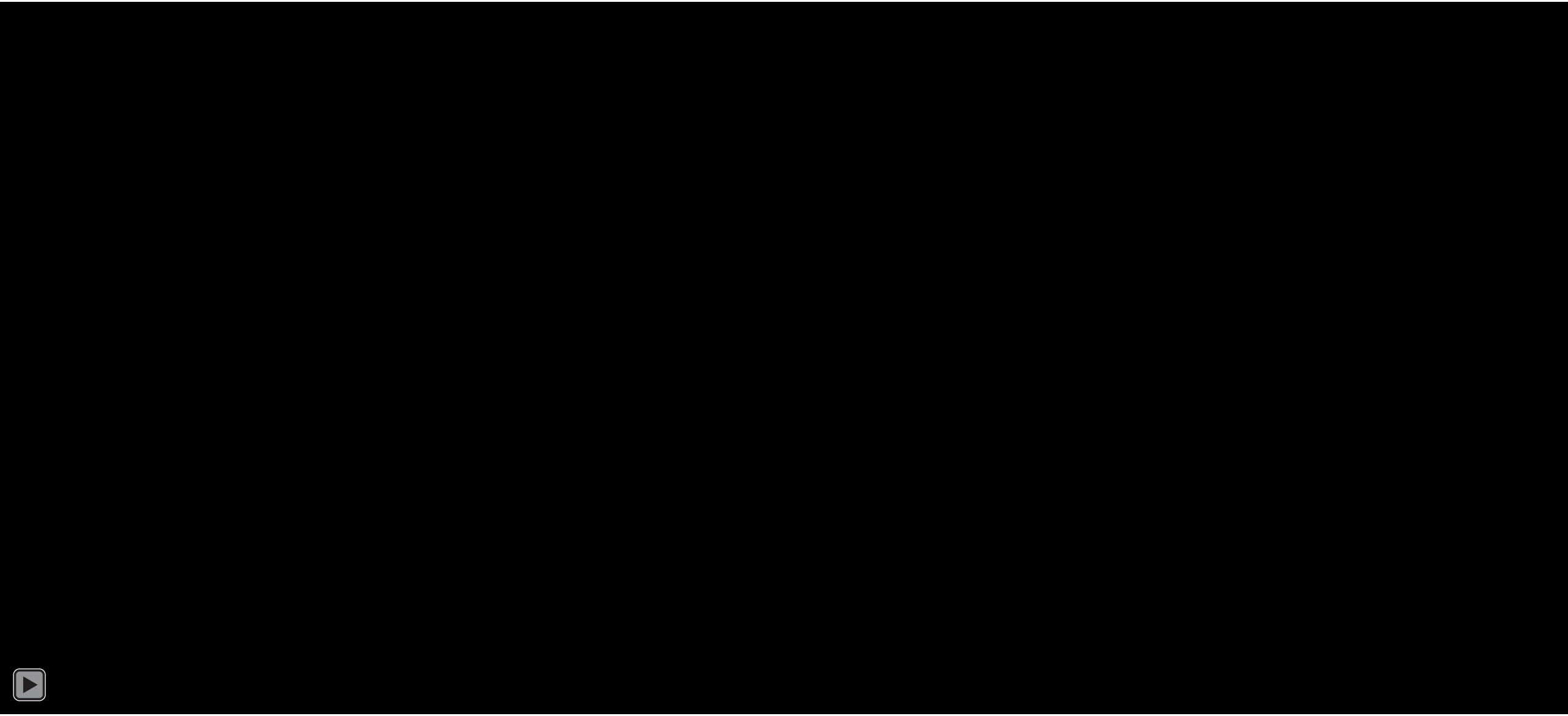
Time Anomaly

Satellite Drop-off

Time Anomaly #2

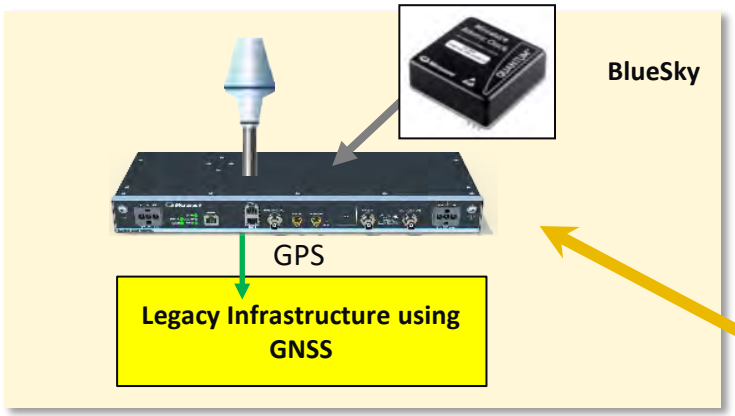


Position Anomaly



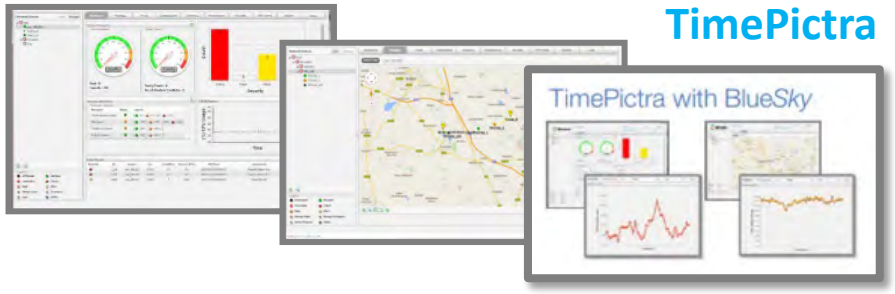
