U. S. Department of Transportation Maritime Administration PNT Resiliency Pilot Program: Phase II

Final Report

Final Report—May 2025
DOT-VNTSC-OST-25-04

Prepared for:
Office of the Assistant Secretary for Research and Technology (OST-R)
Office of PNT and Spectrum Management
1200 New Jersey Avenue, SE
Washington, DC 20590

U.S. Department of Transportation
Volpe Center

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers’ names appear herein solely because they are considered essential to the objective of this report.

REPORT DOCUMENTATION PAGE

1. REPORT DATE
May 2025

2. REPORT TYPE
Final Report

3. DATES COVERED

START DATE

END DATE

4. TITLE AND SUBTITLE
USDOT PNT Pilot Program - MARAD

5a. CONTRACT NUMBER

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

5d. PROJECT NUMBER
OS92AB22

5e. TASK NUMBER
WP469/ABP469

5f. WORK UNIT NUMBER
V-345

6. AUTHOR(S)
Stephen Mackey, Andrew Hansen, Hadi Wassaf, Jonathon Poage, George Mantis, Melanie Soares Schumann, Christopher Scarpone, Robert Samiljan, John Flake, Ali Bowens

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology (OST-R)
John A Volpe National Transportation Systems Center
220 Binney Street
Cambridge, MA 02142-1093

8. PERFORMING ORGANIZATION REPORT NUMBER
DOT-VNTSC-OST-25-04

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of the Asst. Secretary of Transportation
for Research and Technology (OST-R)
Office of Positioning, Navigation and Timing (PNT) and Spectrum Management
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

13. SUPPLEMENTARY NOTES

14. ABSTRACT
In order to improve the resilience of the Nation’s critical infrastructure to GPS disruptions, the President issued Executive Order (EO) 13905 “Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services,” in February 2020 to foster responsible use of PNT services. In accordance with Section 4(g) of EO 13905, the U.S. Department of Transportation (USDOT) undertook a Pilot Program to develop critical infrastructure profiles for the transportation sector. The Department selected to focus on GPS jamming and spoofing in the maritime environment in a partnership between the Office of the Assistant Secretary for Research and Technology (OST-R) and the Maritime Administration (MARAD) as its initial candidate for the PNT Profile Pilot Program. This Phase II report builds on the work completed in Phase I.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

a. REPORT
CUI

b. ABSTRACT
CUI

C. THIS PAGE
CUI

17. LIMITATION OF ABSTRACT
SAR

18. NUMBER OF PAGES
136

19a. NAME OF RESPONSIBLE PERSON
Andrew Hansen

19b. PHONE NUMBER (Include area code)
617-494-6525

SI* (MODERN METRIC) CONVERSION FACTORS

APPROXIMATE CONVERSIONS TO SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
LENGTH				
in	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
AREA				
in^2	square inches	645.2	square millimeters	mm^2
ft^2	square feet	0.093	square meters	m^2
yd^2	square yard	0.836	square meters	m^2
ac	acres	0.405	hectares	ha
mi^2	square miles	2.59	square kilometers	km^2
VOLUME				
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft^3	cubic feet	0.028	cubic meters	m^3
yd^3	cubic yards	0.765	cubic meters	m^3
NOTE: volumes greater than 1000 L shall be shown in m^3				
MASS				
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2000 lb)	0.907	megagrams (or "metric ton")	Mg (or "t")
oz	ounces	28.35	grams	g
TEMPERATURE (exact degrees)				
°F	Fahrenheit	5 (F-32)/9 or (F-32)/1.8	Celsius	°C
ILLUMINATION				
fc	foot-candles	10.76	lux	lx
fl	foot-Lamberts	3.426	candela/m^2	cd/m^2
FORCE and PRESSURE or STRESS				
lbf	poundforce	4.45	newtons	N
lbf/in^2	poundforce per square inch	6.89	kilopascals	kPa

APPROXIMATE CONVERSIONS FROM SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
LENGTH				
mm	millimeters	0.039	inches	in
m	meters	3.28	feet	ft
m	meters	1.09	yards	yd
km	kilometers	0.621	miles	mi
AREA				
mm^2	square millimeters	0.0016	square inches	in^2
m^2	square meters	10.764	square feet	ft^2
m^2	square meters	1.195	square yards	yd^2
ha	hectares	2.47	acres	ac
km^2	square kilometers	0.386	square miles	mi^2
VOLUME				
mL	milliliters	0.034	fluid ounces	fl oz
L	liters	0.264	gallons	gal
m^3	cubic meters	35.314	cubic feet	ft^3
m^3	cubic meters	1.307	cubic yards	yd^3
mL	milliliters	0.034	fluid ounces	fl oz
MASS				
g	grams	0.035	ounces	oz
kg	kilograms	2.202	pounds	lb
Mg (or "t")	megagrams (or "metric ton")	1.103	short tons (2000 lb)	T
g	grams	0.035	ounces	oz
TEMPERATURE (exact degrees)				
°C	Celsius	1.8C+32	Fahrenheit	°F
ILLUMINATION				
lx	lux	0.0929	foot-candles	fc
cd/m^2	candela/m^2	0.2919	foot-Lamberts	fl
FORCE and PRESSURE or STRESS				
N	newtons	0.225	poundforce	lbf
kPa	Kilopascals	0.145	poundforce per square inch	lbf/in^2

*SI is the symbol for the International System of Units. Appropriate rounding should be made to comply with Section 4 of ASTM E380. (Revised March 2003)

Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Term
3D	three dimensional
AGC	automatic gain control
AI	artificial intelligence
AoA	angle of arrival
ASAP	Advanced Scalable Assured PNT
CAI	Cold-atom interferometer
CERN	European Council for Nuclear Research
CKF	Cubature Kalman filter
CONOPS	concept of operations
COTS	commercial off the shelf
CPNT	complementary positioning, navigation, and timing
CRADA	Cooperative Research and Development Agreement
CRPA	controlled reception pattern antenna
CRUCIBLE	Federal data repository of suspected cases of GNSS purposeful interference
CSF	[NIST] Cybersecurity Framework
DEM	Digital elevation map
DF	Direction finding
DUT	Device under test
ECDIS	Electronic chart and information display system
EGI	embedded-GPS-intertial
eLORAN	Enhanced Long-Range Navigation
EO	Executive Order
FMV	full motion video
FSO	Free-space optics
GAINS	Gravity-Aided Inertial Navigation System
GET-CI	GPS Equipment Testing for Critical Infrastructure
GLONASS	GLObal NAvigation Satellite System
GNSS	global navigation satellite system
GPR	Ground penetrating radar
GPS	Global Positioning System
HFR	High-frequency RADAR
IIP	Innovation Program
IMU	inertial measurement unit
INS	inertial navigation system
ITAR	International Traffic in Arms Regulations
LEO	low Earth orbit
LNA	Low-noise amplifier
LOP	Line of position
LWIR	long wave infrared
MARAD	Maritime Administration
MEO	Medium Earth orbit
MRPA	Modified Reception Pattern Antenna
MRPD	Minimum-range prescribed Doppler
MSC	Military Sealift Command
MuWNS	Muometric Wireless Navigation System
NIST	National Institute of Standards and Technology

NISTIR	National Institute of Standards and Technology Internal Report
NIWC	Naval Information Warfare Center
ONR	Office of Naval Research
OST-R	Office of the Assistant Secretary of Transportation for Research and Technology
OSNMA	Galileo Open Service Navigation Message Authentication
PNT	positioning, navigation and timing
PNTAB	Positioning, Navigation and Timing Advisory Board
PoA	power of arrival
PPP	Precise Point Positioning
PTP	Precision Time Protocol
PSD	Power Spectral Density
RF	Radiofrequency
RRF	Ready Reserve Force
SBAS	satellite-based augmentation system
SCAM	Simultaneous calibration and mapping
SLAM	simultaneous location and mapping
SLIM	street level image matching
SLMBRS	Simultaneous Localization and Mapping Based on RF Signals
SONET	Synchronous Optical NETwork, a fiber data protocol
SOOP	Signals of opportunity
SPOTAGE	Sel-Positioning Off Targeted Anti GPS Emitters
SS	steamship
STL	satellite time and location
SWaP	size, weight, and power
TDoA	Time difference of arrival
TDC	Time-to-digital converter
TITAN	Trusted Intertial Terrain-Aided Navigation
TRL	Technology readiness level
USDOT	U.S. Department of Transportation
UTC	Coordinated Universal Time
VBN	vision-based navigation
VDES	VHF Data Exchange System
VHF	Very high frequency
VPS	Visual positioning system
WSMR	White Sands Missile Range

Executive Summary

The Role of GPS in Transportation

The Global Positioning System (GPS) is the cornerstone service for positioning, navigation and timing (PNT) in the U.S. and around the globe. It is used across all transportation modes—aviation, maritime, surface, rail, and even pipelines—to improve the safety and efficiency of the U.S. National Transportation System. Yet, with that ubiquitous dependence comes both greater risk and greater consequence should the GPS signal be disrupted or degraded, whether intentionally or unintentionally.

The U.S. Department of Transportation PNT Profile Pilot Program

In order to improve the resilience of national critical infrastructure to GPS disruptions, the President issued Executive Order (EO) 13905 "Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services" in February 2020. EO 13905 orders U. S. Government agencies to understand and develop responsible use of PNT services through a risk-based approach. In accordance with Section 4(g) of EO 13905, the U.S. Department of Transportation (USDOT) undertook a PNT Pilot Program to develop critical infrastructure PNT dependency profiles for the transportation sector. The Department selected to focus on GPS jamming and spoofing in the maritime environment in a partnership between the Office of the Assistant Secretary for Research and Technology (OST-R) and the Maritime Administration (MARAD) as its initial candidate for the PNT Profile Pilot Program. MARAD maintains over 40 U.S. Government-owned ships as part of the Ready Reserve Force (RRF) to support national security operations around the globe. Each of these ships relies on multiple GPS receivers to acquire PNT data for safe navigation and to support other safety-critical systems.

The PNT Pilot Program raised awareness of the extent to which maritime vessels depend on PNT services; identified approaches for maritime operations to withstand disruption or manipulation of those services; and engaged the maritime community to promote awareness of PNT dependencies and services. In December 2020, USDOT hosted the GPS Jamming and Spoofing in the Maritime Environment Workshop featuring speakers from government, industry, and non-profit PNT organizations. The objective of that workshop was to raise awareness of the extent to which maritime vessels depend on PNT services among commercial vessel operators, regulators, enforcement organizations, technology providers, PNT experts, and policy agencies. In April 2021, the Volpe National Transportation System Center (Volpe Center) began work supporting the PNT Pilot Program through an inter-agency agreement with OST-R.

Working with MARAD, the Program team identified a candidate vessel (the Fast Sealift Ship *SS Antares*) for operational testing. The Program team conducted interviews with MARAD personnel, ship's crews, vessel management services, and equipment vendors to develop a viable testing program. Following the information gathering process, the Program team coordinated three technical data collection efforts to address detailed identification of vulnerabilities, assess threats, and consider complementary PNT and GPS backup services that could serve as mitigations to operational impacts. This completed the first phase of the MARAD PNT Pilot Program.

Based on Phase I findings and recommendations, Phase II of the Program coordinated a live sea trial aboard the *SS Cornhusker State* during a mission abroad from August to December 2023. The Team installed Fleet-representative GPS receivers, a spectrum analyzer, a host of commercial-off-the-shelf (COTS) protective solutions for evaluation, and a ground truth reference system.

The data collected aboard the *Cornhusker State* was supplemented by an extensive data collection effort at the NAVFEST test campaign in May 2024. NAVFEST is an annual Navigation Warfare Systems Command (NAVWAR) GPS testing event conducted by the U.S. Air Force 746th Test Squadron at White Sands Missile Range in New Mexico. The NAVFEST scenarios provided realistic electronic warfare conditions for participants to test equipment and technologies in GPS challenged and denied scenarios. Detailed equipment configurations, data collection descriptions, and analysis are provided in this report.

PNT Pilot Project Findings and Recommendations

The PNT Pilot Program focused on MARAD's Ready Reserve Force vessels and provided findings and recommendations that:

1. Identified specific shipboard systems used in MARAD's Ready Reserve Force vessels that consume or generate PNT information.
2. Identified a complementary PNT data source suitable for maritime operating environments to diversify acquisition of PNT information from non-GPS services by conducting operational testing and data collection.
3. Detected the disruption and manipulation of PNT services in actual marine and simulated environments through successful testing of shipboard PNT equipment in both laboratory and real-world operational settings, under normal and disrupted/manipulated conditions.
4. Provided MARAD with a framework for risk-based management of shipboard systems, networks, and assets dependent on PNT services based on the identification of equipment that provides protection (i.e., shields and/or defeats manipulation) and augmentation (i.e., utilizes complementary PNT signals), and sharing that information with key stakeholders.

In alignment with the actionable objective of the PNT Pilot Program, these findings are suitable for application in the maritime environment and should be considered as capabilities that can be incorporated into a system solution for satisfying PNT resiliency requirements. The protective and diversifying solutions are effective and commercially available.

The primary recommendation for improving PNT resilience is to protect existing or new Global Navigation Satellite System (GNSS) equipage in the RRF with controlled reception pattern antenna (CRPA) technology. Commercial solutions such as the Hexagon GAJT 7 or GAJT 4 antennas can protect GNSS-derived PNT information with no changes to any other shipboard equipment. CRPAs display particular effectiveness at mitigating jamming attacks as well as some spoofing attacks. Further, a dual antenna/receiver pair can be used to detect a spoofing attack through self-differential means. This configuration can optionally serve the detect-and-characterize function (power and direction of arrival) on interfering signals.

While the solutions and recommendations provided in this document are tailored to the focused work on the RRF, the operational impact findings from the CRUCIBLE archive give an initial indication that such protect-and-diversify solutions are likely applicable to a much wider cross-section of maritime vessels and operations. Thus, the USDOT PNT Pilot Program can serve both as an early pathfinder for PNT resilience in the RRF and as a template for effective application of PNT resilience to many operational maritime environments.

1. Introduction

On February 12, 2020, Executive Order (EO) 13905 "Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services" was signed.[1] The goal of the order is to foster responsible use of positioning, navigation, and timing (PNT) services by critical infrastructure owners and operators (including the transportation sector) to strengthen national resilience. EO 13905 seeks to ensure the disruption or manipulation of PNT services does not undermine the reliability or efficiency of critical infrastructure by:

- Raising awareness of the extent to which critical infrastructure depends on PNT services;
- Ensuring critical infrastructure can withstand disruption or manipulation of PNT services; and
- Engaging public and private sectors to promote responsible use of PNT services.

1.1 USDOT PNT Pilot Program, Phase 1

1.1.1 Summary

In alignment with the objectives of the PNT Pilot Program, the maritime environment was identified as having important critical infrastructure suitable for the testing of PNT resiliency requirements. Working with the Maritime Administration (MARAD), the team from the Volpe National Transportation Systems Center (Volpe Center) performed operational testing of jamming-resilient equipment on the Fast Sealift Ship SS *Antares* and supported an inspection of a similar *Algol*-class vessel, the SS *Denebola*, for preliminary assessment of system design, equipment installation, and vessel operations. The Program Team conducted interviews with MARAD personnel, ship's crews, vessel management services, and equipment vendors, to inform the development of a robust testing strategy. Following the preliminary assessment, the Program Team coordinated three technical data-collection efforts to identify vulnerabilities, assess threats, and consider PNT hardening technologies that could serve to mitigate the operational impacts of jamming and spoofing:

1. SS *Antares* static RF environment survey and Turbo Activation dynamic RF survey.
2. Participation in Global Navigation Satellite System Jamming and Spoofing Live-Sky Event (GET-CI).
3. Inclusion of complementary PNT (CPNT) technology to evaluate low Earth orbit (LEO) PNT services with Government furnished equipment.

[1] Donald Trump, Executive Order 13905, "Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services," February 12, 2020, 85 FR 9359, https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing.

1.1.2 Results & Recommendations

The PNT Pilot Program Phase I focused on MARAD's Ready Reserve Force (RRF) vessels and provided findings and recommendations that:

1. Identified specific shipboard systems used in MARAD's Ready Reserve Force vessels that consume or generate PNT information.
2. Identified a complementary PNT data source suitable for maritime operating environments to diversify acquisition of PNT information from non-GPS services by conducting operational testing and data collection.
3. Detected the disruption and manipulation of PNT services in actual marine and simulated environments through successful testing of shipboard PNT equipment in both laboratory and real-world operational settings, under normal and disrupted/manipulated conditions.
4. Provided MARAD with a framework for risk-based management of shipboard systems, networks, and assets dependent on PNT services based on the identification of equipment that provides protection (i.e., shields and/or defeats manipulation) and augmentation (i.e., utilizes complementary PNT signals), and sharing that information with key stakeholders.

The protective and diversifying solutions referenced above are effective and commercially available. The results described in the USDOT PNT Pilot Program Phase I Report demonstrate that these solutions should be further evaluated with respect to the full set of operational requirements for a platform such as MARAD Ready Reserve Force vessels. From the PNT Profile perspective, the USDOT PNT Pilot Program findings lead to two key recommendations for improving PNT resilience.

1. Protect existing or new GPS equipage in the RRF with controlled reception pattern antenna (CRPA) technology. Solutions such as the Hexagon GAJT-410ML can protect GPS-derived PNT outputs with no further changes needed to shipboard equipment. When the GPS receiver is paired with the GAJT CRPA nulling antenna, it will be able to reject jamming signals and exhibit enhanced resiliency to spoofing attacks. This solution, in conjunction with software, has the capability to further serve as a detect-and-characterize function (power and direction of arrival) on interfering signals. Additionally, a dual antenna/receiver pair (or larger antenna array) can be used to detect and locate spoofing attacks through self-differential means.
2. Augment shipboard equipage in the RRF with LEO-based timing and, potentially, positioning technology. Solutions such as theiridium STL/SHOUT service can be added with minimal integration (i.e., human in the loop procedures) to provide both a check of GPS-based PNT outputs and a complementary PNT source for ship management equipage.

While these recommendations are tailored to the focused work on the RRF, the operational impact findings from the Department of Transportation GPS Anomaly Events database archive give an initial indication that such protect-and-diversify solutions are applicable to a much wider cross-section of maritime vessels and operations. Thus, the USDOT PNT Pilot Program can serve both as an early pathfinder for PNT resilience in the RRF and as a template for effective application of PNT resilience to many operational maritime, and potentially non-maritime, environments.

1.2 USDOT PNT Pilot Program, Phase II

The Volpe Center, in coordination with the MARAD Office of Safety, conducted at-sea testing of several controlled reception pattern antennas, as recommended in the MARAD PNT Pilot Program, Phase I Report. Testing was conducted aboard the *Cornhusker State* (T-ACS-6), a crane ship in ready reserve for the U.S. Navy, stationed in Newport News, Virginia under operational control of the Military Sealift Command (MSC). The goal of these sea trials was to evaluate how well the protective technologies perform during periods of intentional manipulation and unintentional interference or outages to GPS.

To accomplish this, the vessel traveled to areas known for GPS disruptions (e.g., Suez Canal). In this report, the Volpe Center will document the results and effectiveness of the technologies against any encountered threats and make recommendations for implementation. Volpe Center activities include:

- Stakeholder engagement with vessel owners and operators
- Test plan development
- Research and market survey of non-CRPA anti-jamming and anti-spoofing technology
- CPNT technology research/pre-assessment
- CRPA and other jamming/spoofing mitigating technology procurement
- Lab-based dry runs of simplified scenarios that validate and debug the test approach
- Equipment setup and installation on test vessels(s)
- Sea trials with installed technology-under-test, truth systems, and supporting data collection
- Processing and analysis of collected data
- Submission of a final report
- Work with MARAD on implementation of solutions on RRF vessels

2. NIST Foundational PNT Profile

In addition to development and implementation of a PNT Profile Pilot Program, EO 13905 seeks to protect the national and economic security of the United States from the disruption or manipulation of systems that form or use PNT data and information vital to the functioning of critical infrastructure and technology-based industries. The EO directs the Department of Commerce to develop PNT profiles that address the four components of responsible use of PNT:

1. Identify systems that use or form PNT data.
2. Identify PNT data sources.
3. Detect disruption and manipulation of the systems that form or use PNT services and data.
4. Manage risk regarding responsible use of these systems.

National Institute of Standards and Technology (NIST) Internal Report 8323 (NISTIR 8323), published in February 2021, Revision 1 2023, applies the NIST Cybersecurity Framework (CSF) to the PNT ecosystem.[2] The NIST Foundational PNT Profile (referred hereafter to as the "PNT Profile") provides a flexible framework for users of PNT services to manage risks when forming and using PNT signals and data.[3] The PNT Profile can be applied to all organizations that use PNT services, regardless of the level of familiarity or knowledge they have with the CSF. Organizations that have fully or partially adopted the CSF, or who have not yet adopted it, can benefit.

Use of the PNT Profile is voluntary and entirely recommendatory in nature and intended to be a foundational set of guidelines. It does not represent any enforceable regulations, define mandatory practices, establish compliance standards, nor carry any statutory authority. Sector Risk Management Agencies and other entities may wish to augment or further develop their own PNT cybersecurity efforts via full or partial implementation of the PNT Profile recommended practices. Any implementation of NIST's recommendations will not necessarily protect organizations from all PNT disruption or manipulation but rather gives each organization risk-based management decision support in the context of their own cyber ecosystem, architecture, and components. The PNT Profile's strategic focus is to supplement existing resilience measures and elevate the postures of less mature initiatives.

2.1 Intended Use

The PNT Profile is a flexible tool that can be used by an organization to help meet mission and business objectives that are dependent on the use of PNT services. The PNT Profile can help organizations determine risks based on their assessments of the potential impacts of manipulation or the disruption of

[2] "Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services," February 2021, Gaithersburg: National Institute of Standards and Technology, https://doi.org/10.6028/NIST.IR.8323.

[3] The text in much of Section 2 of this report highlights the rationale behind the adoption of NISTIR 8283, as described by NIST and adapted for the purposes of this report.

PNT services to their own business and operational objectives, and to prioritize cybersecurity activities based on those objectives. Additionally, the PNT Profile can be used to guide organizations as they identify areas where standards, practices, and other guidance could help manage risks to systems that use PNT services. An organization can use the PNT Profile in conjunction with its own systematic process for identifying, assessing, and managing risk. NIST acknowledges the existing efforts being undertaken by individual entities to address the responsible use of PNT services in their sectors, and the PNT Profile is intended to complement—not replace—those efforts. NIST also encourages the development of sector-specific guidance if more specific risk-management efforts are required.

2.2 Cybersecurity Risk Management

Cybersecurity risk management is the ongoing process of identifying, assessing, and responding to risk as related to an organization's mission objectives. To manage risk, organizations should understand the likelihood that a cybersecurity event will occur and consider the potential impacts of that event. An organization should also consider statutory and policy requirements that may influence or inform cybersecurity decisions.

The PNT Profile supports and is informed by the cybersecurity risk management process. Using the PNT Profile, organizations can make more informed decisions—based on business needs and risk assessment—to select and prioritize cybersecurity activities and expenditures that help identify systems dependent on PNT, identify appropriate PNT sources, detect disturbances and manipulation of PNT service, manage the risk to these systems, and ensure resiliency to their user base.

The PNT Profile also provides a starting point from which organizations can tailor their approach to manage risk to their PNT services and data. A customized approach provides the most appropriate measures, processes, and prioritization of resources for the reliable and efficient functioning of critical infrastructure applications. Organizations can use the PNT Profile in conjunction with existing risk management processes. The PNT Profile assumes that the organization implements cybersecurity risk management processes and provides additional risk management considerations specific to PNT.

2.3 PNT Profile Framework Description

Created through collaboration between industry and Government, the NIST CSF provides prioritized, flexible, risk-based, and voluntary guidance based on existing standards, guidelines, and practices to help organizations better understand, manage, and communicate cybersecurity risks.[4] Although it was designed for organizations that are part of the U.S. critical infrastructure, many other organizations in the private and public sectors (including Federal agencies) may use or implement the NIST CSF. The framework consists of three main components:

[4] "Cybersecurity Framework," National Institute of Standards and Technology, web, https://www.nist.gov/cyberframework.

1. The **Framework Core** provides a catalog of desired cybersecurity activities and outcomes using common language. The Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management process.
2. **Framework Implementation Tiers** provide context for how an organization views cybersecurity risk management. The Tiers help organizations understand whether they have a functioning and repeatable cybersecurity risk management process and the extent to which cybersecurity risk management is integrated with broader organizational risk management decisions.
3. **Framework Profiles** are customized to the outcomes of the Core to align with an organization's requirements. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

The NISTIR 8323 Foundational PNT Profile defines the five Framework Core functions as follows: [5]

1. <u>Identify</u> – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational to the effective use of the Cybersecurity Framework, enabling an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and business needs.
2. <u>Protect</u> – Develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services. The activities in the Protect Function support the ability to limit or contain the impact of a potential PNT cybersecurity event.
3. <u>Detect</u> – Develop and implement the appropriate activities to sense and identify the occurrence of a cybersecurity event. The activities in the Detect Function enable the timely discovery of PNT cybersecurity events.
4. <u>Respond</u> – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The activities in the Respond Function support the ability to contain the impact of a potential PNT cybersecurity event.
5. <u>Recover</u> – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations to reduce the impact of a PNT cybersecurity event.

When considering the five functions, **Identify** and **Protect** can further be characterized as taking place before a PNT cybersecurity event or attack, **Detect** and **Respond** during a cybersecurity attack, and **Recover** either during and/or after a cybersecurity attack (see Figure 1). When considered together, these functions provide a high-level, strategic view of the life cycle of an organization's management of PNT cybersecurity risk.

[5] NISTIR 8232, p. 6.