Aviation Timing Architecture

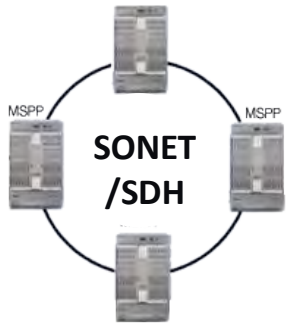
Airport connected via SONET/SDH



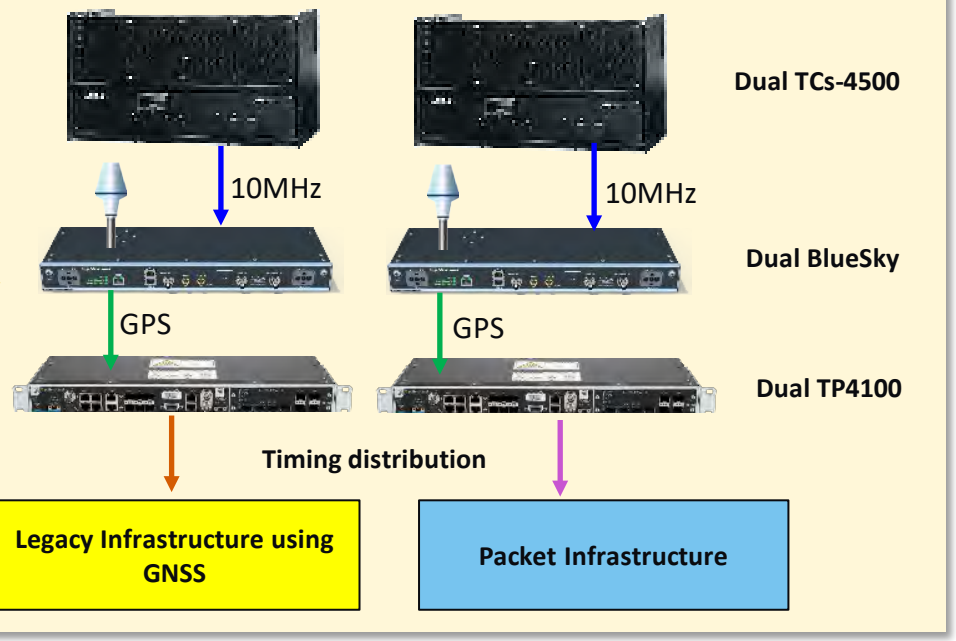
Situational Awareness

TimePictra

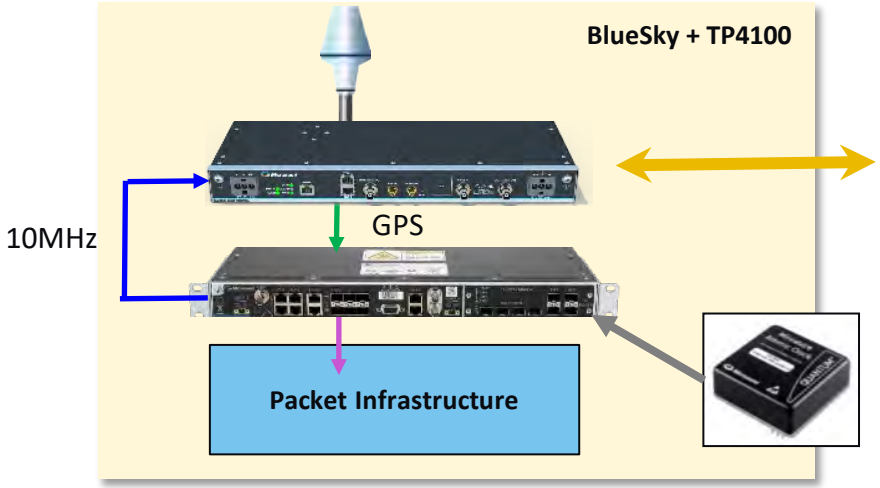




Primary Airport Hub



Airport connected via Packet/MPLS

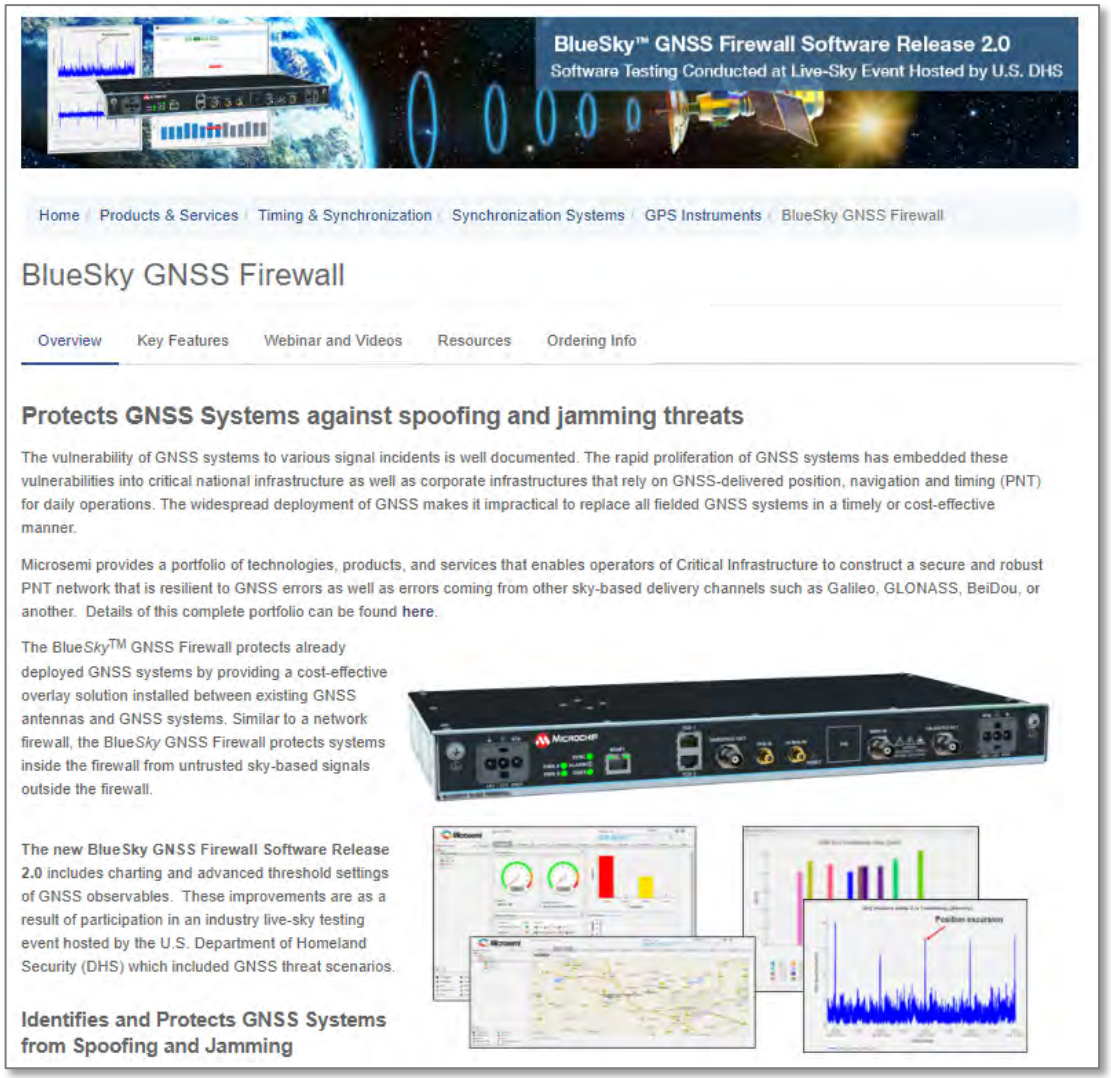