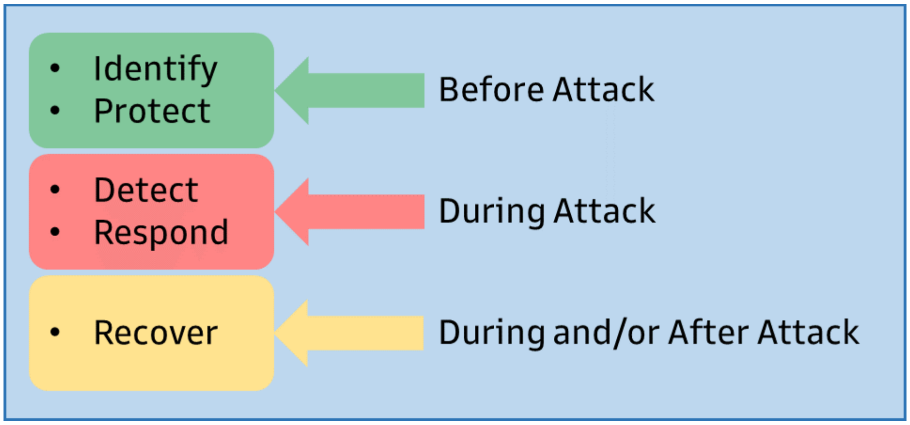


Figure 1: Five Functions within the NIST PNT Profile

2.4 MARAD PNT Profile

Phase II of the PNT Pilot Program kept focus on the Protect function by evaluating the performance of anti-jam technology in real-world operational conditions. The anti-jamming solutions tested during Phase II CRPA antennas and similar in-line devices that are available on the commercial market. Although extensive market research has also been performed of emerging receiver-level GNSS hardening technologies and CPNT technologies, the focus of the Phase II evaluation has been on-easy-to-integrate, minimally intrusive, mature, readily available, and cost-effective solutions that MARAD may incorporate in their near-term procurement cycles for technical upgrades. These technologies and the threats that are driving their importance are discussed in the following sections.

3. Jamming and Spoofing

GNSS signal jamming, whether intentional or unintentional in origin, is defined as a denial or degradation of GNSS signal reception resulting from radio frequency interference. The term *spoofing* in GNSS is much more nuanced and complex. Spoofing is caused by radiofrequency (RF) waveforms that mimic true signals in some ways, but deny, degrade, disrupt, or deceive a receiver's operation when they are processed. Spoofing may be unintentional, such as effects from the signals of a GNSS repeater, or they may be intentional and even malicious. There are two classes of spoofing:

- Measurement spoofing introduces RF waveforms that cause the target receiver to produce incorrect measurements of time of arrival or frequency of arrival, or their rates of change.
- Data spoofing introduces incorrect data to the target receiver for its use in the processing of signals and the calculation of PNT.

Either type of spoofing can cause a range of effects, from incorrect outputs of PNT to receiver malfunction. The onset of these effects can be instantaneous, intermittent, or delayed, and it is possible for effects to continue even after the spoofing has ended.

This report will be referring to and evaluating equipment performance against jamming and measurement spoofing. Since GNSS receivers are designed to lock onto the strongest signals available, this type of spoofing occurs when a bogus GNSS signal overpowers and replaces the authentic or intended GPS signal. Measurement spoofing can be intermittent and subtle or obvious and extreme. For example, it may be easy to detect these spurious signals if your GNSS is suddenly indicating a position hundreds of miles from where you were a few minutes ago or if there is a noticeable time shift.

Alternatively, the spurious signals may only appear intermittently, and subtlety deviate from the authentic signal(s) so that the intended navigation shifts so slowly that the deviation is not noticed until the spoofing target is already off course. Since a higher power level signal is associated with both jamming and signal spoofing, the mitigating equipment tested in this evaluation is based on technology that detects power of arrival (PoA). Some devices also incorporate the ability to detect a pulsating signal and/or angle of arrival (AoA), which is necessary to identify the direction from which the spurious signal was transmitted from. This capability allows for the unwanted signal(s) to be rejected and removed from the solution. However, even with these sophisticated capabilities and devices to enhance the resiliency of GPS, there are existing and emerging threats that are capable of subverting these protective technologies.

3.1 Data Spoofing: A Rapidly Evolving Landscape

As is the case in all facets of cybersecurity, malicious actors are typically one step ahead of those charged with protecting our information systems. In the GNSS realm, data spoofing is an increasingly sophisticated, varied, and potentially damaging form of spoofing that is becoming more prevalent and harder to detect. Data and range spoofing occurs when a spurious GNSS signal is received and processed by a GNSS receiver in lieu of the authentic, intended signal. What differentiates data spoofing is both how evasive to detection and invasive to GPS systems it can be.

Data spoofing attacks are difficult to detect because the spoofing signals may not initially deviate from the authentic signals in terms of data, ranging, timing, and power. The spurious signals may evade detection and take over a system by initially providing correct positioning and timing data and only deviate slightly over time. They may also be transmitted only intermittently so that most of the signals being received are legitimate GPS satellite signals. This means that detection may not occur until significant navigation or timing errors have already occurred.

Data spoofing signals may be actual GNSS signals that have been captured, modified and retransmitted or they may be completely synthesized. Transmission may originate via ground stations or aerial platforms so that PoA and AoA may not be sufficient data points to detect an attack. These disguised and invasive signals can, in effect, act as viruses and cause infected GNSS systems to critically fail or "brick," necessitating complete shutdown, factory repairs and/or equipment replacement. Thus, the typical strategy of detecting and removing the unwanted signal(s) from a mix of legitimate and spurious signals may not be enough to avert significant consequences.

3.2 Data Spoofing: Current and Emerging Countermeasures

Although data spoofing presents serious threats and challenges to resilient PNT, there are a number of solutions currently emerging that will serve as important countermeasures. To ensure data validity checking, the equipment should monitor signal strength as well as cross-reference and analyze location data. Any proposed countermeasures should be designed to be compliant with IS-GPS-200M recommendations. Ultimately, a multi-tiered approach to mitigate data spoofing threats will likely be required to ensure PNT resiliency in the present and future.

1. Using a small network of receiver nodes, a time difference of arrival (TDoA) calculation can be performed to find out where a spurious signal originated. GPS satellites send out a pseudo-random code. Receivers on the ground interpret this code to determine how long the signal takes to reach them, and therefore how far from each satellite they are. Data spoofing can be detected if the signal is determined to be transmitted from relatively near the receiver. This technology also allows for the location of the transmitter to be determined, which is the first step to shutting down the source.
2. Authentication of GNSS signals through use of the Galileo OSNMA (Open Service Navigation Message Authentication) and E6 signals. This allows for the use of OSNMA-enabled receivers that can authenticate the complex keys generated at the satellite level. This technology has similarities to the GPS military code. A civilian authentication mechanism is currently under development for GPS called Chimera.
3. Signal authentication via novel approaches such as a dual-polarized antenna. This hardware and accompanying algorithms, under development by Septentrio, exploits the similarities in polarization of spoofed satellites to identify the spoofed signals from authentic signals.

4. CPNT equipment and services diversify and support a navigation system by providing non-GPS dependent positioning and/or timing inputs. Such information can serve as an important cross-check against anomalies detected in the GPS solution. Depending on the level of interoperability and integration, the PNT system may automatically switch over to the CPNT solution once the GNSS solution has been determined to be compromised. CPNT is discussed in detail in the following section.

4. Complementary Positioning, Navigation, and Timing (CPNT) Technology Survey

When evaluating potential PNT solutions, the technology vendor, service provider, and end-user are important considerations. Wide area PNT resources have primarily been delivered through a domain of Government-owned and operated GNSS satellite constellations that are generally in medium Earth Orbit (MEO), such as GPS (United States), Galileo (European Union), GLONASS (Russia), and BeiDou (China). Complementary PNT (i.e., systems capable of backing up and/or augmenting GNSS) have largely been explored by the private and academic sectors. Five high level categories of complementary PNT technology are:

1. On-board sensors—equipment that supports GNSS by providing augmentation or alternative PNT inputs.
2. Space-based PNT (e.g., low Earth orbit [LEO])—satellite timing and location data from an orbit in space about 25 times closer than GNSS.
3. Terrestrial wireless infrastructure—RF transmitting technologies that operate within a localized environment, defined region, or range, which require ground-based equipment. Broad coverage may be realized with support operations across multiple regions however, this paradigm is not global in nature.
4. Signals of opportunity (SOOP)—location data innovatively derived from radio signals, both cooperative and non-cooperative, not originally designed for PNT end-uses.
5. AI-enhanced mapping and image recognition—advances in mapping technology and complex algorithms supporting the rapid matching of images with map databases have quickly enabled the technological maturity of this technology into commercial operations.
6. Network time transfer—precise timing data from synchronized clocks across a high-speed computer network.

Based on the CPNT categories described above, the following offers a snapshot of the breadth of complementary PNT technologies, both generic and proprietary, across a broad range of technology readiness levels (TRL), that may be part of a multi-layered resiliency plan for PNT across all modes of transportation and critical infrastructure.

4.1 On-board Sensors

On-board sensors/equipment, computing, and software make up the largest and broadest category of CPNT and includes both general concepts, as well as proprietary technologies.

4.1.1 Inertial sensors (IMU, INS)

An inertial navigation system (INS) relies on an inertial measurement unit (IMU) to track position and orientation relative to a known starting point. INS/IMU employ a combination of sensors such as, accelerometers and gyroscopes to estimate position, velocity, and orientation, and can provide continuous navigation information even in GPS-denied environments (dead reckoning), making them useful for ships operating in areas with limited satellite coverage. Providing high short-term accuracy and robustness against interference, many modern GPS receivers integrate IMUs to harden the positioning solution; however, accuracy degrades, sometimes rapidly, as errors accumulate, so a valid position must be provided to recalibrate the INS.

4.1.2 Sensor Fusion

Sensor fusion is an integral process rather than a specific CPNT solution. Aiding through sensor fusion, such as LiDAR/camera or GPS/IMU, takes inputs from two or more sensors to improve the reliability of outputs to provide relative positioning (or absolute once you have a space mapped) using simultaneous location and mapping (SLAM) algorithms. The specific type of, and quantity, of sensors used varies by use case and the complexity of the fusion algorithm; however, the specific sensors chosen will ideally improve each other's performance by providing supporting data. The development of robust sensor fusion algorithms is complex, and these techniques are processing-intensive which increases onboard hardware dependencies. Sensor fusion encompasses a huge variety of sensor types. Whether explicit or not, sensor fusion and associated algorithms are typically a critical part of the underpinnings of various CPNT solutions. Sensor fusion has applicability to all transportation modes.

4.1.3 AI-based Recognition of Real-Time Visual Imagery

A powerful enabling technology, AI-based deep/machine learning is an increasingly important tool in enabling sensor fusion to reach its full potential, particularly regarding visual sensor data which requires complex interpretation. Skyline Nav AI has developed technology that fuses visual sensor data, AI, and digital elevation maps (DEM) and developed algorithms to recognize skyline and horizon features. This capability has been tested in richly featured as well as sparsely detailed settings and demonstrated the capability to geolocate, even with limited field of view. Another proprietary solution, Visual Positioning System (VPS) from Brooklyn, NY based Vermeer, leverages AI, and full motion video (FMV). VPS employs a global geo-rectified 3D map database that feature-matches the platform's FMV feed. VPS software is sensor and system agnostic; it can be applied to an existing vehicle/fleet and work in conjunction with GPS, LIDAR, or on its own.

Advantages of fusing AI and imagery data include full functionality in GNSS-denied environments, suitability in dense urban environments, immunity to jamming and spoofing (i.e., RF independent), wide array of potential end-uses, and purported accuracy of less than 5 meters. This technology may also function as a GPS resiliency complement, dead reckoning calibration source, or backup navigation system. A key disadvantage is that systems operating in the visual range may not be suitable for all weather conditions, especially where visibility is reduced. Nighttime performance will also be degraded, depending on ambient conditions. Featureless environments may also be problematic. Current usefulness may be limited in cases where image data includes near-field obstructions to horizon/skyline/permanent features. Additionally, availability could be limited by gaps in input data (e.g., gaps in reference mapping databases or deficiencies in image matching algorithms).

4.1.4 Long Wave Infrared (LWIR)

Closely related to AI-based recognition of real-time imagery, LWIR techniques leverage the inherent strengths of LWIR versus visible spectrum cameras. Although sensor fusion, image matching, and localization algorithms vary from effort to effort, LWIR is a rapidly developing space that harnesses the power of AI to perform complex feature recognition and image matching in real-time applications.

The U.S. Army Combat Capabilities Development Command (and Leidos) have successfully tested vision-based navigation (VBN) that employs street level image matching (SLIM) to correlate LWIR images to compressed satellite imagery databases. VBN provides absolute position fixes and has been tested on military aircraft at various speeds and altitudes. VBN has demonstrated significant improvement over unaided embedded-GPS-inertial (EGI) performance and consistently provided accurate fixes during testing, even at very low altitudes. Leidos has expanded testing to military ground vehicles with Ground Vehicle Vision-Aided Nav (GVVAN) that leverages improved image matching algorithms. Honeywell has developed a similar system called Honeywell Vision Navigation that uses high resolution geo-referenced and orthorectified imagery with terrain database which correlates position using sensor inputs, including IR cameras and IMUs.

Thales Defense and Security Inc. has done extensive research trying to improve nighttime and indoor performance of LWIR and INS. Although performance gains yielded from improved algorithms have been made, LWIR and daylight cameras have inherent strengths and weaknesses brought forth by lighting conditions and other environmental factors. LWIR performance suffers indoors and in open environments (e.g., parking lots), whereas visible spectrum cameras perform poorly at night or in obscured visibility conditions. Daytime performances are similar. Future work will integrate a novel camera design and synchronized LWIR to address these performance gaps. As is the case with AI-based visual spectrum imagery recognition, availability could be limited, e.g., LWIR position updates do not have 100 percent reliability due to gaps in reference mapping databases or deficiencies in image matching algorithms. Open sea marine applicability may be limited however due to inherent lack of discernable features on the horizon.

4.1.5 Ground Penetrating RADAR (GPR)

Although GPR was first developed over twenty years ago, it has largely been used in niche applications such as archaeology, structural engineering assessment, and utility location. However, due to GPR's unique capabilities to identify underground features, it has gained significant traction as a source of complementary PNT over the last decade. GPR systems work by sending a pulse of electromagnetic radiation into the ground and measuring reflections that originate from scattering below the surface.

Reflections occur at the boundaries between objects of different electromagnetic properties (e.g., the interface between soil and rocks, roots, or man-made features).

GPR sensor data in conjunction with AI-enhanced software can create a detailed image of the subsurface environment. Nearly all discrete objects and soil features are captured—if they are not significantly smaller than the wavelength of the radar frequency and there is sufficient dielectric contrast with the surrounding soil. The premise of GPR localization is that these subsurface features, as represented in GPR data, are sufficiently unique, permanent and impervious to environmental phenomena (e.g., snow and fog) to permit their use as identifiers of the precise location where they were collected. GPR, like other technologies, may be enhanced by fusing with additional sensors, such as GPS, LiDAR, cameras and IMUs.

GPR penetration may not be possible in certain types of unique terrain, such as on metal bridges or similar surfaces. GPR cannot tell the composition of a target. It can only tell if there is a contrast between the target and the surrounding area. Water reflects the signals differently from materials in the ground, which can mask the presence of utility lines or other objects of interest. Depth range of GPR is limited by the electrical conductivity of the medium, the transmitted center frequency, and the radiated power. Applicability for future marine applications is unlikely.

4.1.6 Quantum Technology

Quantum technology advancements are a key enabler to improved sensing capabilities to develop the ultra-sensitive sensors driving new CPNT solutions. Inertial navigation company iXblue is leading a European Space Agency consortium to develop a compact 3-axis cold-atom interferometer (CAI), aimed for use aboard ships, aircraft, and fixed sites. A more sensitive CAI gravimeter would provide a higher frequency of gravity gradient measurements, producing improvements in map matching and could employ SLAM techniques developed for robotics navigation, where maps are created at the same time movement is tracked. This could be used both on a dead reckoning basis—to accurately tally all subsequent movements relative to a starting point, without the gradually accumulated drift of legacy inertial sensors—and to fix positions by matching local gravity measurements to a detailed gravity map. Advances in quantum computing are enabling the development of the first-generation of atomic clocks that fit on a computer chip; however, applying quantum technology advances to CPNT will be a gradual process.

4.1.7 Gravity Aided Navigation

The Office of Naval Research (ONR) has developed a gravimeter—Gravity-Aided Inertial Navigation System (GAINS)—that uses laser-cooled rubidium-87 to sense inertial forces. The gravimeter is easily transportable with quick start-up, capable of operating under ship dynamics, and without moving parts or cryogenic components. These features provide a clear path for integration into a low-SWaP gravity-aided INS. A gravimeter in conjunction with co-sensors enables operation through multi-axis platform dynamics. Under static laboratory conditions, GAINS demonstrated excellent measurement precision and long-term stability during continuous operation of several weeks.

To demonstrate real world operability, two at-sea test campaigns were conducted in 2022. High precision INS outputs aided in recovering gravity anomaly under ship dynamics and provided position for gravity map comparisons. The gravimeter demonstrated greater than 99 percent uptime throughout both test campaigns, even under sea states far exceeding the expected dynamics. Initial results are promising for marine applications; however, further testing and development are required.

4.1.8 Magnetic Navigation

A partnership between the U.S. Air Force Research Lab and MIT Lincoln Labs has successfully tested a prototype navigation system that uses mapping of the Earth’s magnetic field to detect variations and determine position. The system is called MagNav and leverages advancements in machine learning and AI to interpret changes in the Earth’s magnetic field and parse out noise from magnetic interference from the test aircraft and other sources. Position is determined by comparison to a known magnetic map.

Raytheon has extended testing to maritime vessels, although the relatively slow speeds and large amounts of iron in large seagoing vessels create challenges in terms of parsing out noise and detecting subtle magnetic changes in the environment. The Raytheon work further reinforces the need for a new approach to magnetic mapping. Their work has led to research in a technique called simultaneous calibration and mapping (SCAM). Penn State Applied Research Lab has taken a slightly different approach to leveraging the Earth’s magnetic field by using magnetic particle filtering as a means to reduce error and drift in INS measurements.

Key advantages to magnetic navigation include wide area coverage, terrain independent performance, availability in all weather conditions and all times of day, and strong immunity to jamming and spoofing. Disadvantages include the need for large scale, low altitude, aeromagnetic surveying, and advances in such techniques, to create detailed magnetic maps of all areas of interest. Initial testing also indicates the best performance at lower altitudes (for aircraft) and higher speeds (for any vessel). Current magnetic maps used for geological interpretation of specific locations are insufficient. Maps must also be regularly updated, as the Earth’s magnetic field is constantly changing. Limited MagNav testing indicates accuracy around 1 kilometer, a significant downgrade from GPS, although still suitable for many end-uses where visual navigation or landmark recognition guide a vessel to a final destination. Advancements to aeromagnetic surveying in terms of cost and efficiency must be realized before the technology is viable on a large scale.

4.2 Space-based PNT

4.2.1 Low Earth Orbit (LEO) Satellite Constellations

Low Earth orbit (LEO) satellite constellations typically consist of small-sized or miniaturized satellites with potential for worldwide coverage, 2D/3D positioning, and precise timing in one system. Such satellites have low-to-moderate costs of building, launching, and maintenance as compared to medium Earth orbit (MEO) satellites, such as those used in GNSS. Small dimensions, versatility, short development period, high return-to-cost potential, high speed, and proximity to the Earth, make LEO systems good candidates for PNT solutions which may be stand-alone or complementary to MEO/GNSS.

LEO systems have different operational features and performance characteristics than MEO systems, such as increased signal strength, enhanced security, and high speed that produce rapid geometry changes and faster convergence times. LEO satellites have a much smaller instantaneous coverage area than those in MEO, hence many more satellites are required for robust dilution of precision and global coverage. However, this may be an advantage in noisy or jammed environments because beams from LEO can achieve high power signals over small areas. Smaller LEO constellations may also be used to augment MEO constellations and improve trust in PNT reporting.

Some LEO constellations are operational, while others are still in development. "Satellite Time and Location" (STL) from Iridium leverages their constellation and is currently operating at a high TRL, with a multi-year track record of providing reliable service to customers. Similarly, Parsons Government Services has partnered with Globalstar to create wide availability for LEO PNT services. Xona is developing lower-cost satellites using off-the-shelf components with high-power signals to reach indoors; however, the service is not currently operational. Geodetics has focused on improving some of the shortcomings of LEO PNT by targeting research on algorithms, accuracy assessments, developing a position/velocity estimation framework, outlier detection and improving multi-sensor fusion. TrustPoint is building out a C-band constellation which purports to improve performance over legacy LEO providers.

4.2.2 Cosmic Rays: Muometric Positioning System (muPS)

The muon is one of the fundamental subatomic particles, the most basic building blocks of the universe as described in the Standard Model of particle physics. Muons are similar to electrons but weigh more than 207 times as much. Muons from cosmic rays fall equally across the Earth and travel at the same speed regardless of the matter that they traverse. They are capable of penetrating water, buildings, and tunnels, and can travel kilometers into solid rock. While muon imaging has been used previously for archeological research, a team from Japan has recently developed and performed initial testing on a muon-based positioning system.

As muons zip through the gas, they collide with the gas particles and emit a telltale flash of light (scintillation), which is recorded by the detector, allowing scientists to calculate the particle's energy and trajectory, similar to X-ray imaging or ground-penetrating radar, except with naturally occurring high-energy muons rather than X-rays or radio waves. The muon system relies on four muon-detecting reference stations above ground serving as coordinates for the muon-detecting receivers, which are deployed either underground or underwater.

The most recent iteration—the Muometric Wireless Navigation System, or MuWNS—is completely wireless and uses high-precision quartz clocks to synchronize the ground stations with the receiver. Taken together, the reference stations and synchronized clocks make it possible to determine the coordinates of the receiver. Although the current system can only operate in a local test environment, results are promising with accuracies between 2 meters and 25 meters and a range of 100 meters. Improvements to the clock and synchronization between reference stations and receivers will yield improved results however the technology is still in early development.

4.3 Terrestrial Wireless Infrastructure

4.3.1 Terrestrial RF Networks

Several companies have developed technology that employs scalable transmitter/transceiver networks with proprietary RF signals and receiver user equipment. Although frequencies and signal components vary, these networks function much like a ground-based version the GPS constellation. Thus, the number of transmitters, their geometry relative to the receiver, and clear lines of sight are of utmost importance when maximizing positioning accuracy. Locata and NextNav are two leaders in this CPNT field, which offer high TRL positioning, navigation, and timing services. Although terrestrial wireless RF systems are largely robust and GPS independent, they require local infrastructure and currently do not meet the needs of open sea navigation.

4.3.2 eLORAN (Enhanced Long-Range Navigation)

eLORAN is an enhanced version of the original Loran-C system. eLORAN is a very low frequency radio navigation system, whose signals are very difficult to interfere with and disrupt. It uses terrestrial-based radio signals to provide positioning and timing information and is supplemented by a land-based network of communication nodes that enhance resiliency. eLORAN offers a backup option to GPS, with range limitations. At least three eLORAN transmitters are required to derive a positioning solution, including for deep sea positioning capability. However, only one eLORAN transmission is required for precise timing applications.

Current efforts by Hellen Systems and UrsaNav have demonstrated the effectiveness of eLORAN as a robust timing solution. The relatively high cost of building and maintaining eLORAN transmitter stations is a drawback but modern equipment has made advances in cost efficiency. Use cases may include maritime port navigation and precise timing applications.

4.3.3 Terrain Aided Navigation

Sandia National Laboratories has updated legacy terrain-aided radar algorithms, such as originally designed for Tomahawk missiles in the 1980s, which did not perform well at high altitudes. Trusted Inertial Terrain-Aided Navigation (TITAN) uses minimum-range prescribed Doppler (MRPD) measurements for multilateration of the position of the receiver using three or more range measurements from overflown terrain features. Using MRPD measurements, TITAN extracts and correlates the minimum range contour. Radar measurements are blended with an inertial measurement system and a local DEM model with a non-linear Kalman filter.

Current state of development and testing indicates approx. 20-meter position accuracy. However, unmodeled errors degrade the navigation solution. Synthetic data indicates that approx. 5-meter accurate solution is possible. Further development is required and will include full INS and radar integration, enhanced modeling and mitigation of measurement errors, platform testing and real-time demonstration of capabilities. This technology is not optimized for open water environments and is an unlikely candidate for marine applications.

4.4 Signals of Opportunity (SOOP)

These technologies leverage radio signals not intended for navigation. For example, they derive location information from signals such as LTE, Wi-Fi, and Bluetooth transmitted from active devices. Sandia National Labs, among other organizations such as the USDOT University Transportation Center of Excellence, has done extensive research and testing using signal emitters of various types and quality merged with direction finding (DF) arrays (interferometer) and SLAM algorithms for estimating position. The result is Simultaneous Localization and Mapping Based on RF Signals (SLMBRS). SLMBRS uses a Cubature Kalman Filter (CKF) for simultaneous localization and mapping to enable a real-time suitable navigation algorithm.

Signals of opportunity PNT strategies require specialized hardware that can acquire and process signals broadcast across the radio spectrum with a variety of digital waveforms. Some providers not only integrate multiple radio signals but also merge SOOP with other technologies to fine-tune horizontal location, and in some cases, provide a degree of vertical positioning. Opportunistic navigation requires a user to be in a signal-rich environment. For example, there are typically more terrestrial signals in a large city than in the middle of an ocean or other underserved region, thereby making SOOP an attractive solution in urban areas. Marine applicability could be found in a port environment but not on the open ocean. This approach is also limited to positioning end-uses because it does not provide timing information.

4.4.1 Self-Positioning Off Targeted Anti GPS Emitters (SPOTAGE)

SPOTAGE seeks to turn the tables on GPS jammers/spoofers by turning the spurious RF into signals of opportunity for navigation. SPOTAGE is being developed under a Naval Information Warfare Center (NIWC) Pacific (FY22) Innovation Program (IIP) for Rapid Prototyping. It is a low SWaP and cost, real-time augmenting positioning sensor system which leverages the Advanced Scalable Assured PNT (ASAP) sensor fusion system. It is supported by UHU Technologies UHU1000 GPS Threat Mitigation Hardware that provides GPS interference detection, threat angle of arrival (AoA) and uncertainty, anti-jam and anti-spoof nulling and output to ASAP, and that protects timing receivers with antenna disconnect.

Although currently in the prototype phase, SPOTAGE progressed rapidly from theory to demonstrated initial capability in less than two years and NIWC Pacific, via CRADA partnerships, is working toward developing the full capability. Next steps include on-going preparations for transitioning to targeted users and meeting their low SWaP and cost requirements and developing open architecture for joint partners to collaborate on CONOPS and operational testing.