Packet /MPLS

MICROCHIP

Microchip and Microsemi websites

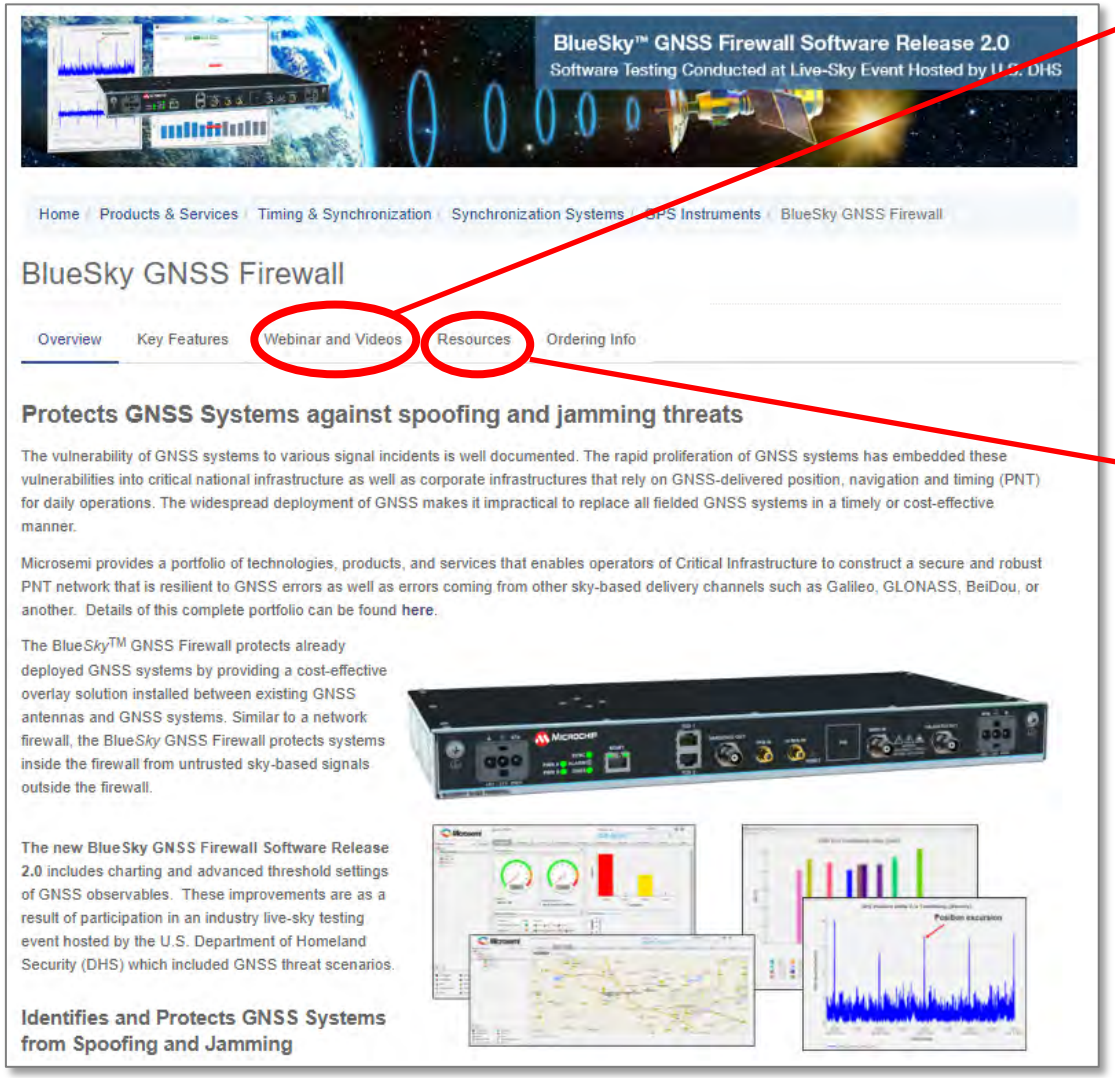
https://www.microchip.com/design-centers/synchronization-and-timing-systems