4.5 Network Time Transfer

These technologies deliver precise timing by synchronizing clocks across a high-speed computer network, typically relying on Gigabit Ethernet or SONET. For example, Precision Time Protocol (PTP) solutions achieve clock accuracy in the sub-microsecond range. The White Rabbit Protocol (born out of research led by CERN) can deliver precise timing in the sub-nanosecond range. Network time transfer can be deployed worldwide but requires a high-speed connection to operate at any given location.

4.5.1 Optical Multilateration

NIWC Pacific has been conducting research and testing a CPNT system which uses optical transfer of timing signals to provide regional “GPS-like” PNT. The system uses free-space optics (FSO) to achieve tight beam divergence. Divergence and frequency may be optimized for mission and channel medium considerations. An optical network with regional coverage is attainable and has advantages over RF, which is easily interfered with. Optical communication equipment, transmitter (laser), receiver (photodiode), and multilateration algorithms are the key system elements. A time-to-digital converter (TDC) has sub-nanosecond accuracy. TDC uses a timing pulse in preamble to measure Time Received: Time Received – Time Sent = Time of Transmission. Multiple time measurements are required (4 to 7) for accurate position estimation. This technology is currently at a low TRL.

4.5.2 Time Over Fiber

As part of the DOT Complementary PNT Rapid Phase I effort, vendors are demonstrating resiliency with time over fiber technology. Safran’s resilient timing distribution system leverages the White Rabbit High Accuracy time transfer protocol to provide timing information from generation to the user equipment. Hoptroff has developed a resilient end-to-end precision timing service which connects to existing infrastructure. Microchip is demonstrating that time transfer over commercial fiber-optic networks using PTP can be reliably implemented.

4.6 Legacy Maritime CPNT Technology

4.6.1 Navigation Aids: RF Beacons or Buoys

These are devices that mark a fixed location and allow direction-finding equipment to determine a relative bearing, but instead of employing visible light, radio beacons transmit electromagnetic radiation in the RF spectrum. They are used for direction-finding systems on ships, aircraft, and other vehicles. Radio beacons transmit a continuous or periodic radio signal with limited information (e.g., an identification code or location on a specified radio frequency). Occasionally, the beacon's transmission includes other information, such as telemetric or meteorological data.

4.6.2 VDES (VHF Data Exchange System)

VDES is a communication system that operates on the VHF (very high frequency) maritime band. It combines data and voice communication with the potential to include positioning and timing services. VDES can be used to enhance navigation safety and provide an alternative means of position fixing.

4.6.3 Marine RADAR

Marine radars aboard ship include X band (8–12 GHz) and S band (2–4 GHz). These systems are used to detect other vessels, aids to navigation, and land obstacles, and provide bearing and distance for collision avoidance and navigation. In commercial and military ships, radars are integrated into a full suite of marine instruments including chart plotters, sonar, two-way marine radio, satellite navigation (GNSS) receivers, and emergency locators (SART). When a vessel is within radar range of land or special radar aids to navigation, the navigation system can calculate distances and angular bearings to charted objects and use these to establish arcs of position and lines of position on a chart.

4.6.4 High-Frequency Radar (HFR)

Radar technology operating in the high-frequency band is used to measure surface currents and provide real-time information on oceanographic conditions. While not a direct replacement for GPS, HFR can complement maritime navigation by providing valuable data on currents and waves.

4.7 Legacy Maritime Navigation Techniques and Tools

4.7.1 Celestial Navigation

Celestial navigation supports the navigation and location of vessels by geo-positioning techniques based on the observation of the sun, stars, and other celestial bodies. Using a sextant and chronometer you can derive a line of position (LOP) from celestial bodies. The variables measured to find the location are the observed angular height of the stars above the horizon (using the sextant) and the time (via the chronometer).

With the data contained in the nautical almanac, it is possible to determine the astronomical coordinates of the observed star. Knowing the coordinates of the observed star and the height above the horizon at which it was observed, the observer's position is within a circle whose center is located at the geographical point directly below the star. Any observer located at any point on that circle will observe the star with the same height above the horizon. The observer can therefore know that their position is somewhere on this circle.

In practice, the mathematical process to "reduce" the observation can be complex. It includes application of a series of corrections to the height observed with the sextant, to compensate for atmospheric refraction, parallax, and other errors. Once this is done, the observer must then solve a spherical triangle problem through mathematical and trigonometric methods. This can be done manually (using formulae and various tables) or through the use of celestial calculators and computers. With the advent of Loran and later GPS, widespread use of celestial navigation declined. However, many mariners are now rediscovering and returning to the use of celestial navigation as an alternative method in case of failure of the on-board electronic navigation system.

4.7.2 Magnetic Direction Finding: Compass

Used to derive bearing, the compass has served for centuries as the primary device for direction-finding on the surface of the Earth. Compasses may operate on magnetic or gyroscopic principles or by determining the direction of the Sun or a star.

4.7.3 Map-based Navigation: Nautical Chart

A nautical chart is a map designed and used primarily for navigation at sea. It presents most of the information used by the marine navigator, including latitude and longitude scales, topographical features, navigation aids (e.g., buoys, lighthouses, radio beacons), data on magnetic compass variation, indications of reefs and other hazards, water depths, and warning notices. Such information allows both plotting a safe course and checking progress while underway.

5. Technology Under Test

The devices-under-test were chosen based on the results of the U.S. Department of Transportation Maritime Administration PNT Resiliency Pilot Program, Phase I Report as well as subsequent research by the Volpe Center.[6] Several of the devices evaluated during Phase II testing have International Traffic in Arms Regulations (ITAR) restrictions. Additional equipment was deployed during the sea trials to provide reference data and supporting information during analysis.

5.1 Furuno GP170

The Furuno GP170 is the positioning system used on all the MARAD RRF vessels. The GP170 GPS receiver was selected for Phase II testing because it is representative of a MARAD GNSS system and assures continuity throughout test phases and compatibility with existing GPS equipage.

5.2 Protective Technologies

CRPAs are specialized antennas that help protect GPS receivers from interference and jamming. These antennas create spatial filters from an array of antenna elements to focus on the desired GPS signal and cancel out the unwanted jamming signals. This is typically accomplished through space-time adaptive processing or space-frequency adaptive processing. Additionally, the CRPA does not require any changes to the GPS receiver, but simply replaces the existing antenna.[7] Table 1 lists the equipment/technologies under test during Phase II.

Table 1. Protective equipment under test

Manufacturer	Description	Model	Civil GPS/M-Code	Interference Rejection
Hexagon/NovAtel	4 element CRPA antenna	GAJT-410MS	Yes/Yes	L1/E1 and L2 protected. Capable of 3 simultaneous adaptive nulls
	7 element CRPA antenna	GAJT-710MS	Yes/Yes	L1/E1 and L2 protected. Capable of 6 simultaneous adaptive nulls
InfiniDome	In-line CRPA device using 2 external antennas	Otosphere	Yes/No	L1 protected, L5 & G1 passthrough. Capable of 1 adaptive null

NovAtel/Hexagon provides multi-element anti-jam antennas for the marine environment. The Program tested the GAJT-410MS and GAJT-710MS CRPAs aboard the SS Cornhusker State as well as at NAVFEST. The GAJT-410MS employs 4 elements and uses an adaptive digital null forming algorithm to identify

[6] Awaiting Publication

[7] https://www.gpsworld.com/anti-jam-technology-demystifying-the-crpa/

interference and jamming signals, adjusting its gain on reliable satellite signals to maintain PNT.[8] It is capable of forming three independent nulls to potentially mitigate up to three simultaneous interference sources. The GAJT-710MS is a 7-element CRPA and provides anti-jam protection in dynamic multi-jammer scenarios across a wide band of signals including GPS L1/L2, QZSS L1/L2, SBAS L1, and Galileo E1. This antenna is capable of forming 6 independent nulls and thus can simultaneously mitigate up to 6 sources of interference and jamming.

The Infinidome Otosphere is an inline device for GPS receivers which is placed between the receiver and antennas.[9] The filtering algorithm combines patterns from two omni-directional antennas to determine interference direction and filter out those signals. The Otosphere is capable of forming one adaptive null, thus mitigating one interference or jamming source and is compatible with most available GNSS receivers.

[8] https://novatel.com/products/anti-jam-antenna-systems-gajt/gajt-410ms-anti-jam-antenna

[9] https://infinidome.com/otosphere/

6. Data Collection

The focus of the MARAD PNT Pilot Program, Phase II, data collection effort is to assess the performance of the proposed technologies in protecting the representative Furuno GP170 receiver from real-world jamming and spoofing. A sea trial was conducted in an area where jamming and spoofing are known to be a common occurrence. The sea trial provided an in-situ scenario with the intent of encountering jamming/spoofing signals.

During the sea trial, the equipment under test along with the reference system and RF monitoring system collected data during normal operations, separate from, but in parallel with, the ships navigation system, for comparison. Collection periods included travel to and from areas of interest, as these periods are largely free of external interference and therefore suitable in assessing baseline performance of devices under test.

6.1 SS Cornhusker State

The *Cornhusker State* (T-ACS-6) served as the host vessel for the live sea trial data collection. The *Cornhusker State* is a crane ship in ready reserve for the U.S. Navy, stationed in Newport News, Virginia under operational control of the Military Sealift Command. The ship (originally named *CV Stag Hound*) was built by Bath Iron Works in Bath, Maine to a MARAD type C5-S-73b container ship design. She was laid down on November 27, 1967, launched on November 2, 1968, and delivered to MARAD on June 20, 1969. In 1987–1988 the ship was converted to a type C5-S-MA73c crane ship by Norfolk Shipbuilding & Drydock and placed in service as the *Cornhusker State* and assigned to the RRF.

6.2 Test Setup Overview

Equipment-under-test was installed and exercised during sea operations to international destinations. The testing was conducted such that there was no impact on normal maritime operations. To this end, the technologies were isolated and operated in parallel to "truth" and native PNT systems installed on the vessel. Figure 2 depicts the equipment, networking and basic functions of the systems deployed onboard the SS Cornhusker State. The four high-level categories of equipment labeled in the diagram are *Spectrum*, *Reference*, *Native*, and *Protected*. *Spectrum* refers to the RF spectrum analyzer. *Reference* refers to the "truth" system used for comparison. *Native* refers to the equipment that is representative of the ship's operational GNSS system, and *Protected* refers to the protective technologies under test. Additionally, once per minute positioning and timing information from the ship's navigation system was saved and provided as an additional data check point after the completion of the sea trial. Instrumentation includes:

- Native: Furuno GPS-017S (NAT)
- Protected:
  - NovaTel GAJT-4 (GJ4)
  - NovaTel GAJT-7 (GJ7)

- InfiniDome Otosphere (OTO) with Furuno GPS-017S

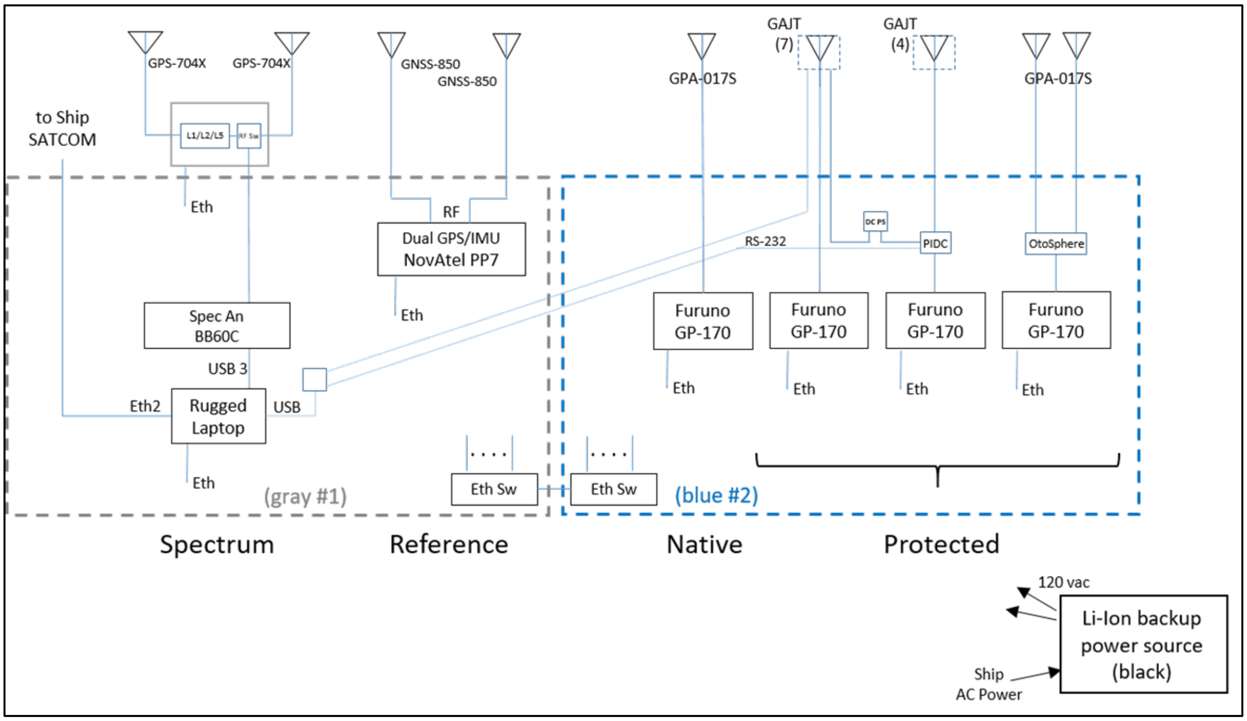


Figure 2. Test Setup Overview

Figure 3 shows the antenna and receiver installations aboard the *Cornhusker State*. The gray and blue compartments in the left image show the location of the instrumentation shown within the grey and blue dotted lines in Figure 2. Figure 4 indicates the relative position of each antenna and the IMU relative to the inner side of the handrail on the starboard side of the aft deck.

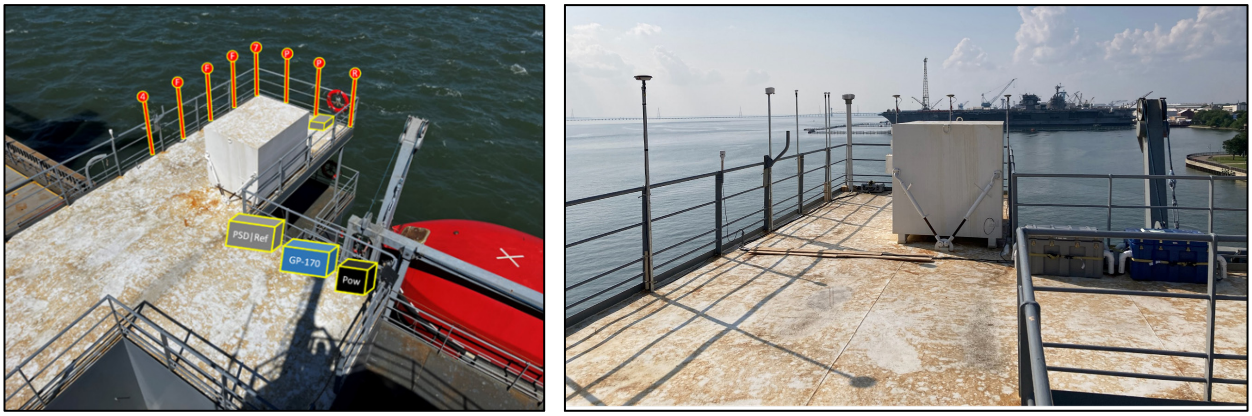


Figure 3. Notional Layout and Deployment Photograph

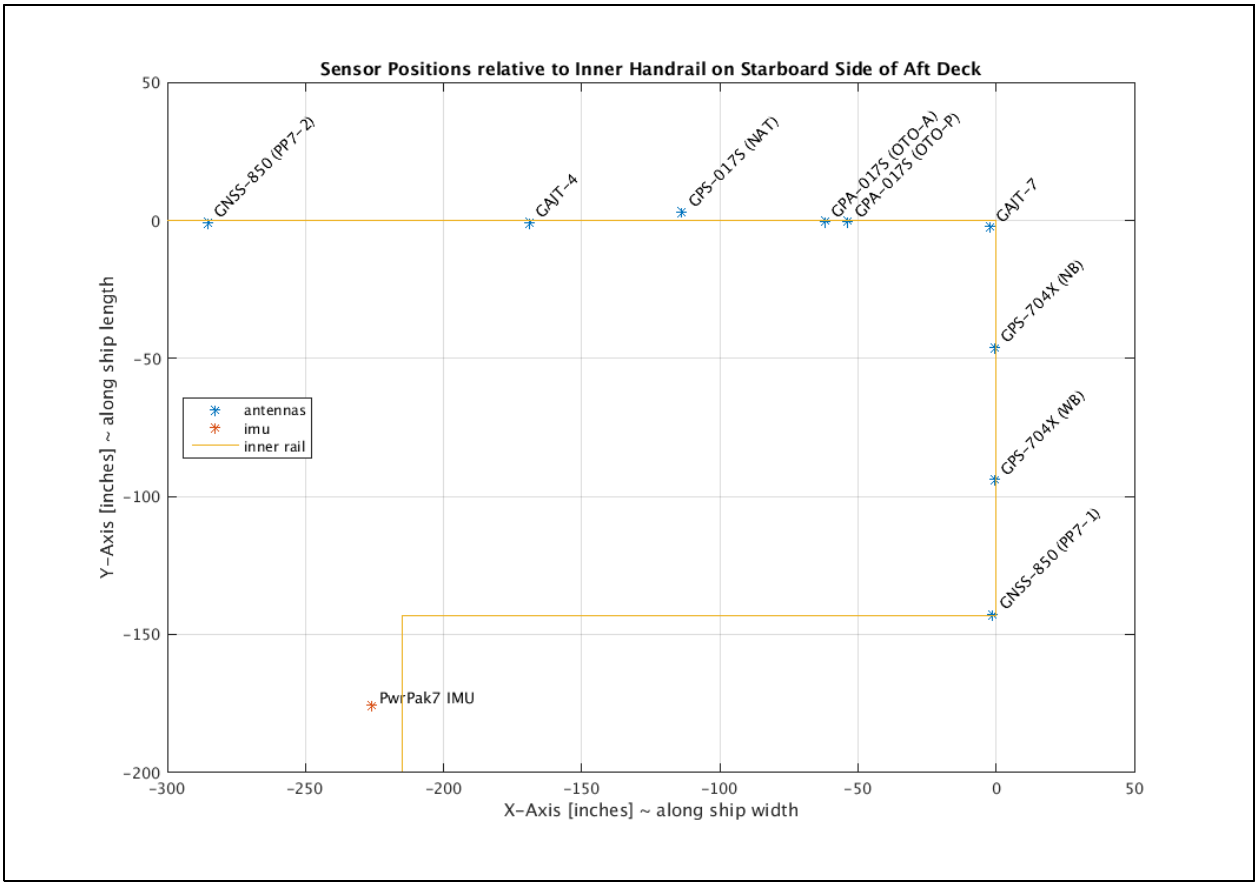


Figure 4: Deployed Sensor Positions

6.3 RF Monitoring

Radio frequency spectrum was collected before and during the sea trial to characterize the operational RF environment and provide the data resolution needed to understand the inherent challenges and potential threats to the intended operation of GPS on-board the test vessel.

6.3.1 Site Survey

The ambient RF environment existing on a large sea vessel is active and can be complex. A site survey was conducted in advance of the sea trial to identify any challenges to a nominal RF environment for GPS, including interference from ancillary electronic systems, signal blockages, and multipath reflections.

6.3.2 GNSS-Band Spectrum Collection

Time-stamped collection of spectral data for GPS L1, L2, and L5 were taken with use of a tri-band low-noise amplifier (LNA) in proximity to the antenna to retain full sensitivity for a high-resolution view of RF activity in the critical GPS bands. This information was used to characterize jamming and spoofing signals and offer insight into data anomalies experienced in either test or reference PNT systems.

6.3.3 Broad Spectrum Collection

Wider band RF spectral data was also collected to provide an understanding of out-of-band RF activity. High powered RF signals, whether with malicious intent or not, may considerably degrade GPS performance.

6.4 Sources of Reference PNT

6.4.1 Dual-antenna GNSS Reference System

Consistent with Phase I procedures, GNSS data collection was conducted with a dual-antenna NovAtel PwrPak7D-E2 (PwrPak7). This PwrPak7 comes integrated with an Epson G370N IMU and was paired with two NovAtel GNSS-850 antennas. The PwrPak7 was configured to receive and process signals from multiple GNSS constellations including GPS, Galileo, GLONASS, BeiDou, and SBAS. Additionally, the TerraStar-C PRO Precise Point Positioning (PPP) service was used to enhance the precision of the positioning solution in shore areas.

6.4.2 SS Cornhusker State Navigation System

Position and timing data acquired by the navigation system/Electronic Chart Display and Information System (ECDIS) of the test vessel was provided by MARAD. Two positioning snapshots, ECDIS 1 and ECDIS 2, were acquired once per minute and served as valuable reference data.

7. Data Analysis

Data was collected over 120 days from August to December 2023 during deployment to the Mediterranean Sea. August 17 is the reference Day 1. The analysis effort focused on Day 75 through Day 91 where the instrumentation indicated potential GNSS signal interference on the final two active legs of the ship's mission before returning to the United States.

7.1 Collection Artifacts Investigation

With the large amount of data collected, filters were applied to data gaps to focus the effort on more likely instances of interference.

7.1.1 Missing Receiver Data

A total of 72 gap periods (lasting 1 to 16 minutes) were identified in collected receiver data, more than two-thirds of which occurred during or after the return voyage to the United States. The noted gaps correlate between the four GP-170 receivers as well as with gaps noted in the collection of spectral data. In many cases the data gaps can be associated with process restarts and system reboots through comparison with log messages from automated system checks (where available). In such cases, the data gap merely indicates a cessation of data logging restored through an automated process restart or system reboot rather than any indication of RF interference.

7.1.2 Extended Periods of Power Fluctuation in PSD Sweeps

13 extended periods of power fluctuation were identified in spectral data sweeps ranging from 4 hours to 11 days in the data collection period. Ten of these instances occurred during or after the return to home port. The fluctuation starts and stops coincided with PSD data gaps and no corresponding effects were observed in the GPS receiver data. Fluctuations were determined to be due to an issue with the RF switching between antenna sources (one high power, one low power) prior to analyzer input.

7.2 Spectrum Analyzer Interference

The spectrum analyzer was used to determine times when instances of higher power appeared in and around the L1 band. Figure 5 displays three days of falling raster plots of spectrum analyzer sweeps. The blue regions show the noise floor with the centered green band showing GPS signals. Instances of higher power (yellow and red) began to appear late on the Day 80 plot and were ultimately present throughout Day 82. Similar power was evident on adjacent days as well, all providing evidence of interference on L1.

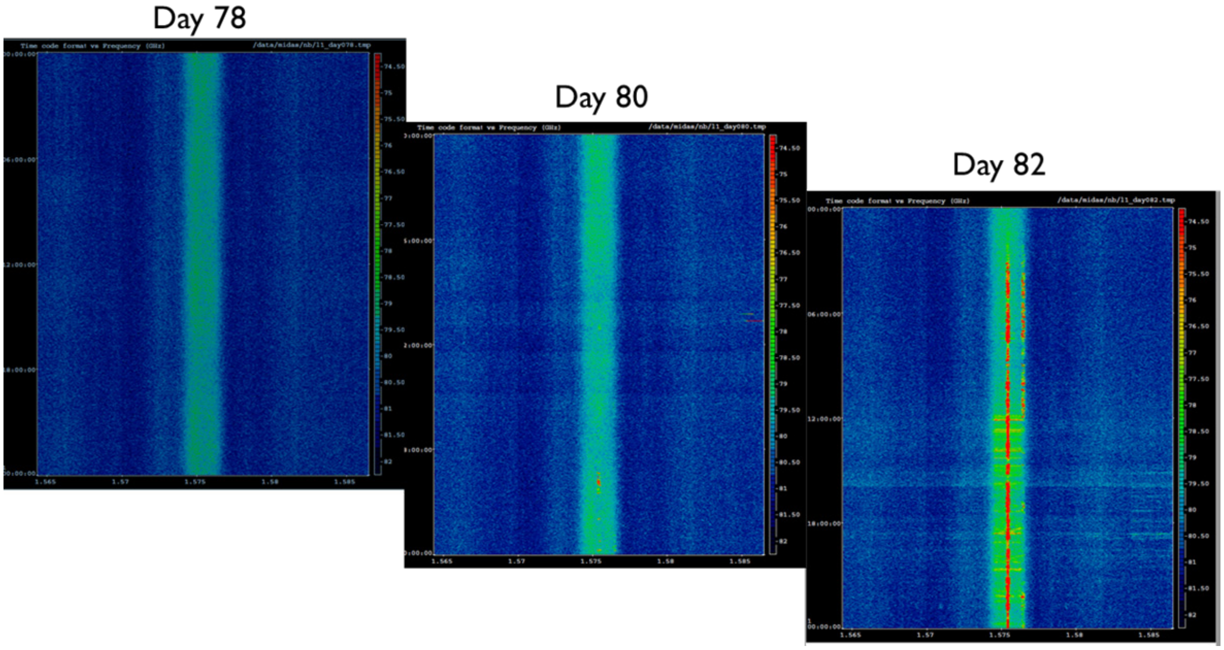


Figure 5. Falling Raster Plots of L1 Spectrum Analyzer Sweeps

7.3 Detected Anomalies

Anomaly detection techniques were implemented using multiple data sources to search for time frames with suspected interference. One time frame was identified with considerable interference and anomalous behavior in the reported device measurements. The performance of the protected technologies under test compared to native and reference technologies was analyzed in detail within this time frame.

7.3.1 Anomaly Detection Approach

Anomalies were detected using a multi-step approach that incorporated different data sources. First, a machine learning algorithm detected anomalies in the reported distance between the unprotected native device and the GAJT7 protected device. The reported distances were expected to vary slightly due to factors such as sensor noise. Typical distance values were quantified based on measurements from time periods that had minimal evident interference. Eras with sustained, abnormally large distances were identified as potential periods of interference. Figure 6 displays the detected eras.

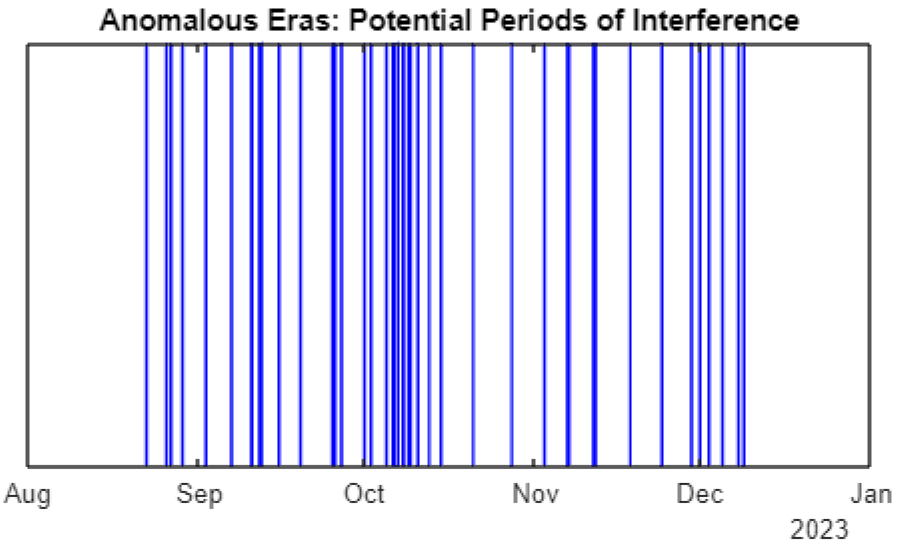


Figure 6. Eras with Abnormally Large Distances Between Unprotected Device and GAJT(7) Protected Device

Next, these eras were cross-referenced with other data sources. Day 80 (November 4) through Day 83 (November 7) were found to have the strongest indications of interference. The falling raster plots of the L1 band spectrum analyzer sweeps indicate sustained patterns of interference during this time frame. In addition, the reported position of the native device shows the largest deviations from the protected devices within this timeframe. The deviations on Day 83 are orders of magnitude larger than on any other day over the entire data collection period, as shown in Figure 7.

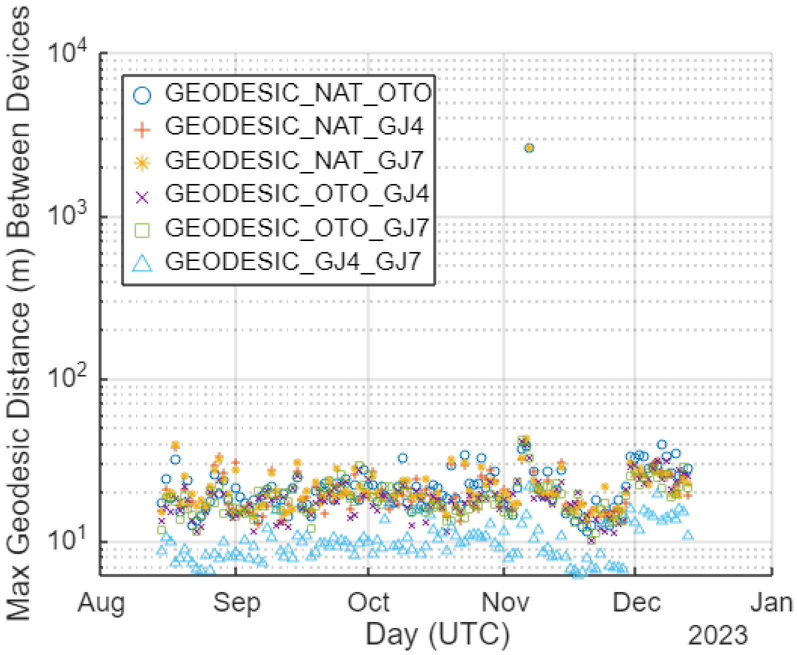


Figure 7. Daily Max Geodesic Distance Between Devices

7.3.2 Trajectory Deviation

On Day 83, the native device showed an instance of deviation in trajectory as seen in Figure 8. The protected devices were not affected and continued to show data along trajectory in conjunction with the ship's ECDIS position recordings.

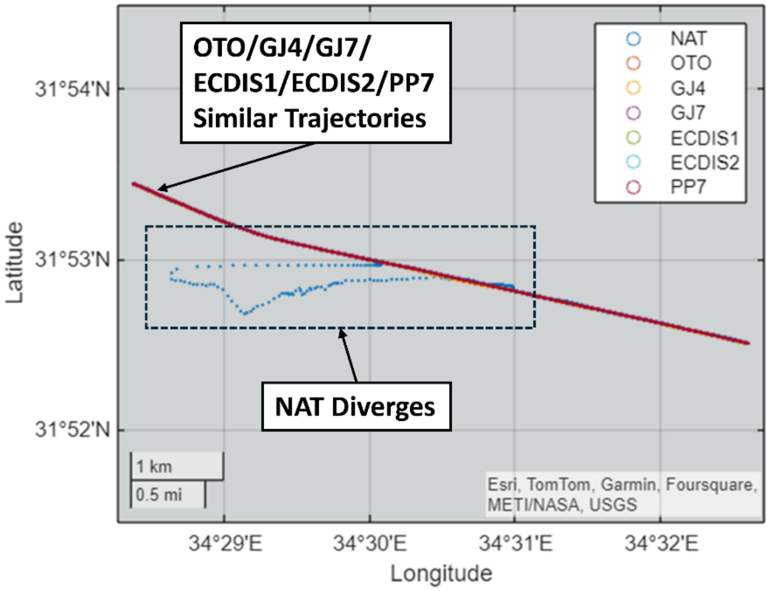


Figure 8. Location of Deviation on Day 83

Figure 9 shows the maximum hourly geodesic distance between the PwrPak7 (PP7) and other devices around the diversion timeframe. On Day 83, the large deviation of the native system from other sensors is evident.

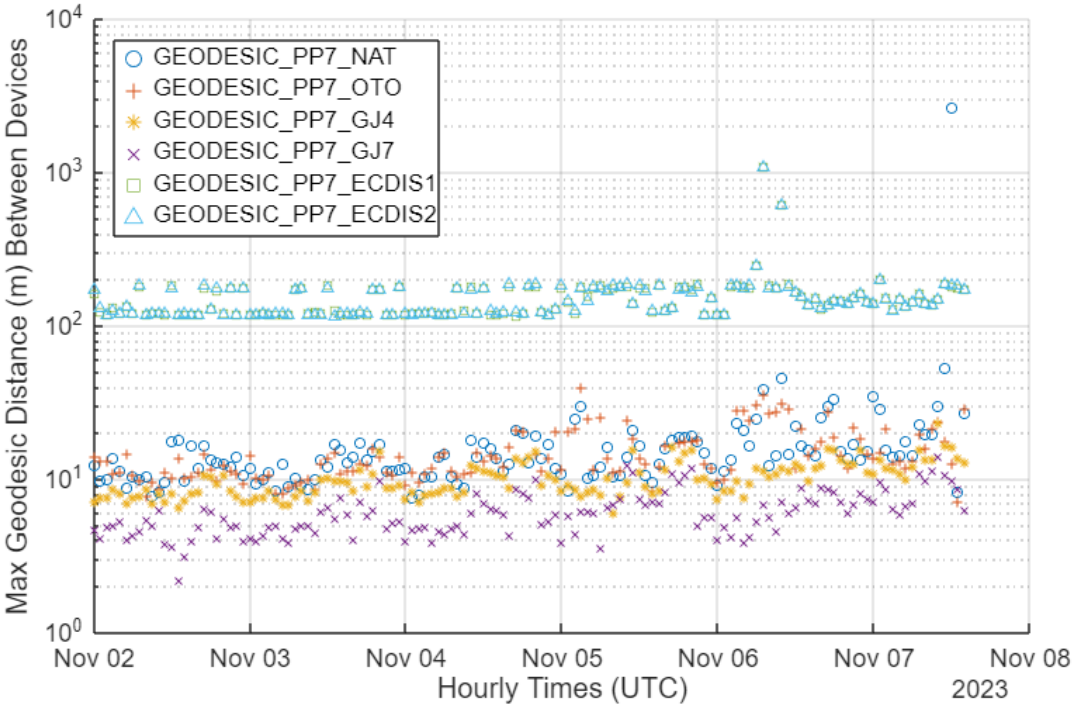


Figure 9. Hourly Max Geodesic Distance Between Devices

Figure 9 also shows large deviations for ECDIS 1 and ECDIS 2 compared to other devices on Day 82. The protected antennas were not affected during these times and showed reasonable deviations with respect to the PwrPak7. The root cause of the deviations in ECDIS 1 and ECDIS 2 was not investigated further, as the analysis focused on the performance of the protected equipment under test. Note that the higher baseline distance in ECDIS time series is due to the associated antennas being on the forward part of the ship, where the separation may also allow for differences in encountered interference and related positioning effects.

7.3.3 Position Error Example

Figure 10 details an example of position error around the time of the deviation described in the previous section. The reference position was provided by PwrPak7 BESTPOS. The corrections for antenna offsets applied using ship heading were derived from PwrPak7 dual-antenna heading. The higher variance in Days 82 and 83 may reflect the effects of interference on devices under test (DUTs), PwrPak7, or both. The higher error variance for the native and Otosphere equipment may reflect poor multipath mitigation performance of the GPA-017S source antenna.

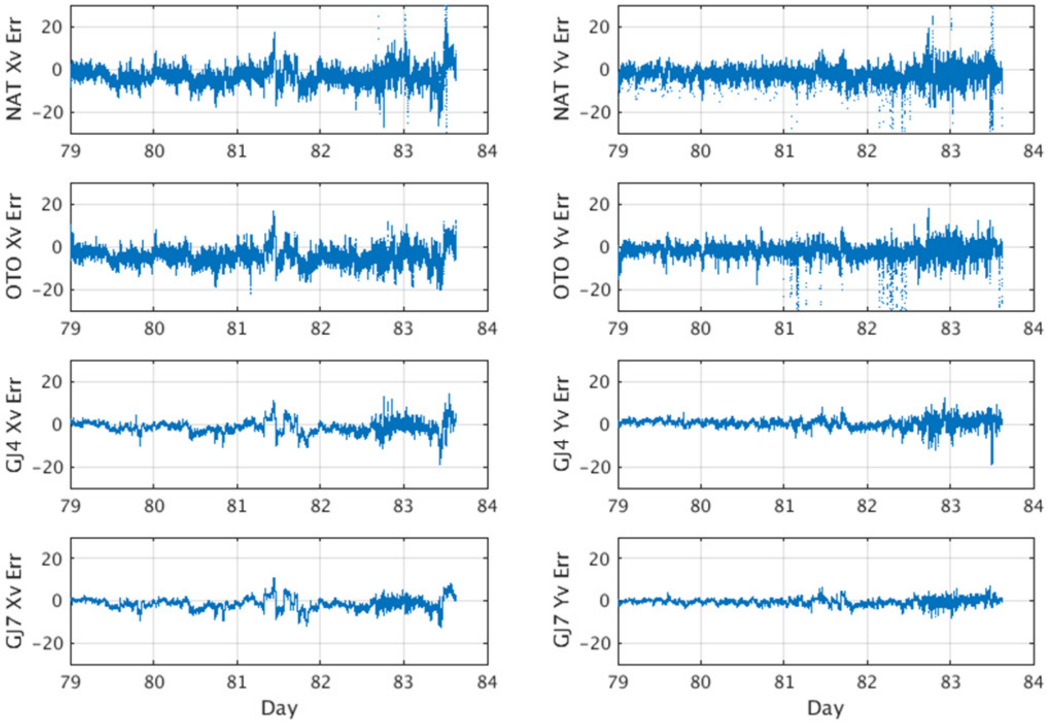


Figure 10. Position Error Example

7.4 Additional Equipment Testing: NAVFEST Test Campaign

The USDOT PNT Pilot Program leveraged an additional opportunity for equipment testing that emerged after the conclusion of the sea trials. This unique event, NAVFEST, enabled the testing of the same protective devices used during the sea trial in an environment with known jamming and spoofing threats. This opportunity provided an excellent test bed for further exploring the anti-jam capabilities of the proposed protected equipment to better inform recommendations for MARAD deployment.

NAVFEST is an annual innovative GPS interference event at White Sands Missile Range (WSMR) in New Mexico executed by the U.S. Army's 746th Test Squadron. NAVFEST is designed to simulate an electronic warfare environment. All protected equipment deployed aboard the *Cornhusker State* was further tested in various static and dynamic jamming scenarios over two weeks.

7.4.1 NAVFEST Test Scenarios and Schedule

NAVFEST provided a nightly schedule of scenarios with adverse conditions of jamming and spoofing. Variations in waveform types, power levels, location of jammers and threat types defined the different scenarios. Table 2 describes the high-level types of scenarios. More detailed information is provided in the subsequent test matrices.

Table 2. Scenario types and descriptions

Acronym	Short Name	Description
Spoofing Scenarios		
ET	Emerging Threat	Sophisticated jamming from a single location
CET	Complex Emerging Threat	Measurement / Signal or Data spoofing from a single location
Jamming Scenarios **(CT – Conventional Threat)**		
AL	Area Low Power	GPS jamming pattern that provides jamming from one small location radiating 360 degrees
AM	Area Medium Power	GPS jamming pattern that provides medium power jamming across a large area
AH	Area High Power	GPS jamming pattern that provides high power jamming across a large area
LH	Line High Power	GPS jamming pattern that provides a nominal line of jamming
NH	NOP High Power	GPS jamming pattern that provides jamming from a high elevation location
CH	Corridor High Power	GPS jamming pattern that provides jamming along one stretch of road (RR7)
BMA/BMB	Blink (Pattern A / Pattern B)	Jammers will vary in number of jammers in sequence & notional ON/OFF schedule for a period of 1 hour
RO	Rotate	Jammers will rotate as single emitters from 1-8 in a sequence
CUSTOMER	Customer	Custom jamming pattern utilizing customer technology

The nightly test matrices for NAVFEST are given in Table 3 and Table 4. At the start of each night, a Knock-Off (KO) jamming event was scheduled before each of the ET and CET scenarios. This is meant to “knock-off” GPS receivers from their valid solution. The table cells are color coded to indicate high-level threat type: ET – yellow, CET – orange, CT – green). The second line within each cell indicates the USDOT test team’s site location, and motion type for each scenario. NA designates scenarios that were cancelled by the NAVFEST operators. The local time represents 15-minute periods ending at the displayed time. Scenario start- and end-times are approximate. In addition to ground-based jammers, an airborne jammer (ABJ) was active for some scenarios.

Table 3. Test Matrix – Week 1

Date	7-May-24	8-May-24	9-May-24	10-May-24
Night ID	1	2	3	4
0:15				
0:30				
0:45	KO (10 Min) Melton | Static	NA	KO (10 Min) Melton | Static	KO (10 Min) Stallion | Static
1:00	ET Melton | Static	NA	ET Melton | Dynamic 1	ET Stallion | Static
1:15				
1:30				
1:45	KO (10 Min) Melton | Static	KO (10 Min) Melton | Static	KO (10 Min) Melton | Static	KO (10 Min) Stallion | Static
2:00	CET Melton | Dynamic 1	CET Melton | Dynamic 1	CET Melton | Static	CET Stallion | Static
2:15				
2:30				
2:45	AL Melton | Static	AH Melton | Static	AH Melton | Static	AH Convoy | SRC to Phets
3:00				
3:15				
3:30	AL Melton | Static	LH + ABJ Melton | Static	LH + ABJ Melton | Static	AH Melton | Dynamic 1
3:45				
4:00				
4:15	AM Melton | Static	CH + ABJ Melton | Static	CH + ABJ Melton | Static	AH Melton | Static
4:30				
4:45				
5:00	AM Melton | Static	NH + ABJ Melton | Static	NH + ABJ Extended Convoy | SE of Phets to SRC	AH Melton | Static
5:15				
5:30				

Table 4. Test Matrix – Week 2

Date	14-May-24	15-May-24	16-May-24	17-May-24
Night ID	5	6	7	8
0:15				
0:30				
0:45	KO (10 Min) Weap | Static	KO (10 Min) Convoy | SRC to Phets	KO (10 Min) Weap | Dynamic 2	KO (10 Min) Norma Access | Static
1:00	ET Weap | Static	ET Convoy | SRC to Phets	ET Weap | Dynamic 2	ET Norma Access | Static
1:15				
1:30				
1:45	KO (10 Min) Weap | Static	KO (10 Min) Convoy | Phets to SRC	KO (10 Min) Weap | Dynamic 2	KO (10 Min) Norma Access | Static
2:00	CET Weap | Static	CET Convoy | Phets to SRC	CET Weap | Dynamic 2	CET Norma Access | Static
2:15				
2:30				
2:45	BMA Weap | Static	AH + ABJ Convoy | SRC to Phets	BMB Melton | Dynamic 2	AH + ABJ Weap | Dynamic 2
3:00				
3:15				
3:30		LH + ABJ Convoy | Phets to SRC		LH + ABJ Weap | Static + Dynamic 2
3:45				
4:00	RO Weap | Static		NA	
4:15		CH + ABJ Convoy | SRC to Phets		CH + ABJ Weap | Static + Dynamic 2
4:30				
4:45				
5:00	CUSTOMER Weap | Static	NH + ABJ Convoy | Phets to SRC	NA	NH + ABJ Weap | Dynamic 2
5:15				
5:30				

7.4.2 Test Setup

The USDOT team conducted operations out of a Sprinter van for both static and dynamic operations. The Sprinter van served as the platform for the USDOT ground truth reference system(s), as well as all devices under test. The van is outfitted with a 3,000-Watt, van integrated, pure sine wave inverter for powering equipment; an upgraded alternator; a large roof rack with rear ladder; and tie-down points inside the van. Two portable lithium-ion power stations provided for assured power. Reference antennas and test system antennas were installed on the roof rack, as depicted in Figure 11. Lateral and/or vertical offsets between the reference antennas, test antennas and ground truth reference positions were measured prior to, during, and after testing, as appropriate.

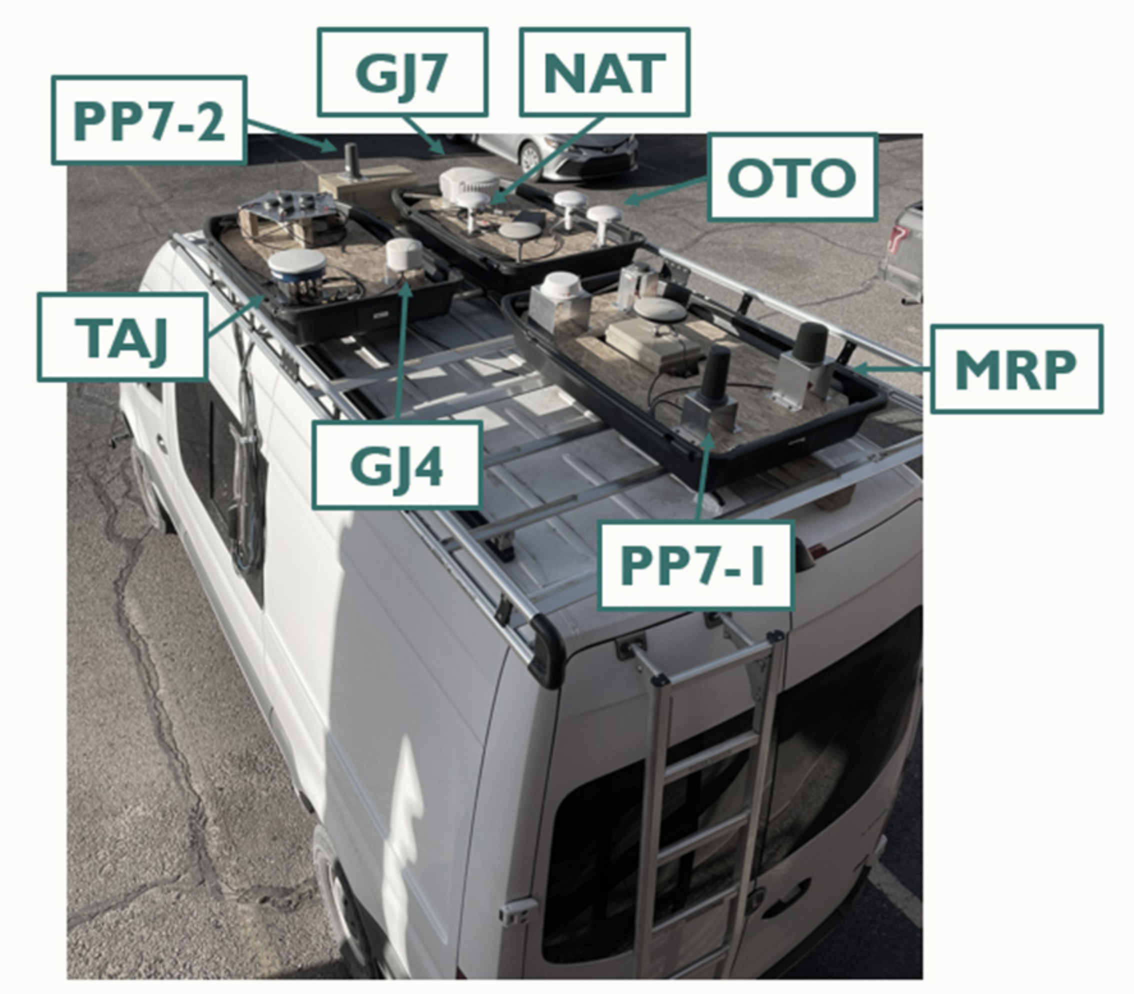


Figure 11. USDOT Sprinter van with mounted device layout for NAVFEST

Table 5 gives a detailed listing of the protective devices-under-test on-board the Sprinter test vehicle, most of which had been previously tested aboard a MARAD Ready Reserve Fleet vessel. NAVFEST provides the opportunity to evaluate performance under a controlled and diverse set of electronic warfare threats. As with the sea trials, the reference system included the PwrPak7 with PPP service. In addition, AGC data from an on-board WAAS G-III Reference Receiver was used to aid with delimiting test event periods. For completeness, all systems installed in the van for NAVFEST are depicted in a block diagram in Figure 12. Note not all installed systems are relevant to MARAD objectives.

Table 5. Protective Equipment-Under-Test at NAVFEST

Receiver	In-line Device	Antenna	Device/Capability-Under-Test
Furuno GP170	None	Furuno GPA-020S (NAT)	Unprotected representative MARAD configuration
Furuno GP170	None	Tualcom 3300D (TAJ)	3-element CRPA w/pulse blanking and adaptive notch filtering
Furuno GP170	None	NovaTel GAJT-4 (GJ4)	4-element CRPA
Furuno GP170	None	NovaTel GAJT-7 (GJ7)	7-element CRPA
Furuno GP170	None	*Gen Dyn MRPA (MRP)	Horizon-limiting MRPA
Furuno GP170	InfiniDome Otosphere (OTO)	Furuno GPA-020S (x2)	In-line CRPA device using 2 external antennas

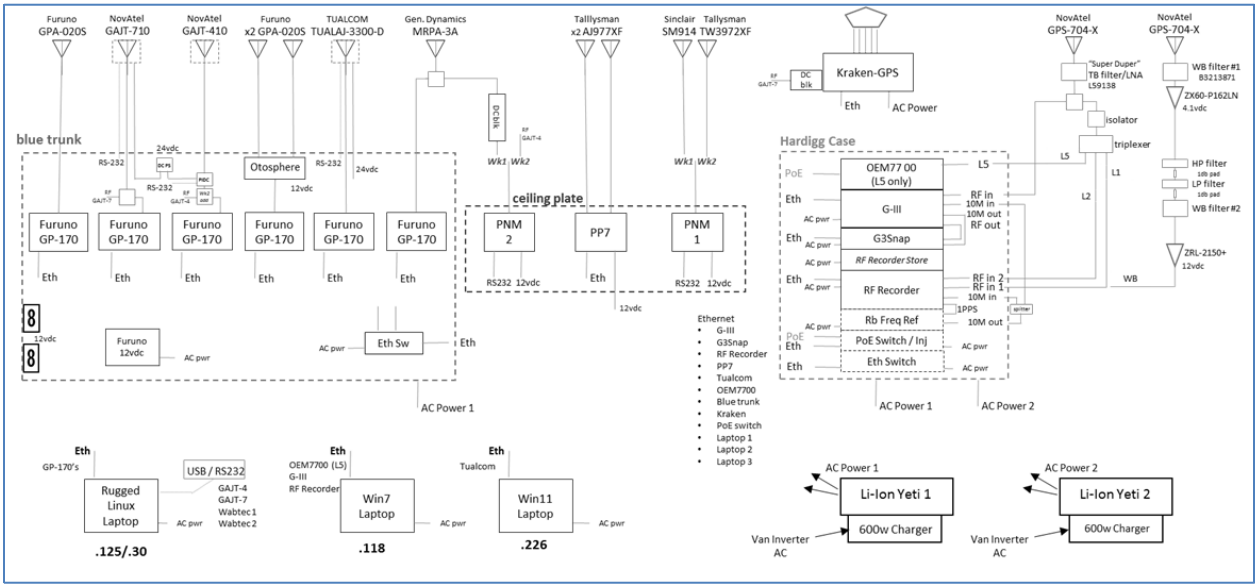


Figure 12: Block diagram of all NAVFEST Equipment

7.4.3 Data Collection

NAVFEST testing occurred during eight nights across two weeks in May 2024. Nights 1–4 spanned May 7 through May 10, and nights 5–8 spanned May 14 through May 17. Reference data was also collected on

May 6 (day 0) during clear conditions to serve as ground truth for positioning. Figure 13 shows the locations of all emitters (red) and USDOT site locations (yellow) used during NAVFEST testing.

Data was collected in the USDOT Sprinter test vehicle during static and dynamic operations at four sites: Melton, Weap, Norma, and Stallion. A "Dynamic 1" route involved driving back and forth between two reference points, with brief periods holding the van stationary at each point. Only one Dynamic 1 route was used for testing. A "Dynamic 2" route involved driving with continuous motion. The van also collected data on dynamic routes as part of the convoy that drove along Range Road (RR) 7 between Stallion Range Complex (SRC) at the north end of WSMR and Phets located at the intersection of RR7 and RR20.