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

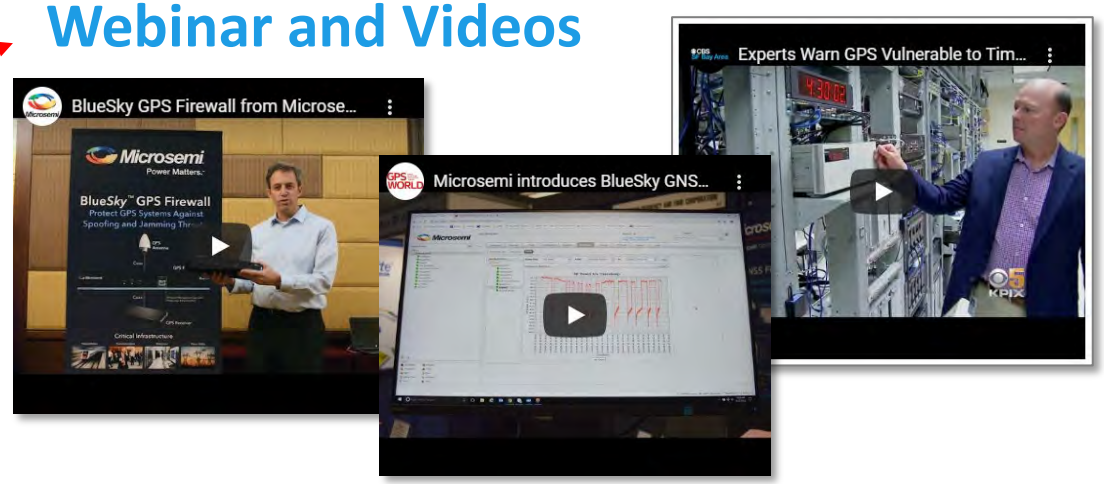
MICROCHIP

www.microsemi.com

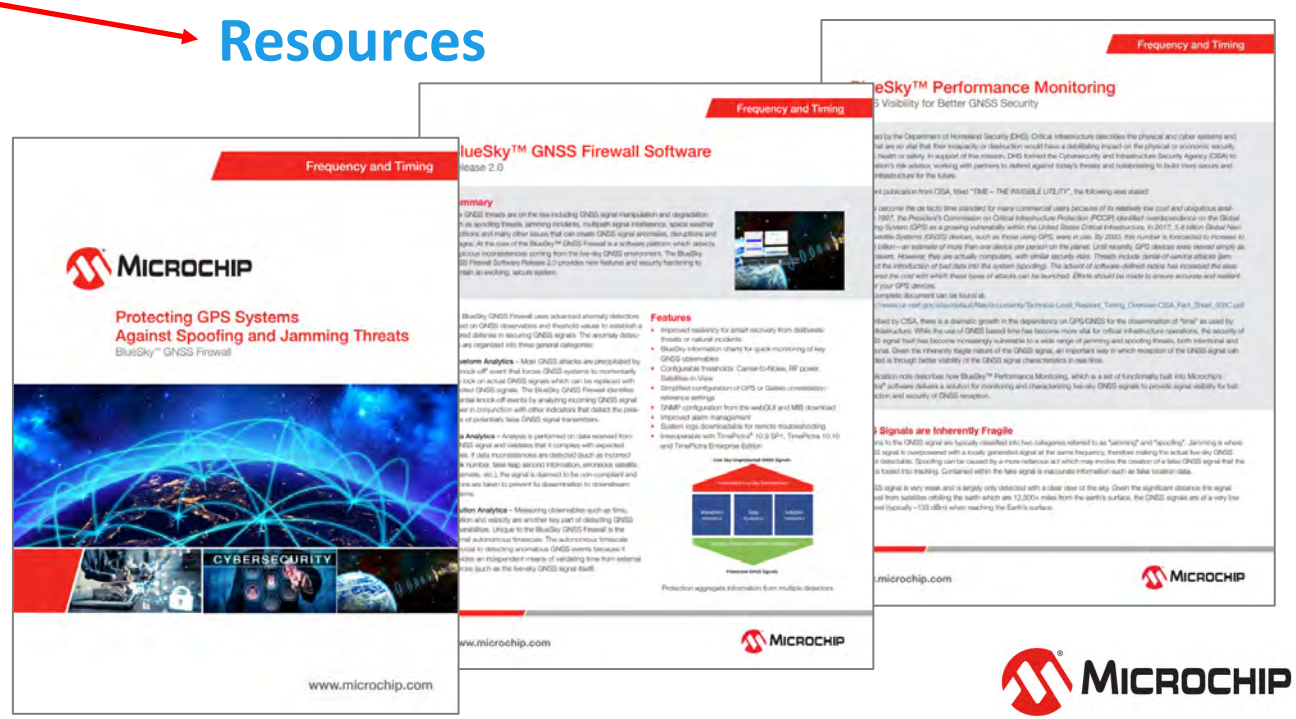


https://www.microsemi.com/product-directory/gps-instruments/4398-bluesky-gps-firewall

Webinar and Videos



Resources



MICROCHIP

Questions?

MICROCHIP