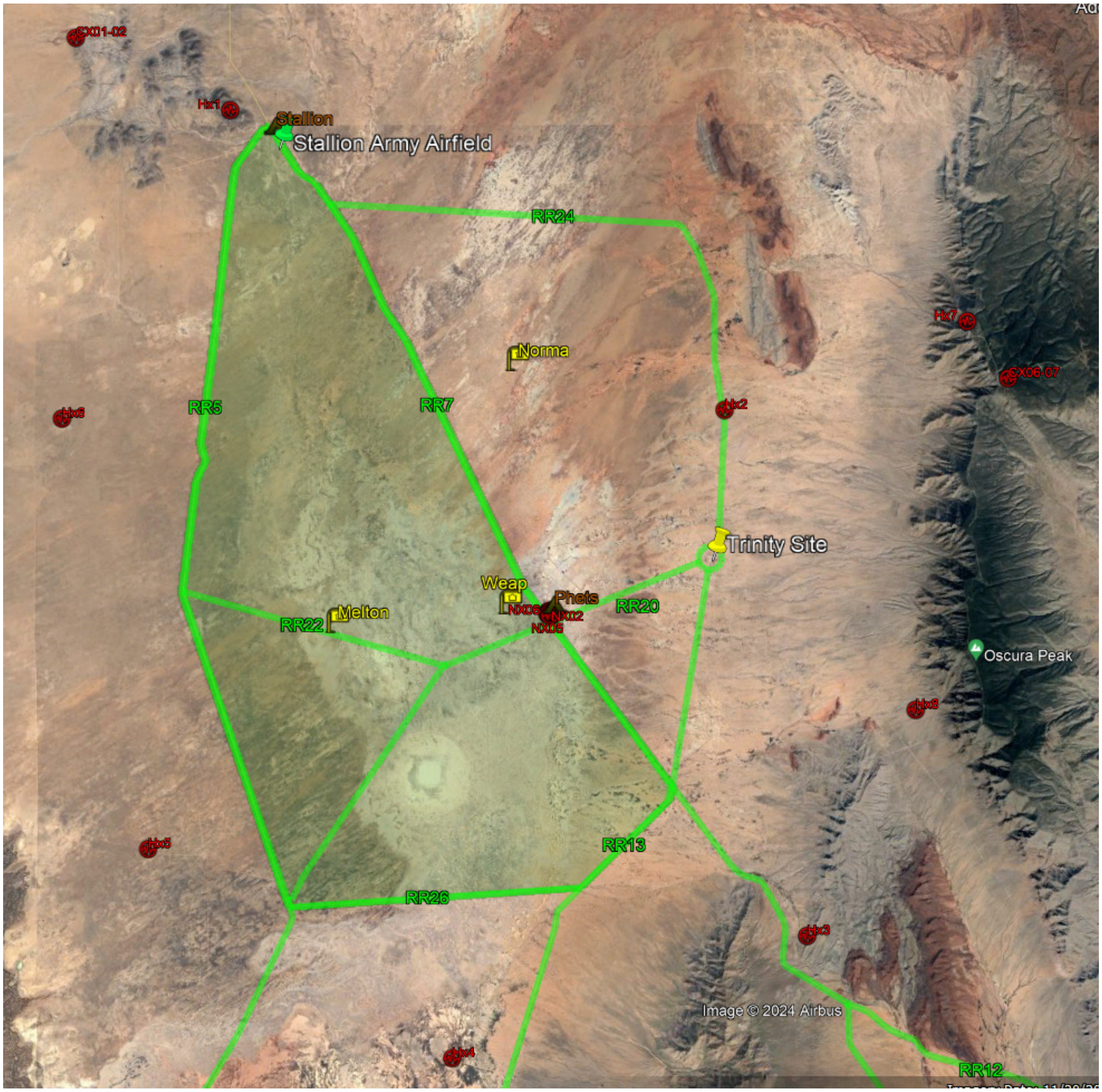


Figure 13: USDOT Site Locations and Emitters at WSMR

7.4.3.1 Melton Site

The Melton site is seen in Figure 14. Operations consisted of static data collection at Melton Point 1. Dynamic 1 type data was collected between Melton Point 1 and Melton Point 2. Dynamic 2 type data was collected around the oval path indicated nominally by the red path.

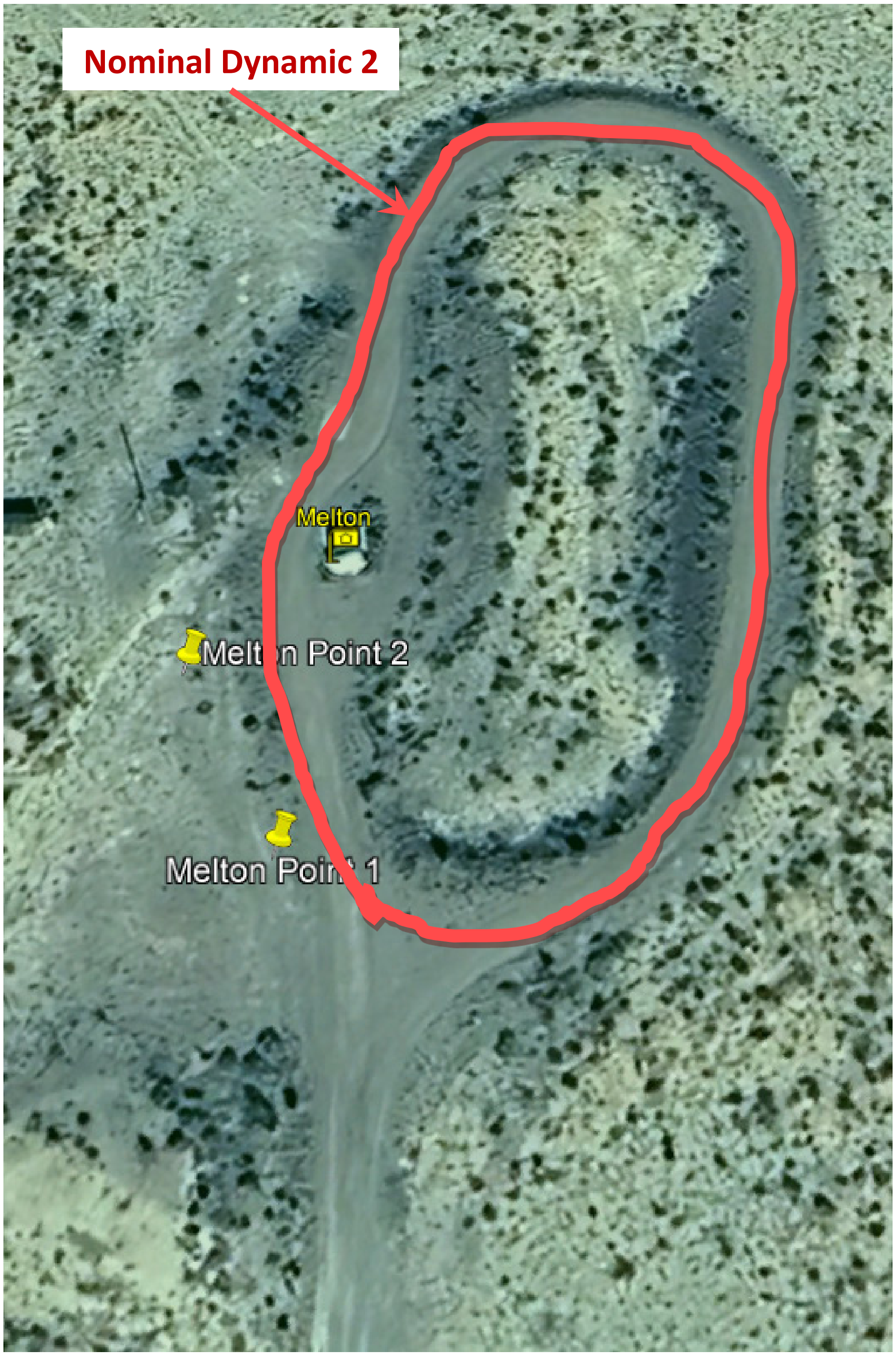


Figure 14. Melton Site Reference Points and Dynamic Routes

7.4.3.2 Weap Site

Operations at Weap can be seen in Figure 15, which consisted of static type data collection at Weap Point 1. There were no Dynamic 1 routes performed at Weap. Dynamic 2 data was collected around the oval indicated nominally by the red path.

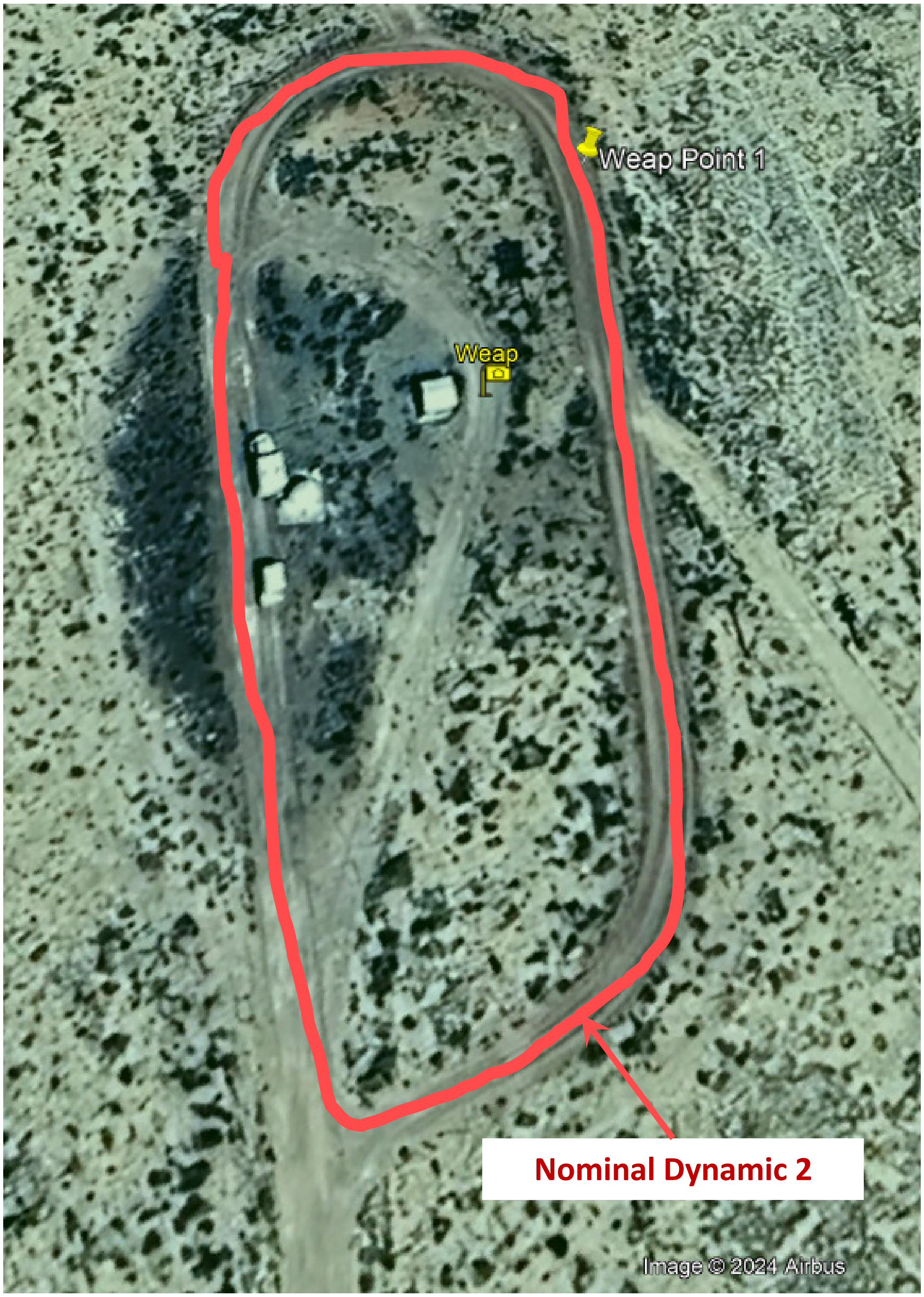


Figure 15. Weap Site Reference Point and Dynamic Route

7.4.3.3 Norma Site

Operations near the Norma site can be seen in Figure 16, which consisted of static data collection at Norma Point 1, also referred to as Norma Access due to the proximity to the access road to Norma. There were no Dynamic 1 or Dynamic 2 operations collected at the Norma site.

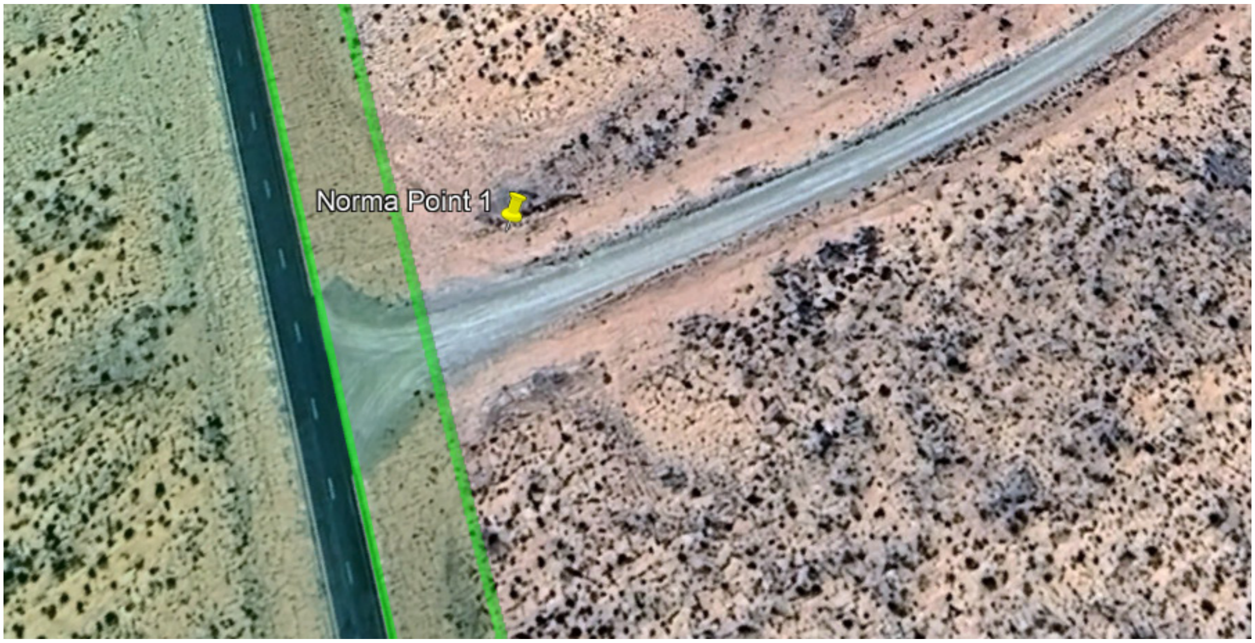


Figure 16. Norma Site Reference Point

7.4.3.4 Stallion Range Complex (SRC) Site

Operations at the Stallion site can be seen in Figure 17 which consisted of static data collection at Stallion Point 1. There were no Dynamic 1 or Dynamic 2 operations at the Stallion site.

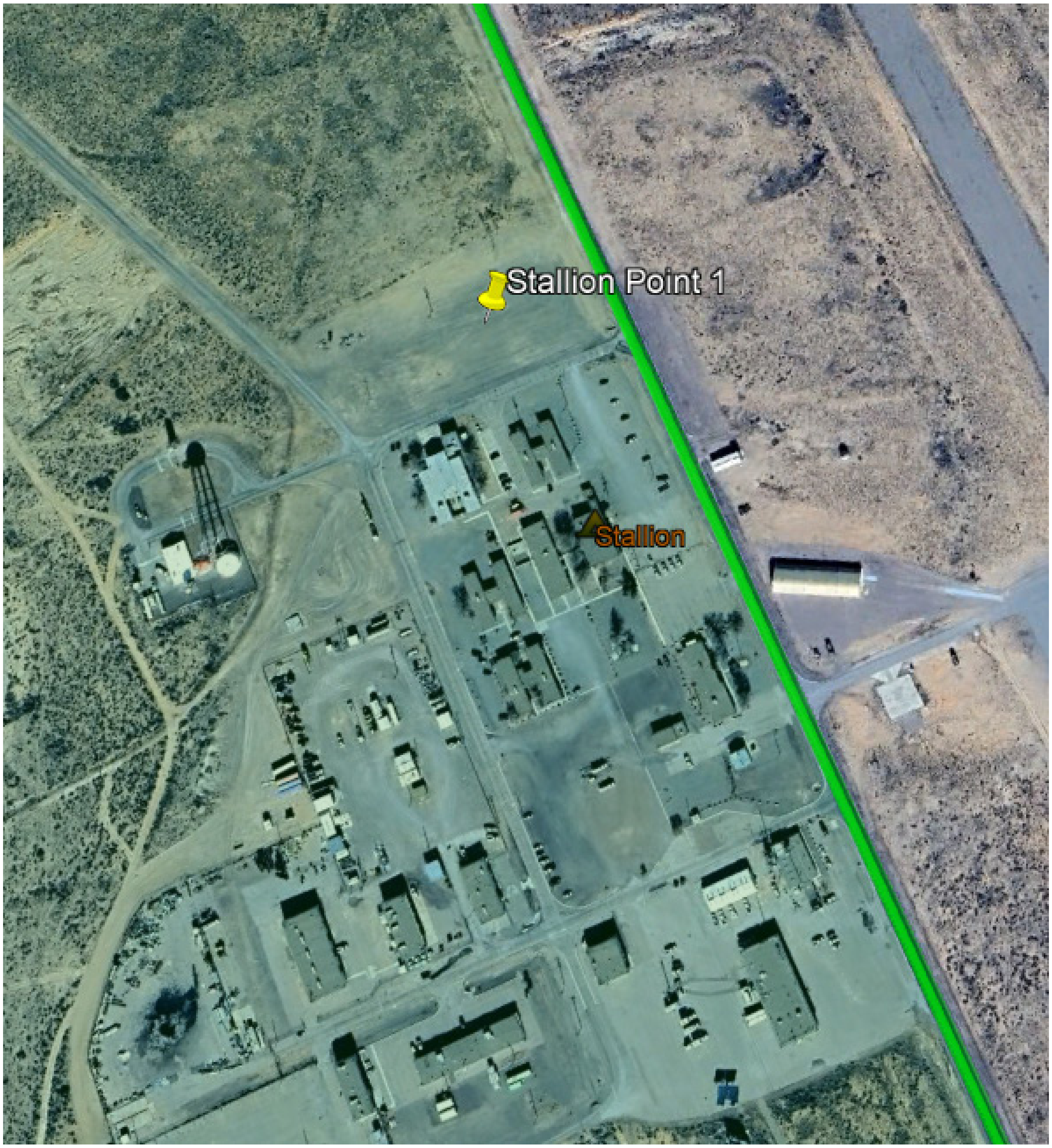


Figure 17. Stallion Site Reference Point

7.4.3.5 Convoy and Extended Convoy Route

The convoy route operation shown in Figure 18 ran between Stallion and Phets along RR7. The convoy lead vehicle, belonging to the 746th Test Squadron, provided ground truth data. This route was driven back and forth throughout each night of testing, with USDOT participating in some test scenarios. In one case, for the final event of Night 3, the van was pre-positioned farther southeast than Phets on RR7 and from there driven at a constant speed along RR7 toward the northwest passing Phets and continuing along the convoy route (but independent of the convoy) all the way to SRC. This route is denoted "Extended Convoy" in Table 3.

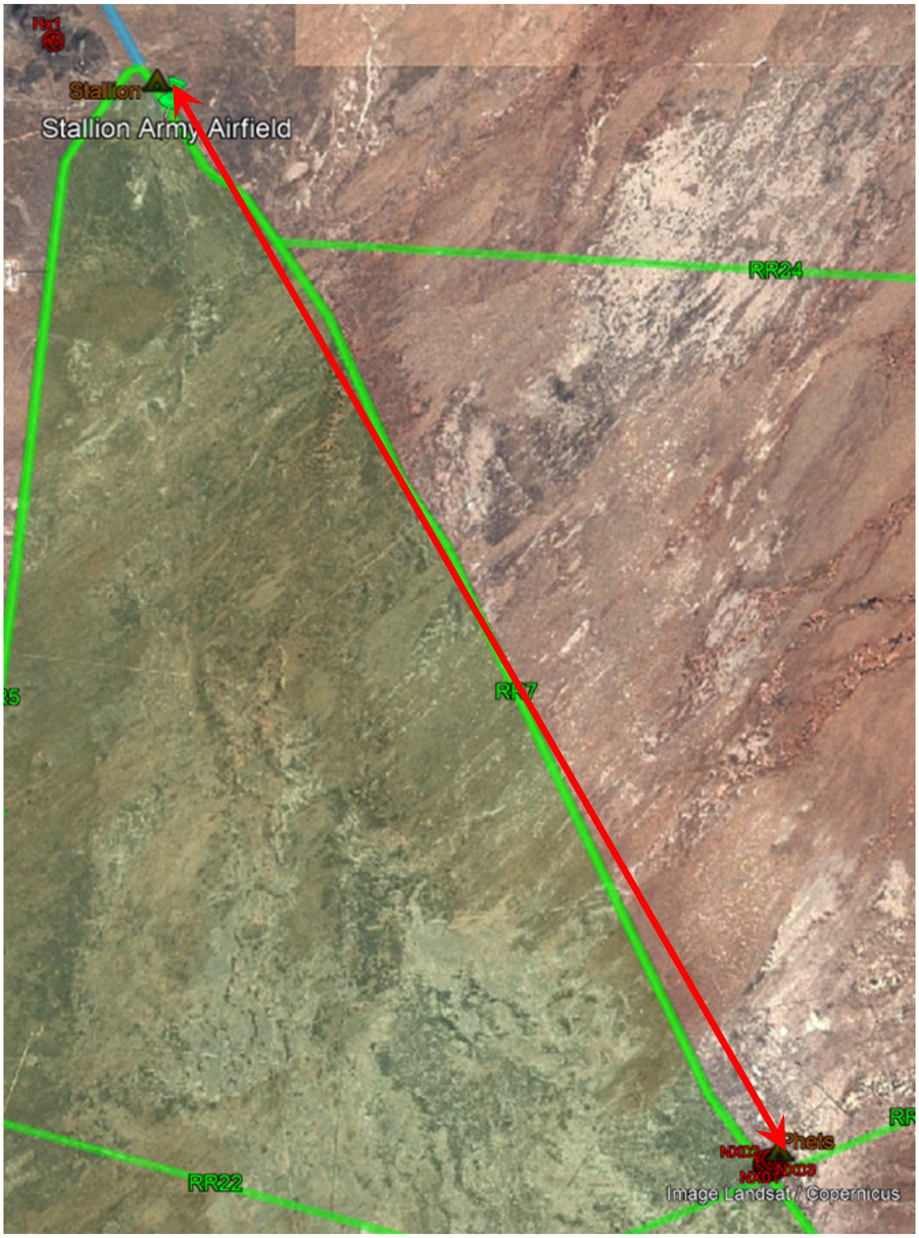


Figure 18. Convoy Route; red arrow between Stallion (top) and Phets (bottom)

7.4.4 Data Analysis

This section contains the analysis of the data collected at NAVFEST. Several investigations were performed to evaluate device performance under a variety of criteria and conditions. The investigations are summarized and key findings are discussed.

7.4.4.1 Detecting Interference

The L1 AGC pulse width data collected by the WAAS G-III reference receiver was used to identify time periods with observed interference. The data was collected during time periods with interference as well as periods without interference for comparison. The full data set was inspected to determine typical baseline values without interference. Thresholds were selected to separate baseline values from values that indicate interference. Values below threshold indicate interference.

Baseline distributions varied by night due to changes in data collection configurations. Figure 19 shows the L1 AGC pulse width histograms grouped by nights with similar configurations.

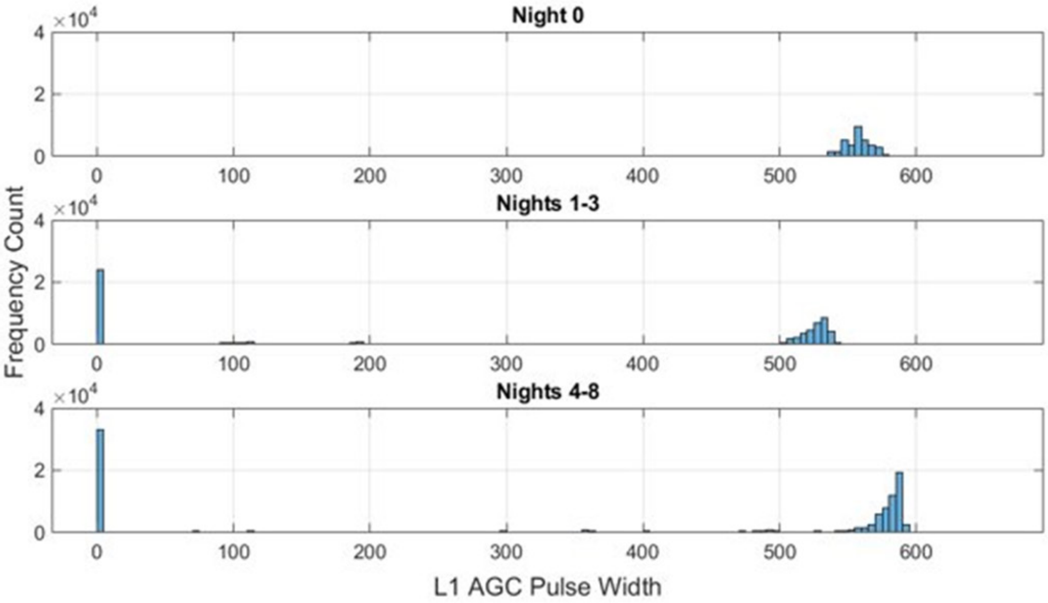


Figure 19. L1 AGC Pulse Width distributions

The scheduled periods of interference were cross referenced with observed periods of interference. In the case of discrepancies, the observed interference times were used to indicate the scenario start and end times for jamming events. Figure 20 shows a comparison of the scheduled and observed scenario time frames for Night 1 as an example. The ABJ was not scheduled at any time during this night. (The full set of time frame comparisons for all nights can be found in Appendix A: NAVFEST Scenario Time Frames.)

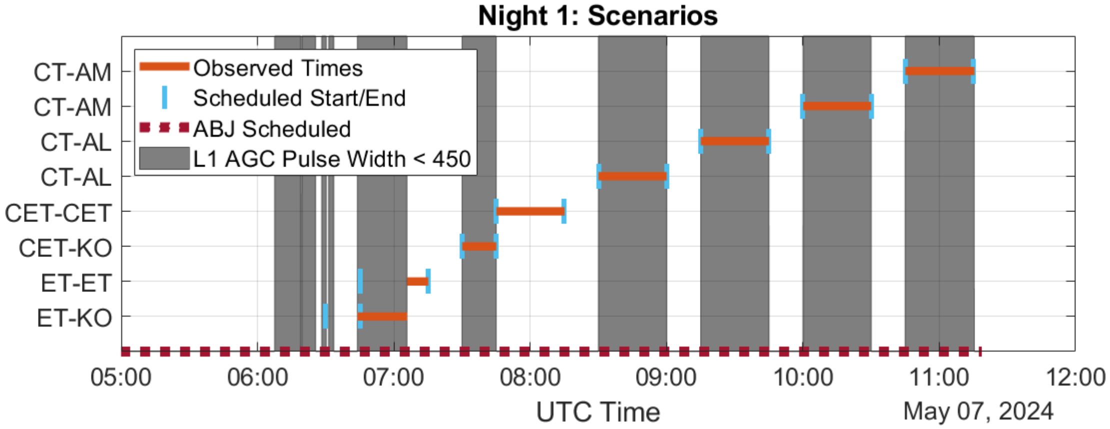


Figure 20. Scenario time frames for Night 1

7.4.4.2 *Signal Availability*

The signal availability analysis investigated how often valid horizontal position data (i.e., latitude and longitude) was reported for each device throughout each scenario. The analysis also investigated how often the number of satellites tracked is reported, as well as how many satellites are tracked. Note that data collection was disrupted for GJ4, TAJ, OTO, MRP, and NAT on Night 4 due to issues with reported times. This impacts scenario IDs 26 through 30 for these devices.

Figure 21 shows how often horizontal position data was reported for each device (vertical axis) throughout each scenario (horizontal axis) throughout NAVFEST. Scenarios are ordered based on scenario type, to visually group similar types of events. Higher values (dark blue) indicate more favorable performance.

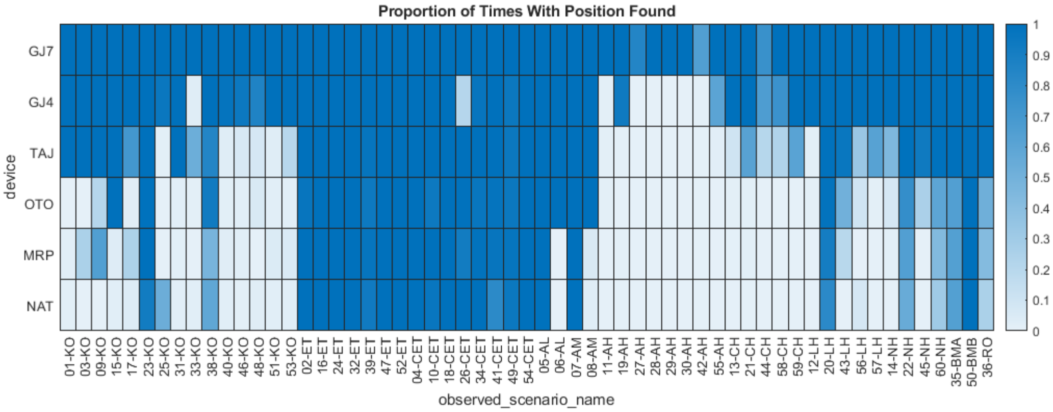


Figure 21. Heatmap with proportion of times a valid horizontal position is reported

Figure 22 shows how often data was reported for satellites tracked for each device throughout each scenario. Higher values (dark blue) indicate more favorable performance.

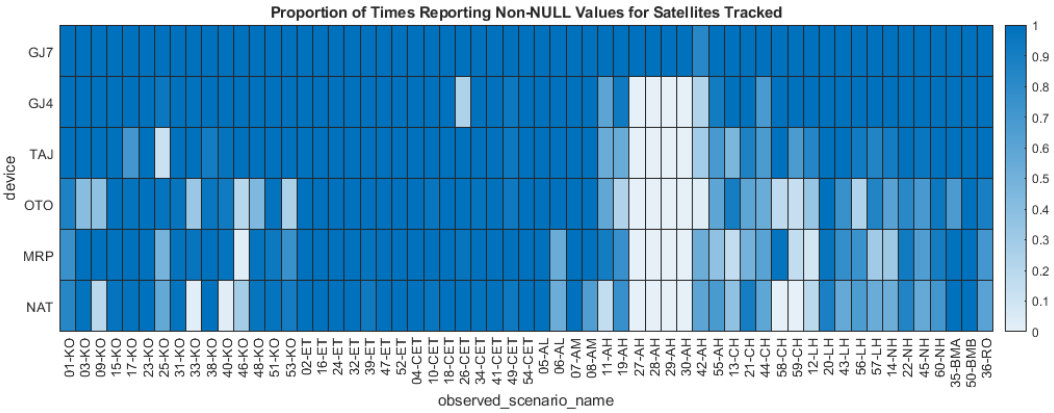


Figure 22. Heatmap with proportion of times reporting a valid number of satellites tracked

Figure 23 shows the mean number of satellites tracked for each device throughout each scenario. Higher values (dark blue) indicate more favorable performance.

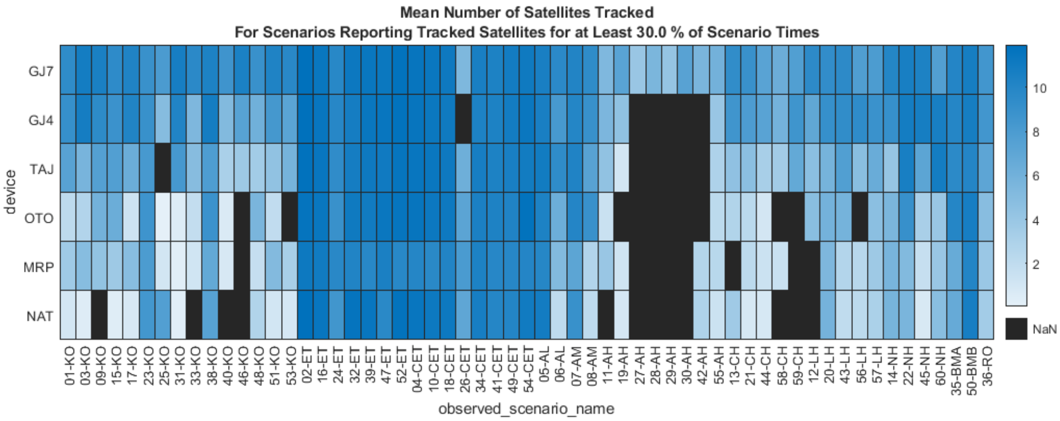


Figure 23. Heatmap with mean number of satellites tracked

The results of the signal availability analysis indicate an overall relative order or performance from high to low: GJ7, GJ4, TAJ, OTO, MRP, NAT. However, there are occasional exceptions for certain scenarios.

7.4.4.3 *Static Reference Data*

Five reference locations were used for static data collection:

- A: Melton Point 1
- B: Melton Point 2
- C: Weap Point 1
- N: Norma Point 1
- S: Stallion Point 1

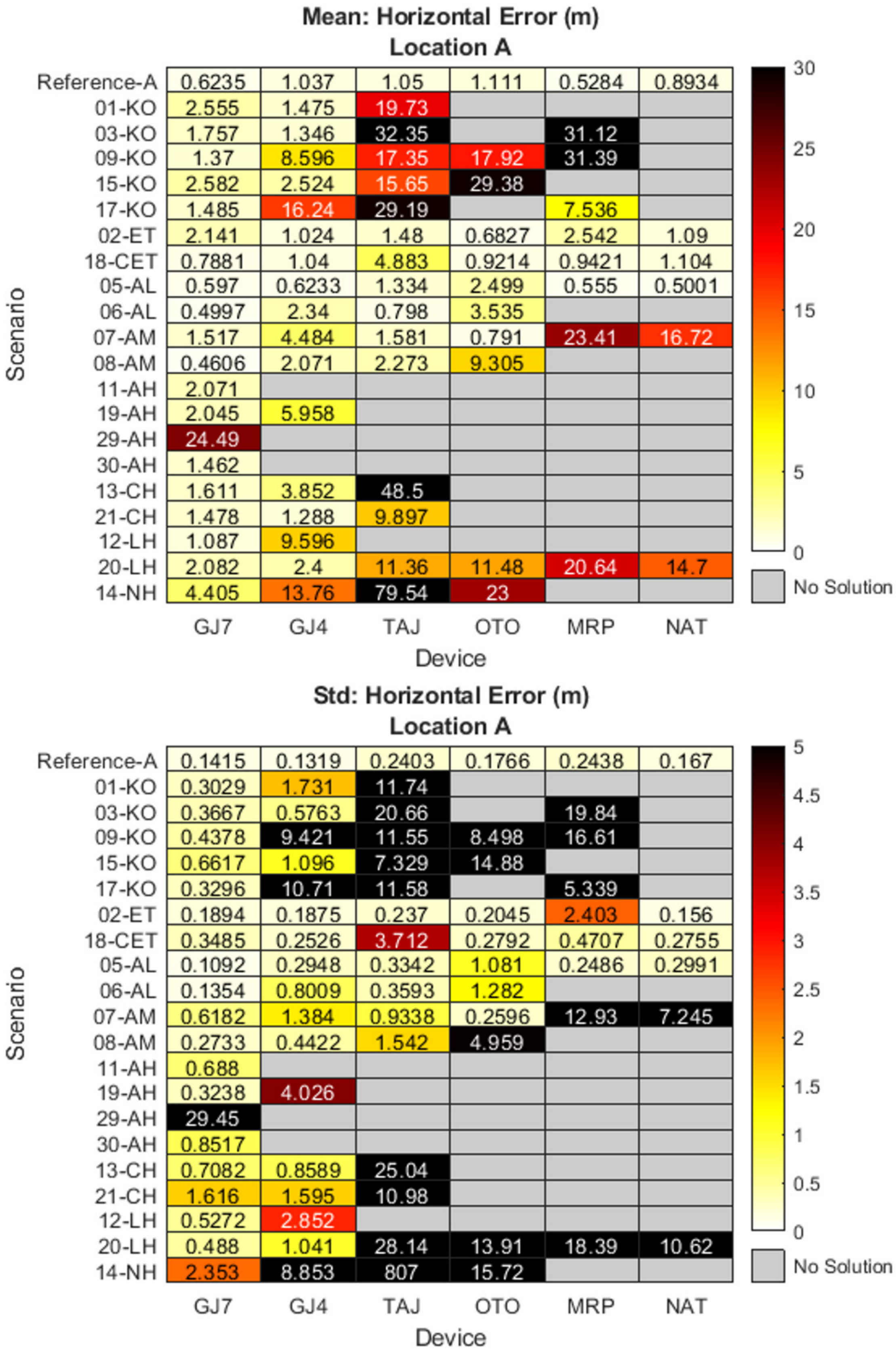
Reference position data was collected at each static location under clear conditions during reference time frames to characterize baseline performance for each device. Horizontal position errors were derived for each device by comparing the reported position to the reference position provided by the

PwrPak7 after adjusting for the device's measured physical offset on the van's roof. For certain sites, the van's position and orientation during the reference data collection was marked by a line on the ground. The van had two laser levels attached pointing down. Upon leaving the site and revisiting later, the van could be returned to approximately the same position and orientation by aligning the lasers with the ground markings. Horizontal alignment was consistently achieved within centimeters. (Note that location B was used for reference data collection as well as a hold position in the Dynamic 1 route at Melton. None of the scenarios had fully static data collection at this location.)

7.4.4.4 Static Response

The static response analysis investigated characteristics of horizontal position errors for each device during static scenarios. This analysis includes descriptive statistics as well as time series plots. Results are restricted to cases where a device reports position data for at least 60 seconds during the scenario, to avoid extremely low sample sizes.

The following figures show descriptive statistics for the horizontal position errors of each device (horizontal axis) throughout each static scenario (vertical axis). The title of the heatmap indicates the statistic (mean vs standard deviation) as well as the location. Lower values (light yellow) indicate favorable performance. Instances without sufficient position data available (i.e. less than 60 seconds) are left blank and indicated as No Solution. The top row of each heatmap shows nominal performance levels during a reference period without interference for comparison against the jamming and spoofing scenarios.



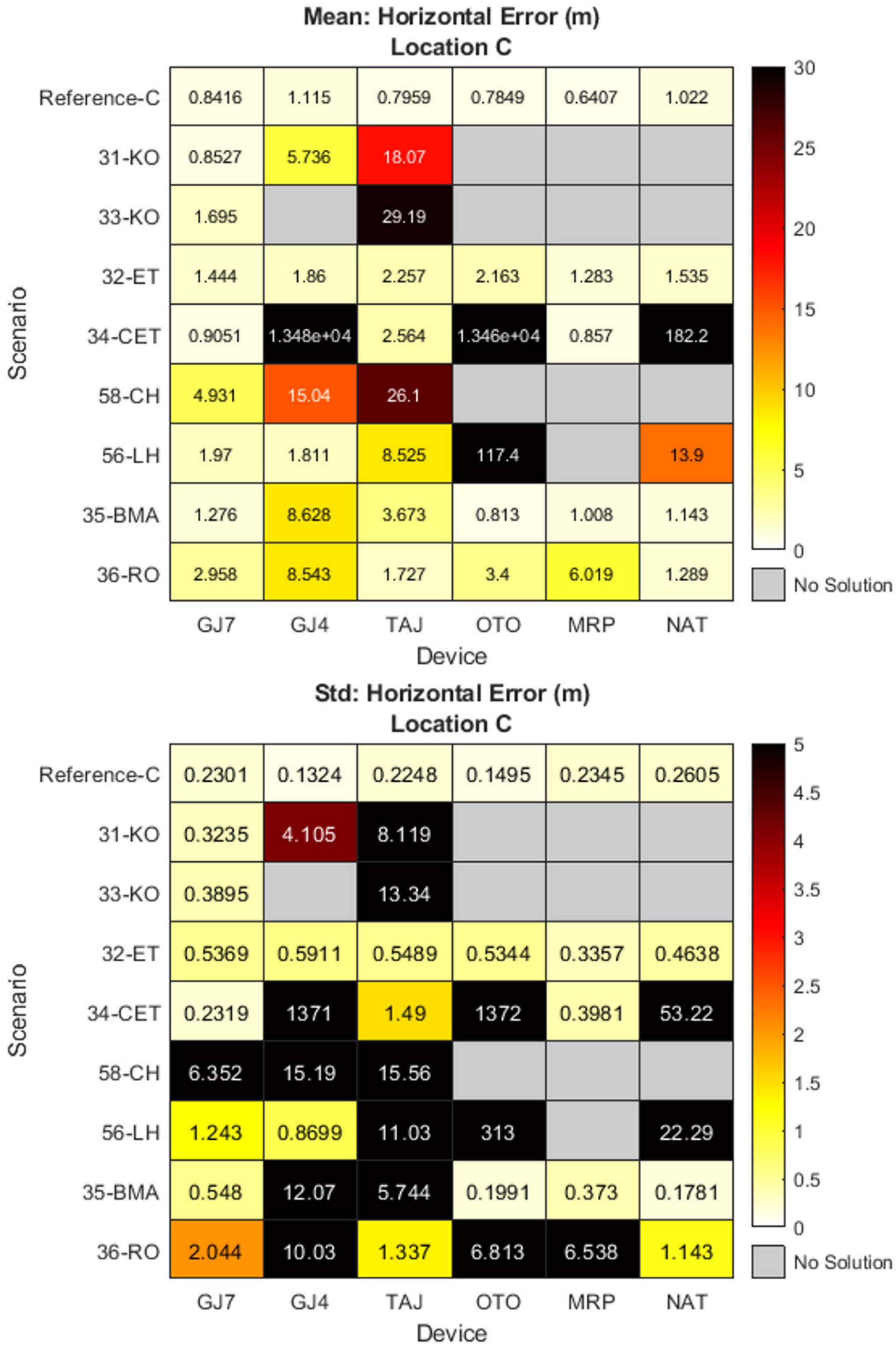
Mean: Horizontal Error (m)
Location A

Scenario	GJ7	GJ4	TAJ	OTO	MRP	NAT
Reference-A	0.6235	1.037	1.05	1.111	0.5284	0.8934
01-KO	2.555	1.475	19.73			
03-KO	1.757	1.346	32.35		31.12	
09-KO	1.37	8.596	17.35	17.92	31.39	
15-KO	2.582	2.524	15.65	29.38		
17-KO	1.485	16.24	29.19		7.536	
02-ET	2.141	1.024	1.48	0.6827	2.542	1.09
18-CET	0.7881	1.04	4.883	0.9214	0.9421	1.104
05-AL	0.597	0.6233	1.334	2.499	0.555	0.5001
06-AL	0.4997	2.34	0.798	3.535		
07-AM	1.517	4.484	1.581	0.791	23.41	16.72
08-AM	0.4606	2.071	2.273	9.305		
11-AH	2.071					
19-AH	2.045	5.958				
29-AH	24.49					
30-AH	1.462					
13-CH	1.611	3.852	48.5			
21-CH	1.478	1.288	9.897			
12-LH	1.087	9.596				
20-LH	2.082	2.4	11.36	11.48	20.64	14.7
14-NH	4.405	13.76	79.54	23		

Std: Horizontal Error (m)
Location A

Scenario	GJ7	GJ4	TAJ	OTO	MRP	NAT
Reference-A	0.1415	0.1319	0.2403	0.1766	0.2438	0.167
01-KO	0.3029	1.731	11.74			
03-KO	0.3667	0.5763	20.66		19.84	
09-KO	0.4378	9.421	11.55	8.498	16.61	
15-KO	0.6617	1.096	7.329	14.88		
17-KO	0.3296	10.71	11.58		5.339	
02-ET	0.1894	0.1875	0.237	0.2045	2.403	0.156
18-CET	0.3485	0.2526	3.712	0.2792	0.4707	0.2755
05-AL	0.1092	0.2948	0.3342	1.081	0.2486	0.2991
06-AL	0.1354	0.8009	0.3593	1.282		
07-AM	0.6182	1.384	0.9338	0.2596	12.93	7.245
08-AM	0.2733	0.4422	1.542	4.959		
11-AH	0.688					
19-AH	0.3238	4.026				
29-AH	29.45					
30-AH	0.8517					
13-CH	0.7082	0.8589	25.04			
21-CH	1.616	1.595	10.98			
12-LH	0.5272	2.852				
20-LH	0.488	1.041	28.14	13.91	18.39	10.62
14-NH	2.353	8.853	807	15.72		

Figure 24. Heatmaps with horizontal position error statistics by device and scenario for location A



Mean: Horizontal Error (m) Location C

Scenario	GJ7	GJ4	TAJ	OTO	MRP	NAT
Reference-C	0.8416	1.115	0.7959	0.7849	0.6407	1.022
31-KO	0.8527	5.736	18.07			
33-KO	1.695		29.19			
32-ET	1.444	1.86	2.257	2.163	1.283	1.535
34-CET	0.9051	1.348e+04	2.564	1.346e+04	0.857	182.2
58-CH	4.931	15.04	26.1			
56-LH	1.97	1.811	8.525	117.4		13.9
35-BMA	1.276	8.628	3.673	0.813	1.008	1.143
36-RO	2.958	8.543	1.727	3.4	6.019	1.289

Std: Horizontal Error (m) Location C

Scenario	GJ7	GJ4	TAJ	OTO	MRP	NAT
Reference-C	0.2301	0.1324	0.2248	0.1495	0.2345	0.2605
31-KO	0.3235	4.105	8.119			
33-KO	0.3895		13.34			
32-ET	0.5369	0.5911	0.5489	0.5344	0.3357	0.4638
34-CET	0.2319	1371	1.49	1372	0.3981	53.22
58-CH	6.352	15.19	15.56			
56-LH	1.243	0.8699	11.03	313		22.29
35-BMA	0.548	12.07	5.744	0.1991	0.373	0.1781
36-RO	2.044	10.03	1.337	6.813	6.538	1.143

Figure 25. Heatmaps with horizontal position error statistics by device and scenario for location C

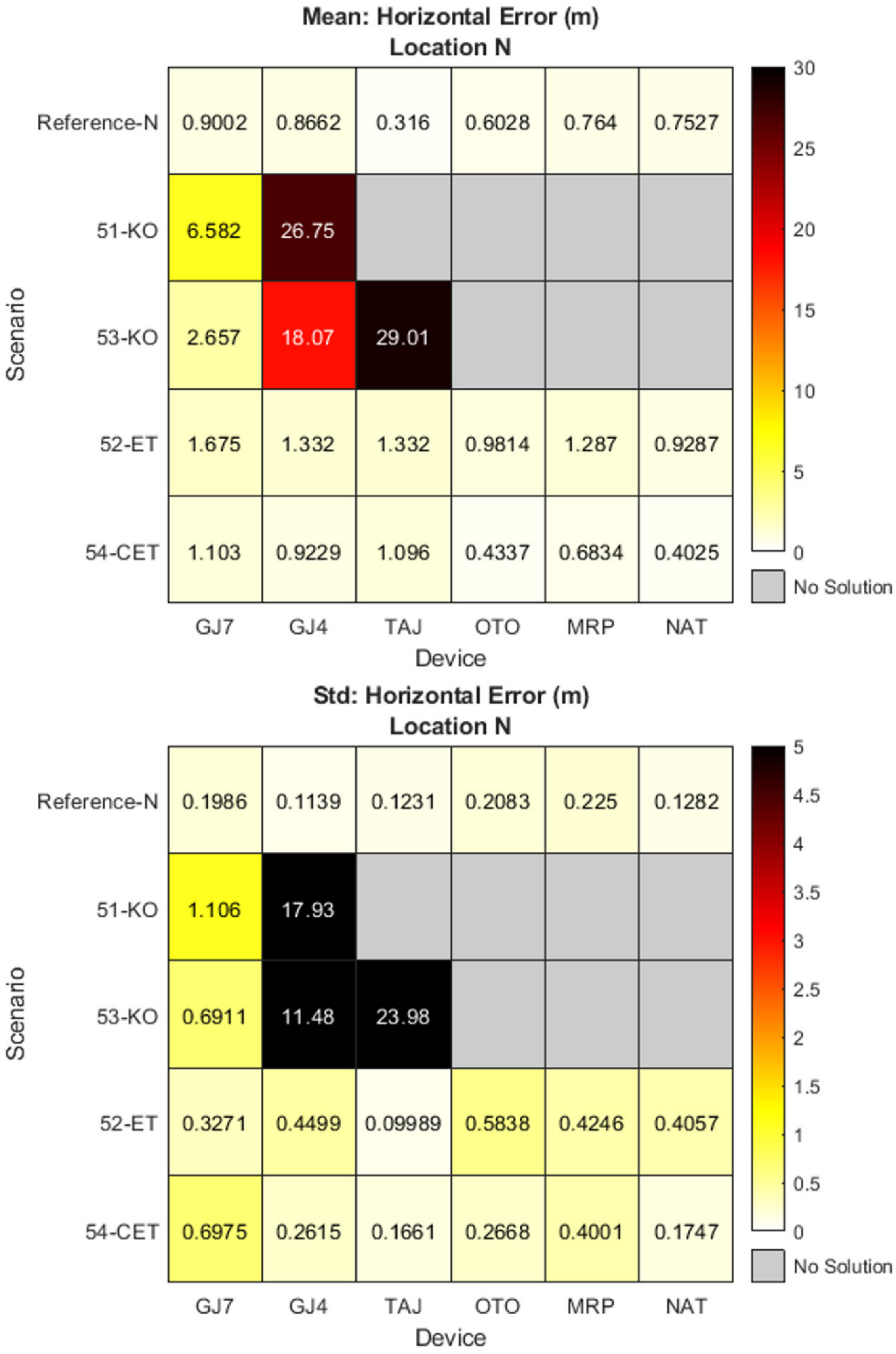


Figure 26. Heatmaps with horizontal position error statistics by device and scenario for location N

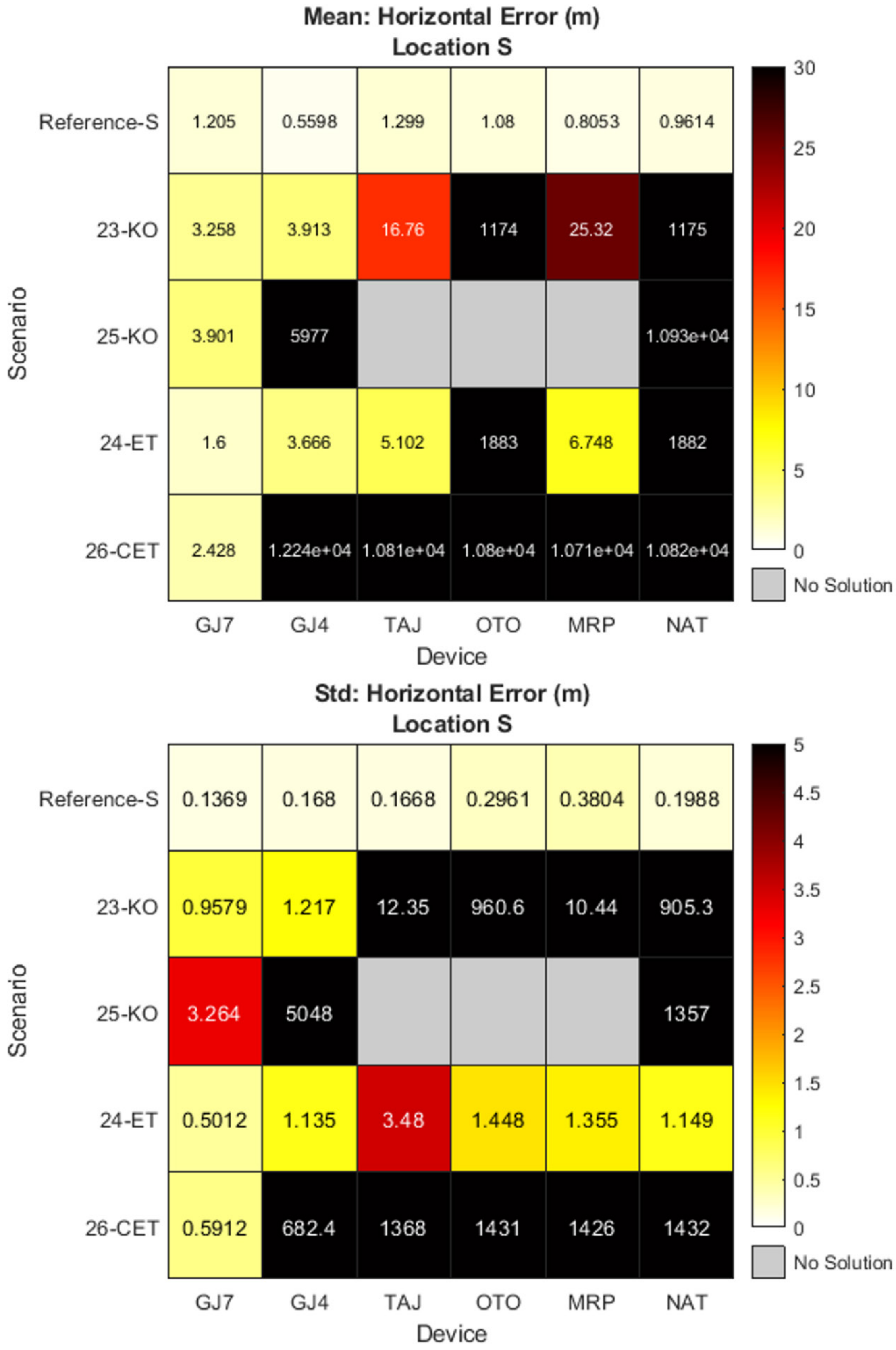


Figure 27. Heatmaps with horizontal position error statistics by device and scenario for location S

The devices show a variety of performance levels across different scenarios. Overall, the heatmaps indicate that GJ7 is typically the top performer, followed by GJ4. The heatmaps also suggest that certain devices were spoofed during three spoofing events, as indicated by a large mean horizontal position error or a large standard deviation:

- 34-CET: GJ4, OTO, NAT
- 24-ET: OTO, NAT
- 26-CET: GJ4, TAJ, OTO, MRP, NAT

Figure 24 displays the horizontal position error time series during scenario 26-CET as an example. The top plot shows an extended view of the errors. This plot demonstrates the wide range of errors from the scale of centimeters to over 10,000 meters. The middle plot shows the same data with a more focused view on errors below 5 meters. The bottom plot indicates times for which valid position data was reported for each device. All devices except GJ7 reported large horizontal position errors above 10,000 meters, which potentially indicate spoofing.

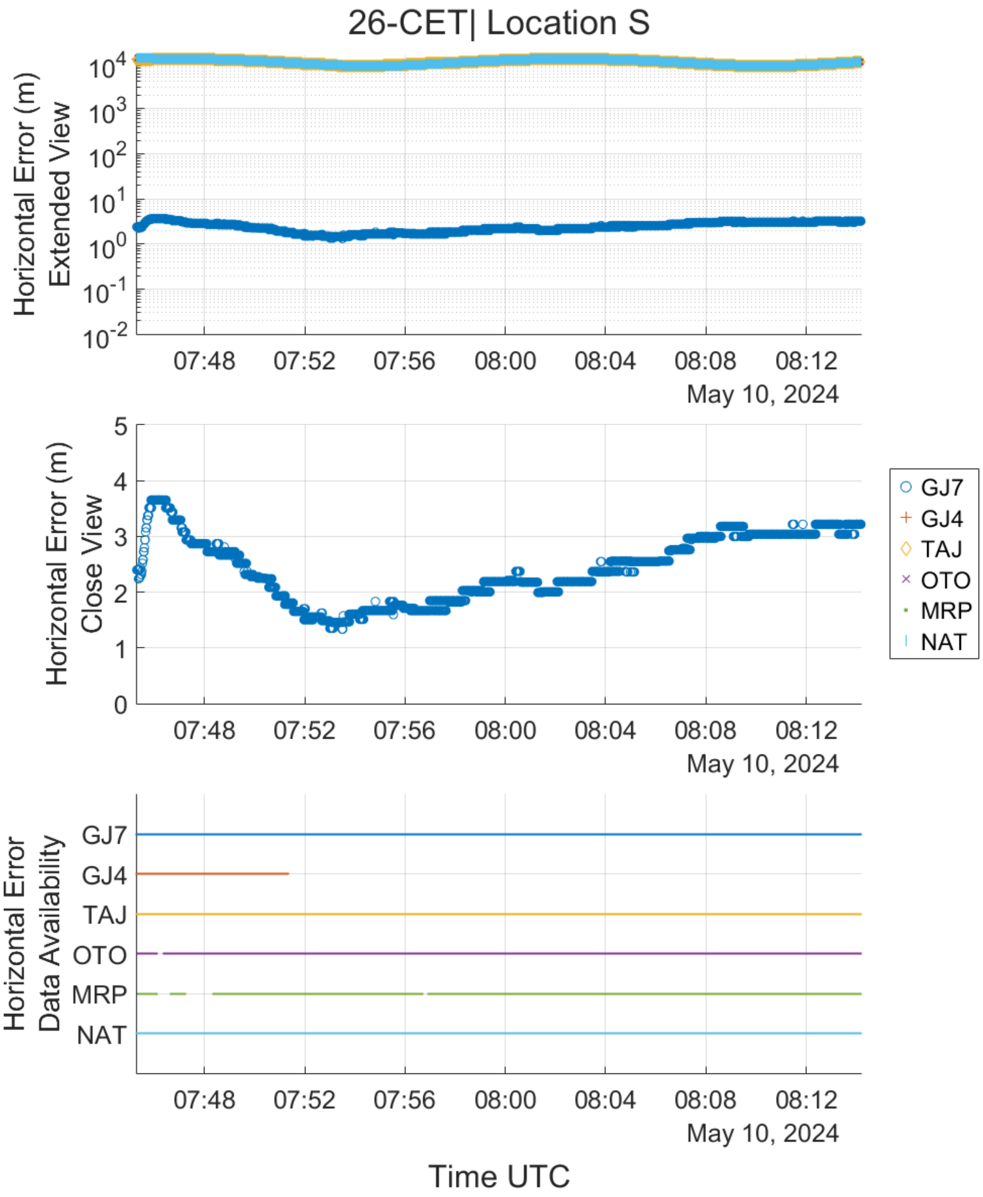


Figure 28. Time series of horizontal position errors during spoofing scenario 26-CET

The full set of horizontal position error time series plots for the static response analysis can be found in Appendix B: NAVFEST Static Response Analysis .

The results of the static response analysis indicate an overall relative order or performance from high to low: GJ7, GJ4, TAJ, OTO, MRP, NAT. However, there are occasional exceptions for certain scenarios.

7.4.4.5 Static Recovery

The static recovery analysis investigated the ability of each device to return to baseline performance levels after jamming/spoofing during static scenarios ended. This analysis was restricted to static scenarios with at least eleven minutes immediately after the scenario ended for which the van remained stationary with no interference observed, to allow sufficient time and opportunity for devices to recover to baseline performance levels. This analysis investigated recovery statistics based on recovery success vs failure, time to recovery, and recovery start condition.

Note that GJ4, TAJ, OTO, MRP, and NAT were excluded for scenario 29-AH due to a lack of usable data caused by an earlier event. Specifically, during scenario 26-CET the date reported by these five receivers jumped forward by 72 weeks, after which the receivers ceased updating time and position for the reminder of the night. Thus, only GJ7 was included for scenario 29-AH.

7.4.4.6 Recovery Definition

Device performance recovery was defined based on the characteristics of the horizontal position errors over time. The horizontal errors from the static reference data sets were used to quantify the baseline performance levels. A nominal threshold representing the upper bound of baseline performance was defined for each device by scaling the 99th percentile of the reference horizontal position errors by a factor of 1.1, to avoid the influence of extreme outliers.

A recovery window is defined as the 10 minutes immediately following the end of the static jamming/spoofing scenario. A device has recovered when it reports a horizontal position error below the threshold within the recovery window, and then continues to report horizontal position errors below the threshold for at least 60 seconds (i.e., the confirmation window). The device fails to recover if this condition is not met. Figure 25 demonstrates an example of device recovery.

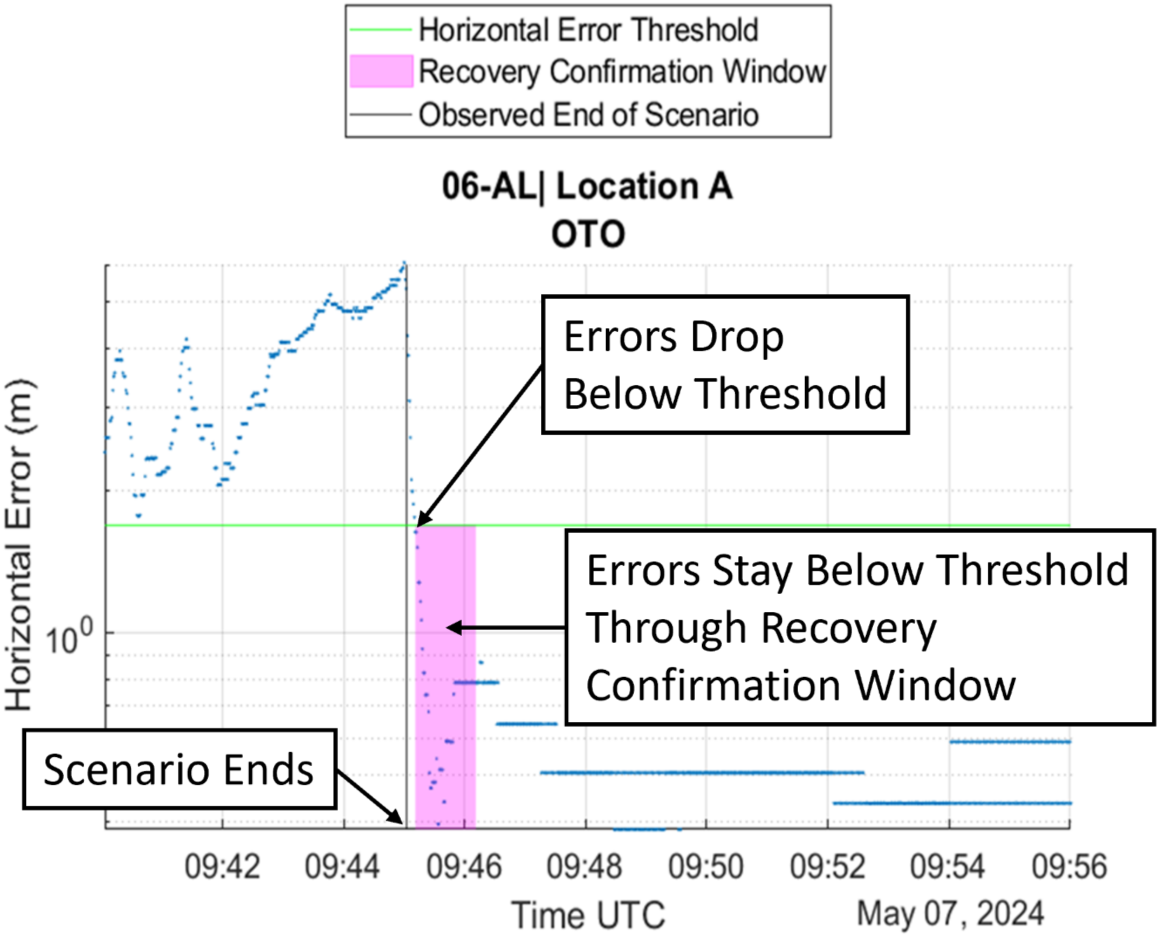


Figure 29. Time Series of horizontal position errors demonstrating performance recovery after a static jamming scenario

The full set of time series plots for the static recovery analysis can be found in Appendix C: NAVFEST Static Recovery Analysis Time Series Plots.

7.4.4.7 Recovery Start Condition

The recovery start condition for a device is defined based on the horizontal position error value reported at the end of the static jamming/spoofing scenario:

- No Error: No horizontal position reported
- Above Nominal Threshold: Horizontal position error above threshold
- Below Nominal Threshold: Horizontal position error below threshold

Recovery start condition is an important consideration for time to recovery. For example, if a device already demonstrates baseline performance levels at the end of a scenario, there may not be any delay until it is considered recovered for this analysis (i.e., time to recovery is zero seconds). Conversely, if the device reports abnormally large errors or fails to report a position at the end of the static scenario, it may be expected to take some time to recover.

7.4.4.8 Static Recovery Results

Table 6 displays the number of static scenarios with no recovery for each device, grouped by recovery start condition.

Table 6. Static scenarios with failure to recover by device and start condition

Recovery Start Condition	GJ7	GJ4	TAJ	OTO	MRP	NAT
Above Nominal Threshold	0	1	1	1	1	0
Below Nominal Threshold	1	1	0	0	0	0
No Error	0	0	0	0	0	1

All devices recovered for most static jamming and spoofing scenarios. GJ4 failed to recover twice, while all other devices failed to recover once. All devices failed to recover after scenario 24-ET. A root cause investigation of those failures for scenario 24-ET was inconclusive. Possible explanations could include the atypical proximity of the van to the emitter during the 24-ET scenario, or lingering effects from the spoofing signals. GJ4 failed to recover after scenario 06-AL; a root cause investigation for scenario 06-AL was inconclusive, though inspection of the horizontal errors suggests that the device was trending towards a recovery at the end of the recovery window. Figure 26 shows the distribution of time to recovery for each device.

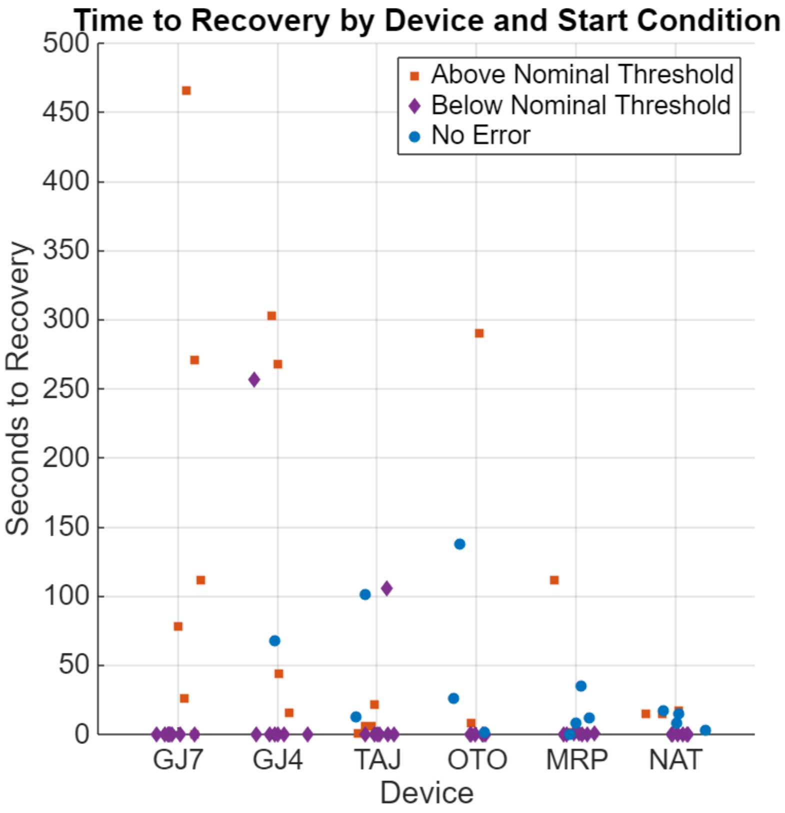


Figure 30. Time to recovery distributions for each device

Most devices demonstrate a range of times to recovery. NAT has consistently low times to recovery. This could indicate that the sophistication of the protective devices introduces a lag in recovery relative to the unprotected device. That is, there may be a hysteresis period where jamming signals must be absent before a solution is output. Such a delay in recovery may help avert the use of invalid solutions. The other devices show times ranging from zero seconds (immediate recovery, often with start conditions already below nominal threshold) to several minutes.

The notably high time to recovery for GJ7 occurred during scenario 29-AH. There are no analogous data points from other devices to compare against, because the other devices were excluded from the analysis for this scenario due to disruption of reported dates during data collection. It is unknown if the other devices would have produced similarly large times to recover for this scenario.

7.4.4.9 NAVFEST Conclusions

In general, the results of the NAVFEST data analysis indicated a relative overall order of device performance under a variety of spoofing and jamming conditions, though exceptions occasionally occurred for certain performance criteria in certain scenarios. The overall order of device performance is listed below from high to low:

1. GJ7

2. GJ4
3. TAJ
4. OTO
5. MRP
6. NAT

This order of performance is consistent with the level of sophistication of the protection technologies. For example, more elements are expected to provide greater protection than fewer elements.

8. Conclusions and Recommendations

Threats to GNSS positioning information, both incidental and nefarious, have become a fact of life. For critical infrastructure and operational environments with safety of life implications, some threats to GNSS can have devastating impacts. Per EO 13905, it is incumbent upon critical infrastructure owners and operator to foster the responsible use of PNT, with a particular focus on GPS. During the MARAD, Phase II test effort, several protective technologies were evaluated, both in operational settings via live sea trials and electronic warfare simulation at NAVFEST. The results of the performance analysis have yielded intuitive results. That is, the level of protection provided by the equipment-under-test has scaled with sophistication, and more explicitly the number of elements, i.e., antennas, the system employs.

This was particularly evident at NAVFEST where multiple jamming emitters were used at different locations simultaneously. CRPAs, by design, create discrete adaptive nulls that scale with the number of elements. For example, a two element CRPA can create one directional null to mitigate interference coming from a particular location. A three element CPRA can produce two discrete nulls, and so forth. There are other performance factors to consider, such as the depth of the null which dictates how much jamming power can be mitigated or switching speed which determines how quickly the nulls can form and adapt to changes in jammer location.

With this understanding of how the technology works, it is not surprising that the GAJT-7, seven element CRPA, was able to outperform CRPAs with fewer elements. The capability to create up to six adaptive nulls allowed the GAJT-7 to maintain a valid solution throughout most of the multi-jammer scenarios at NAVFEST. There are, however, other considerations beyond performance.

Although the GAJT-7 outperformed the CRPAs with fewer elements, it is also apparent from the test results that some protection is better than no protection. During many incidents at sea, there may be no more than one or two emitters within range. There may, in fact, be few instances where a MARAD vessel would be subjected to six jamming sources simultaneously, although these instances likely exist when navigating near land in an area of conflict. The decision regarding how much protection is enough can be aided by other practical concerns such as cost, vendor lead times, ease of integration and ITAR considerations.

It is no surprise that the cost of the protective devices rises with complexity, feature set, and general performance. Additionally, although all the tested technologies are unintrusive in that they either replace an existing antenna or are installed in-line between an antenna and receiver, some of the devices require separate connections for power, RF, and ancillary data via a serial port, whereas others only require a standard RF connection to the receiver. Lead times will need to be discussed individually with vendors and will have dependencies on specified requirements and quantities requested.

ITAR restrictions on CPRA technology are another important consideration. The United States Munitions List (USML) Category XI(c)(10) lays out specific feature limitations which greatly restrict the capabilities of CPRA devices for civil applications. The main limitations dictate fewer than four elements, with additional limits on null depth, signal attenuation and speed. Although well intended when first established, these restrictions are outdated and create unneeded threat exposure to critical infrastructure. On January 17, 2025, The U.S. State Department which is responsible for the USML has published the interim final rule which removes ITAR restrictions on CRPA technology allowing integration of these antennas as a protective solution as recommended by the Positioning, Navigation and Timing Advisory Board (PNTAB). The final rule is expected to be effective September 15, 2025[10].

The primary Phase II recommendation is that MARAD invest in and implement GPS-protective technology for RRF and other MARAD vessels as soon as possible. The best choice of protective solutions among those tested during the PNT Pilot Program, Phase II effort should be subject to a careful consideration of device performance and specifications, cost, ease of integration, lead times, and ITAR regulations. The secondary recommendation is for MARAD to adopt a layered approach for adding complementary PNT technologies that meet the PNT resilience for operational performance under EO 13905 developed PNT Profiles. That is, GPS-independent sources of PNT should be included as inputs to a ship's navigation system. Such inputs serve as cross-checks to the validity of GPS derived solutions for the NISTIR 8323 "detect" function and potentially as a PNT source for recovery in the event of GNSS compromise or denial.

[10] https://www.federalregister.gov/documents/2025/01/17/2025-01313/international-traffic-in-arms-regulations-us-munitions-list-targeted-revisions

9. Appendix A: NAVFEST Scenario Time Frames

This appendix contains plots comparing scheduled and observed scenario time frames for all nights of testing at NAVFEST.

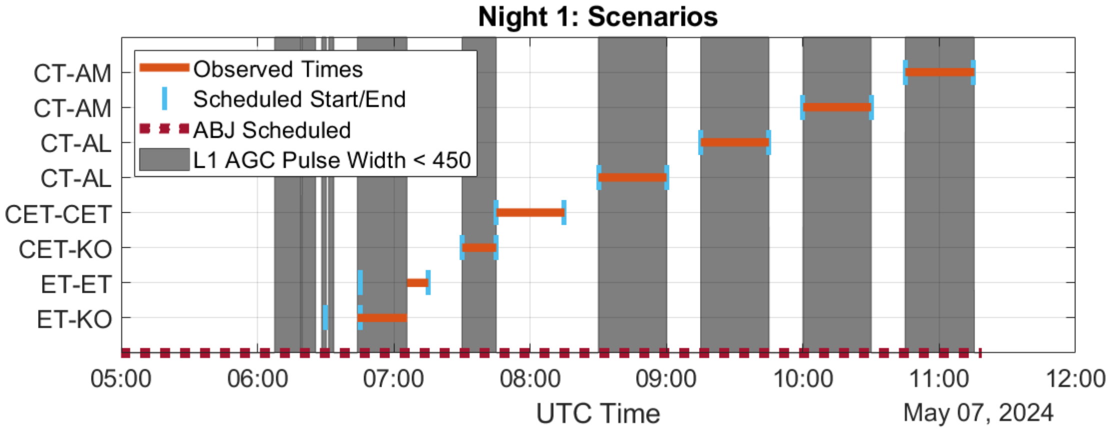


Figure 31. Scenario time frames for Night 1

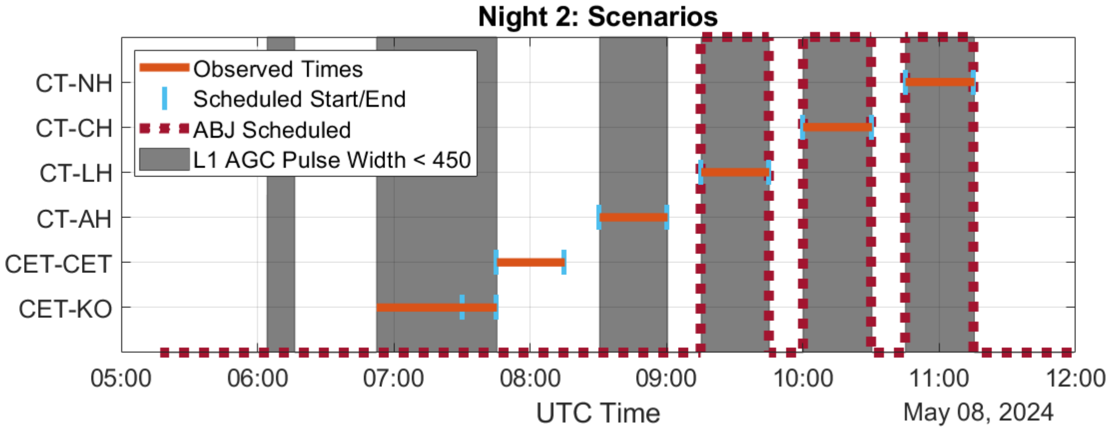


Figure 32. Scenario time frames for Night 2

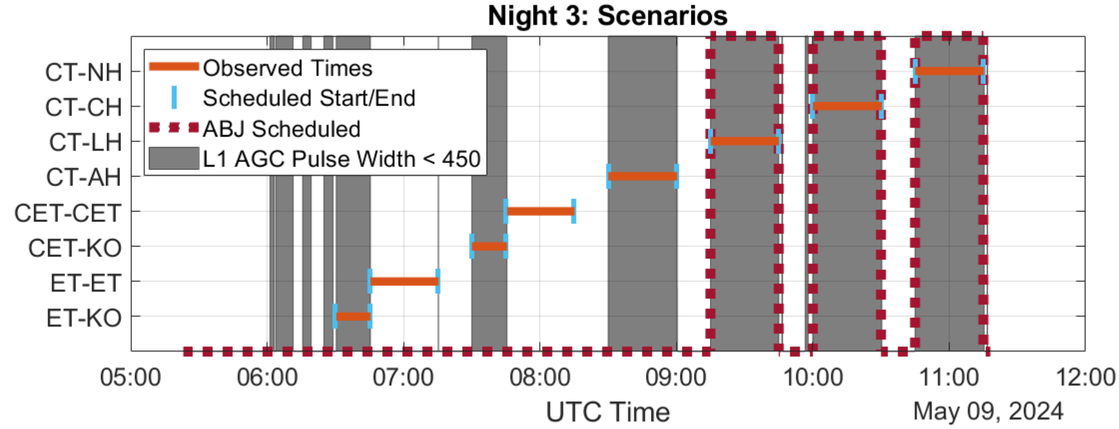


Figure 33. Scenario time frames for Night 3

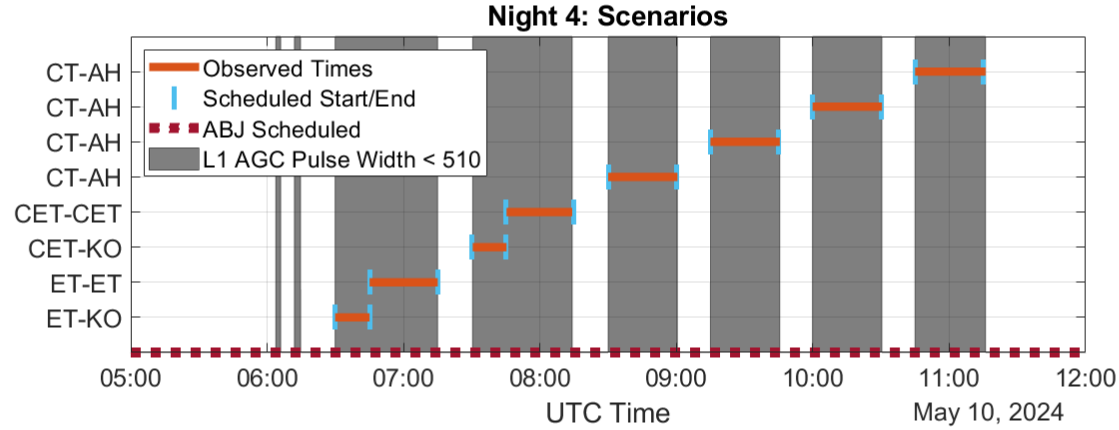


Figure 34. Scenario time frames for Night 4

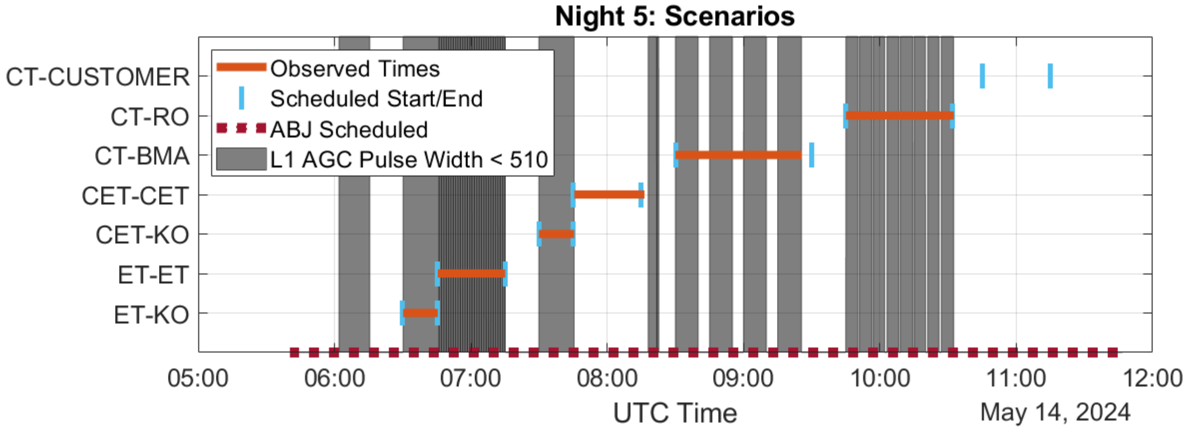


Figure 35. Scenario time frames for Night 5

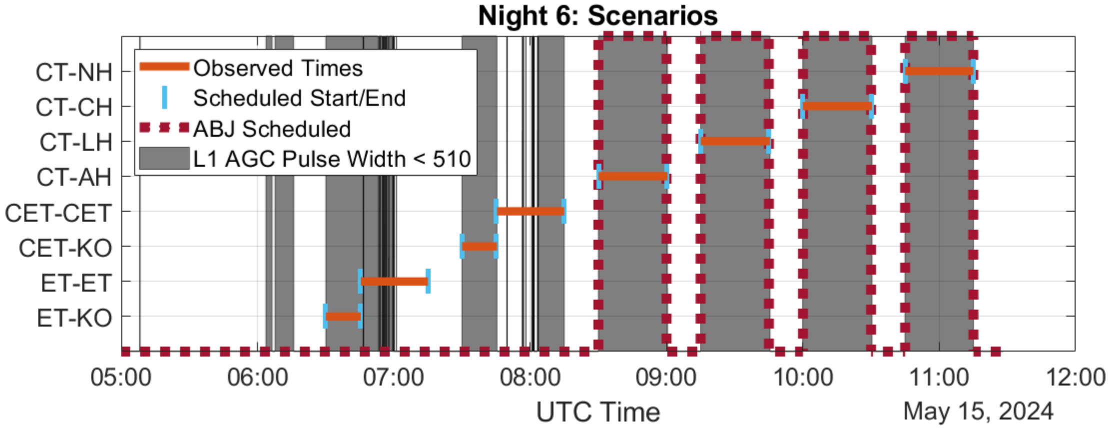


Figure 36. Scenario time frames for Night 6

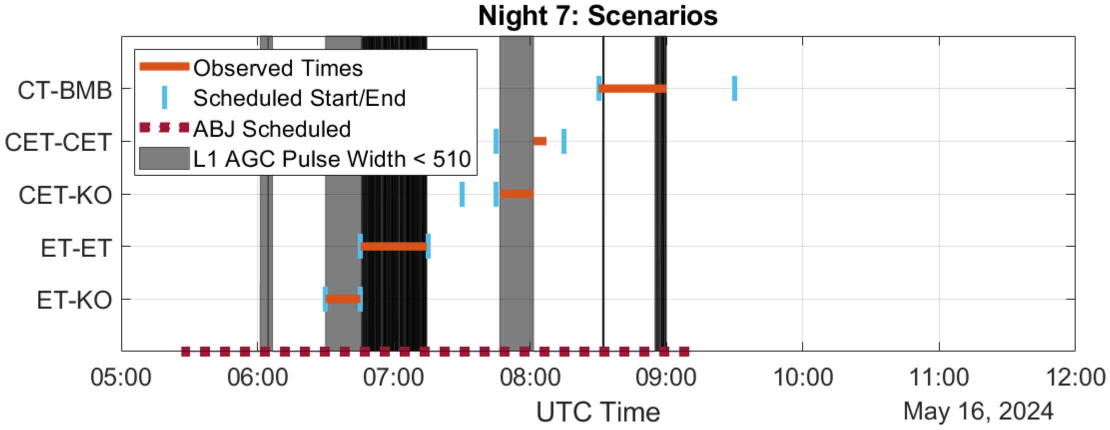


Figure 37. Scenario time frames for Night 7

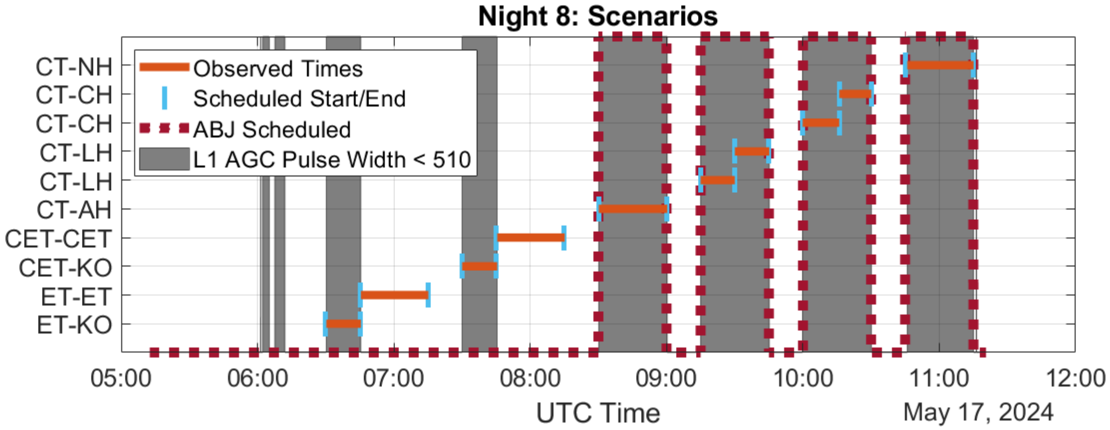


Figure 38. Scenario time frames for Night 8

10. Appendix B: NAVFEST Static Response Analysis Time Series Plots

This appendix contains horizontal position error time series plots for all scenarios used in the NAVFEST static response analysis.

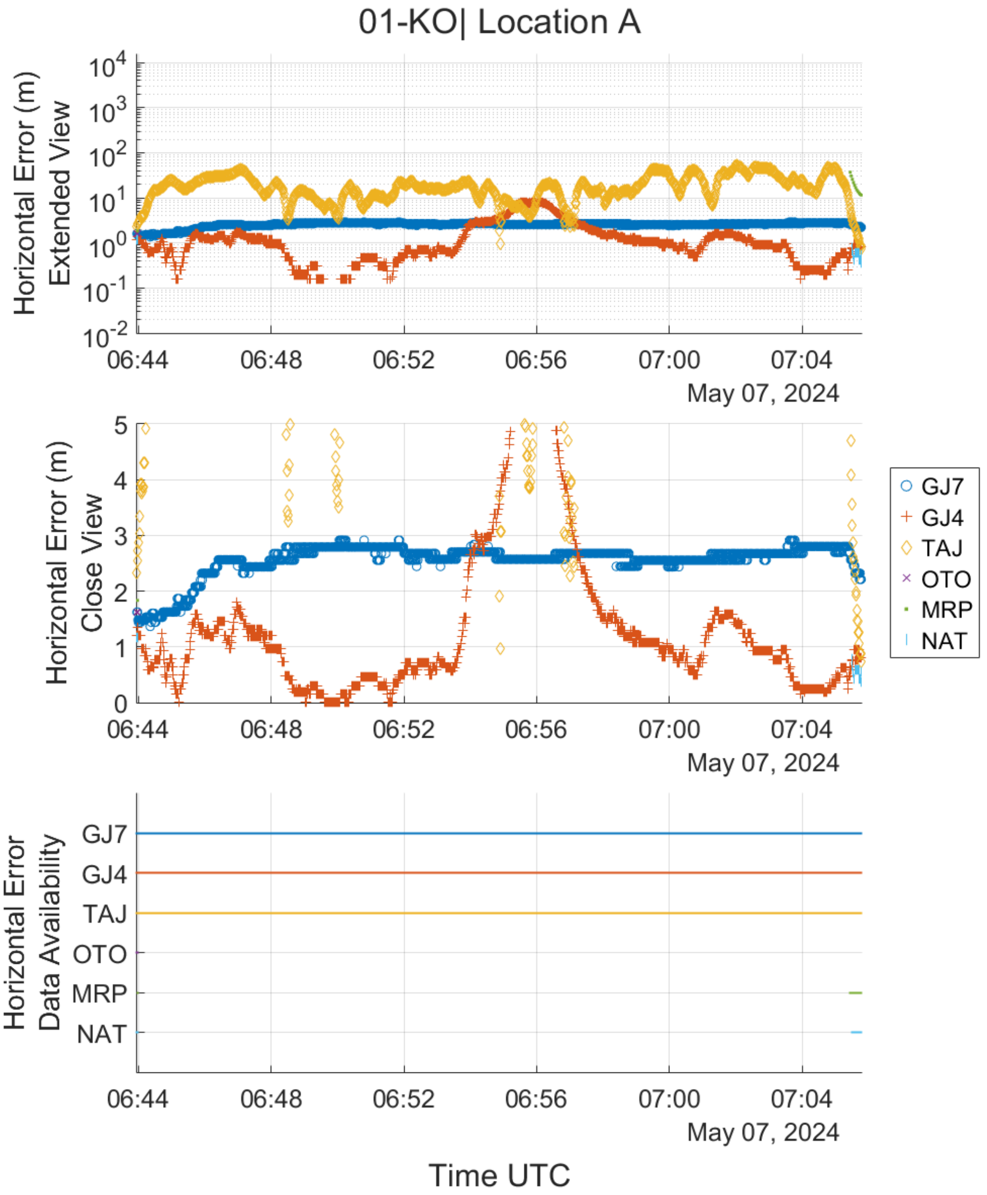


Figure 39. Horizontal position errors during scenario 01-KO

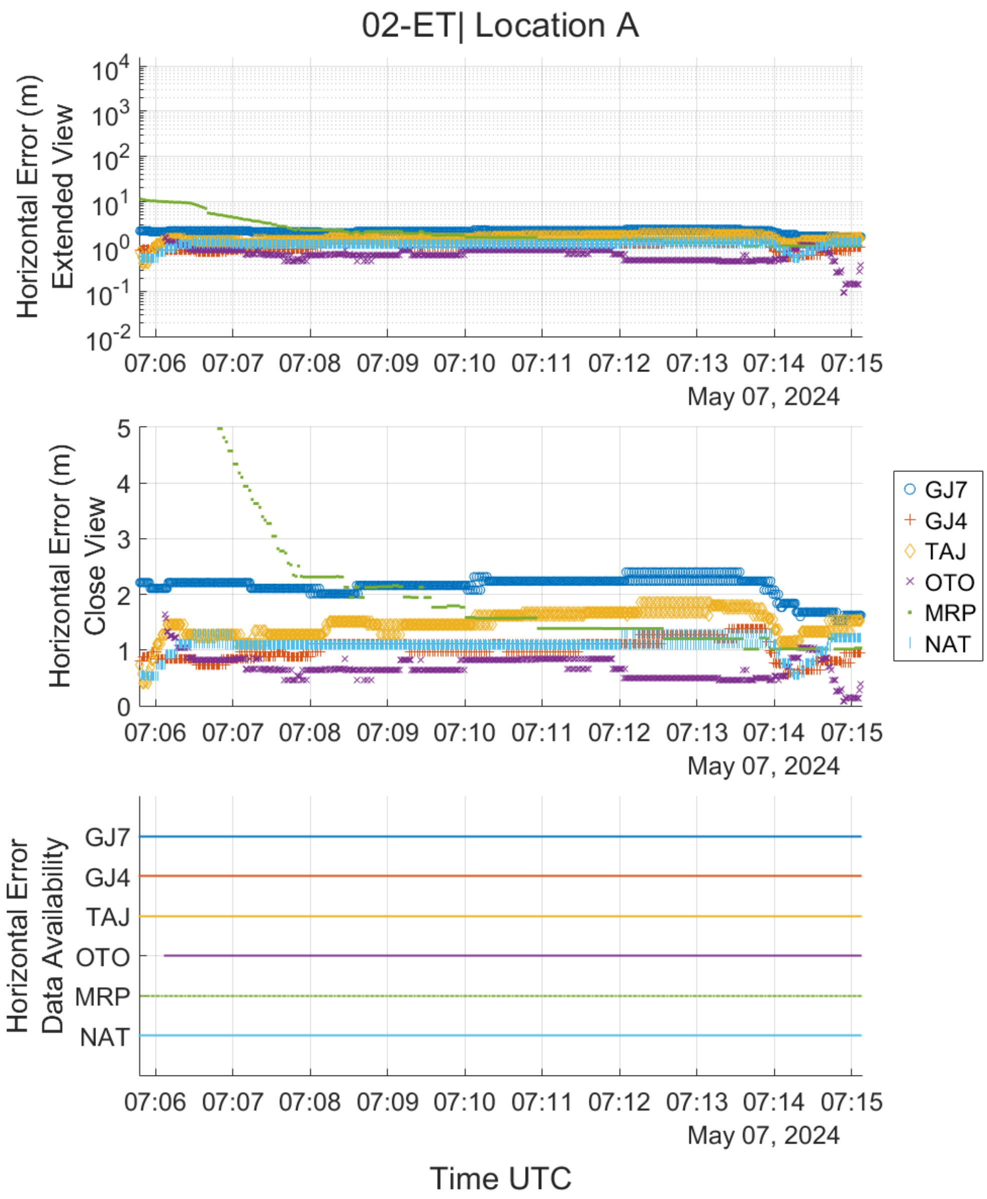


Figure 40. Horizontal position errors during scenario 02-ET

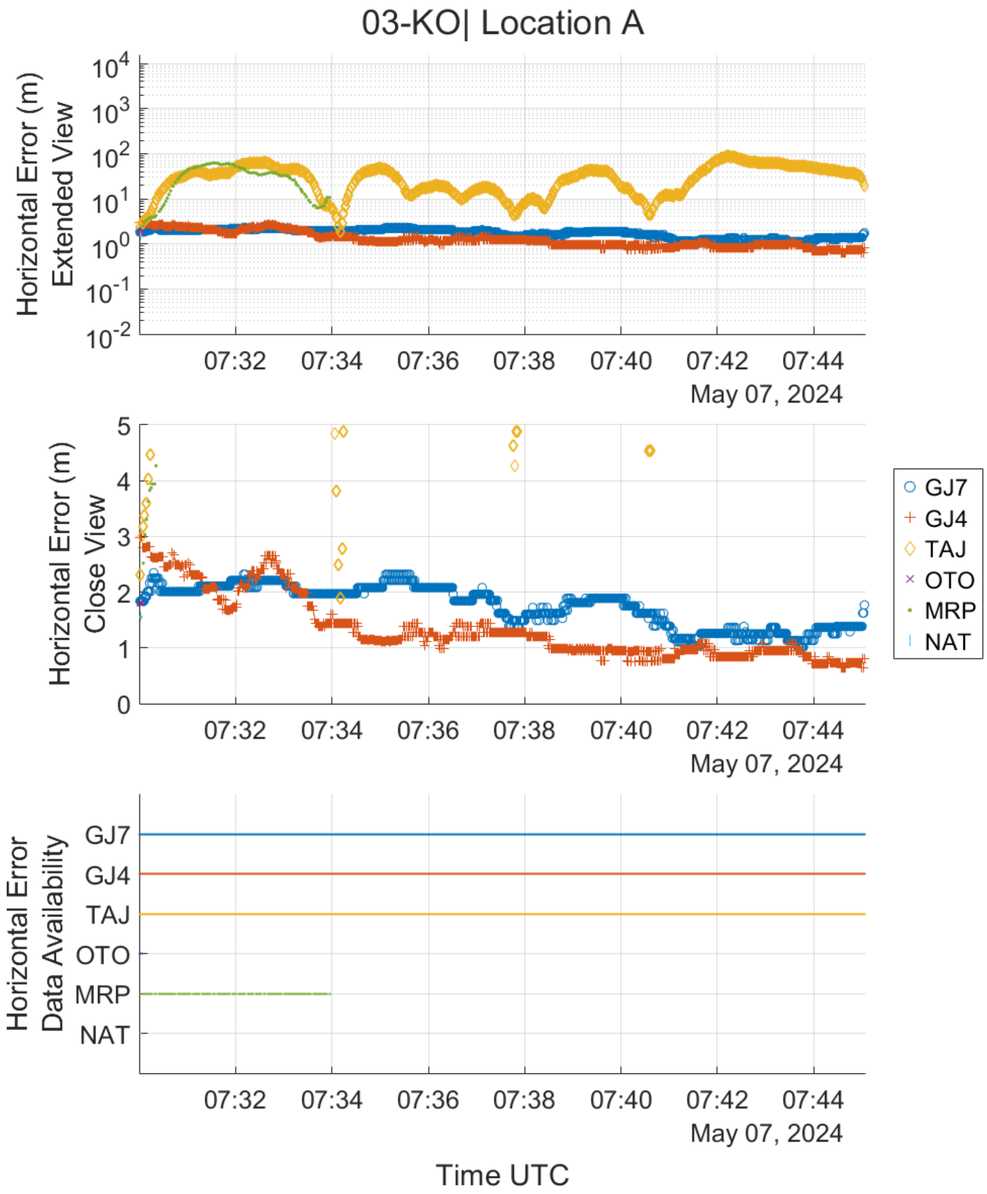


Figure 41. Horizontal position errors during scenario 03-KO

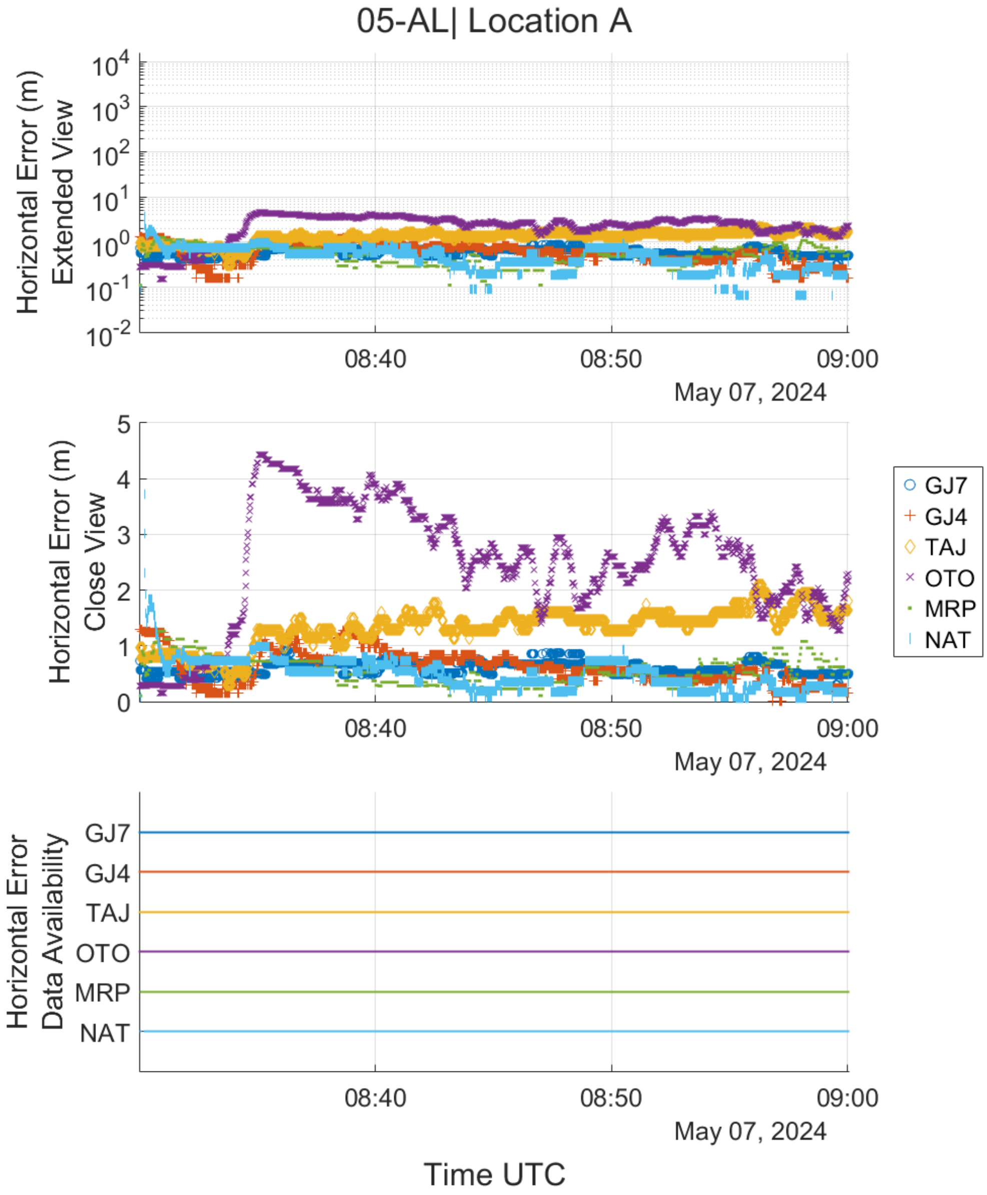


Figure 42. Horizontal position errors during scenario 05-AL

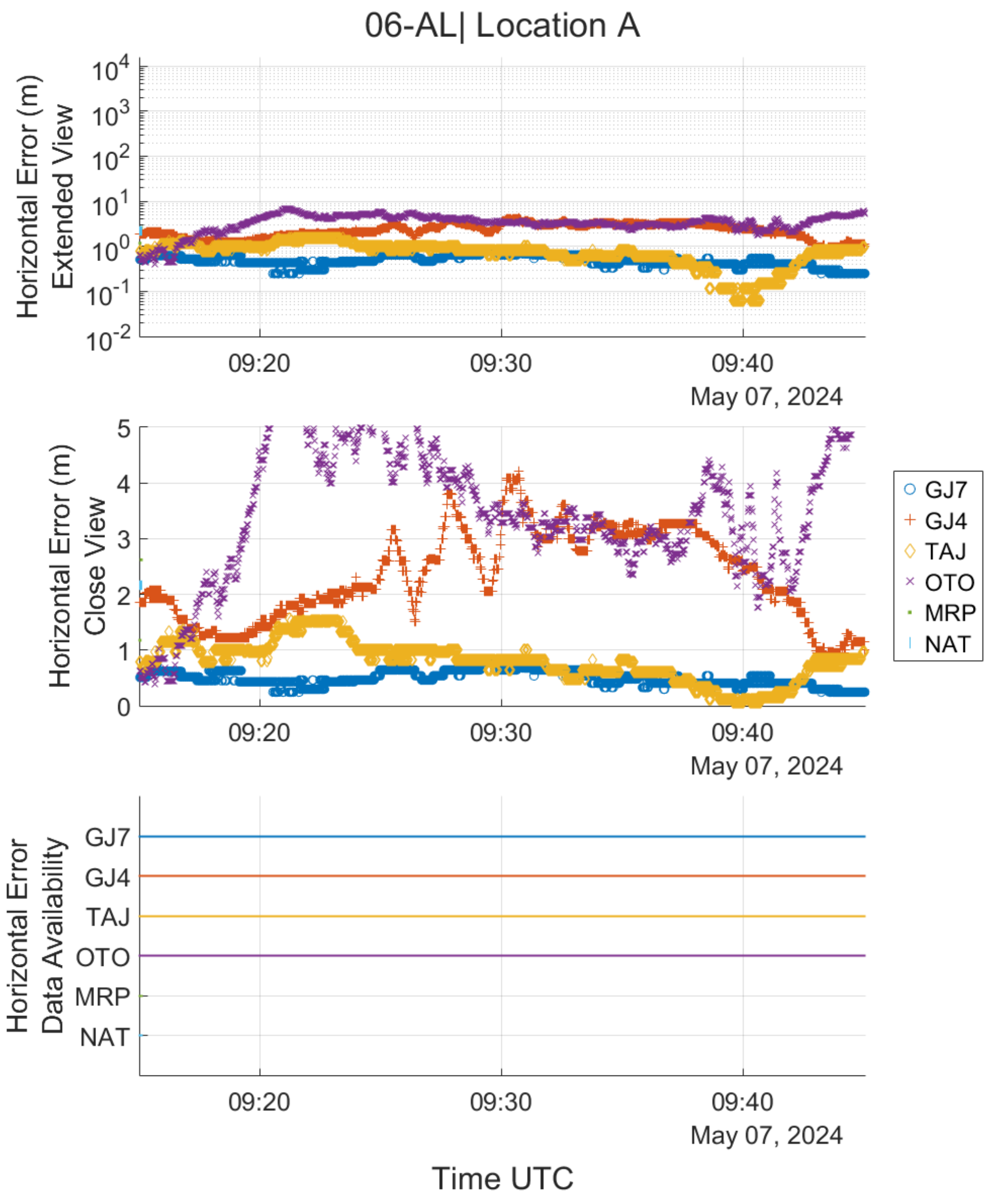


Figure 43. Horizontal position errors during scenario 06-AL

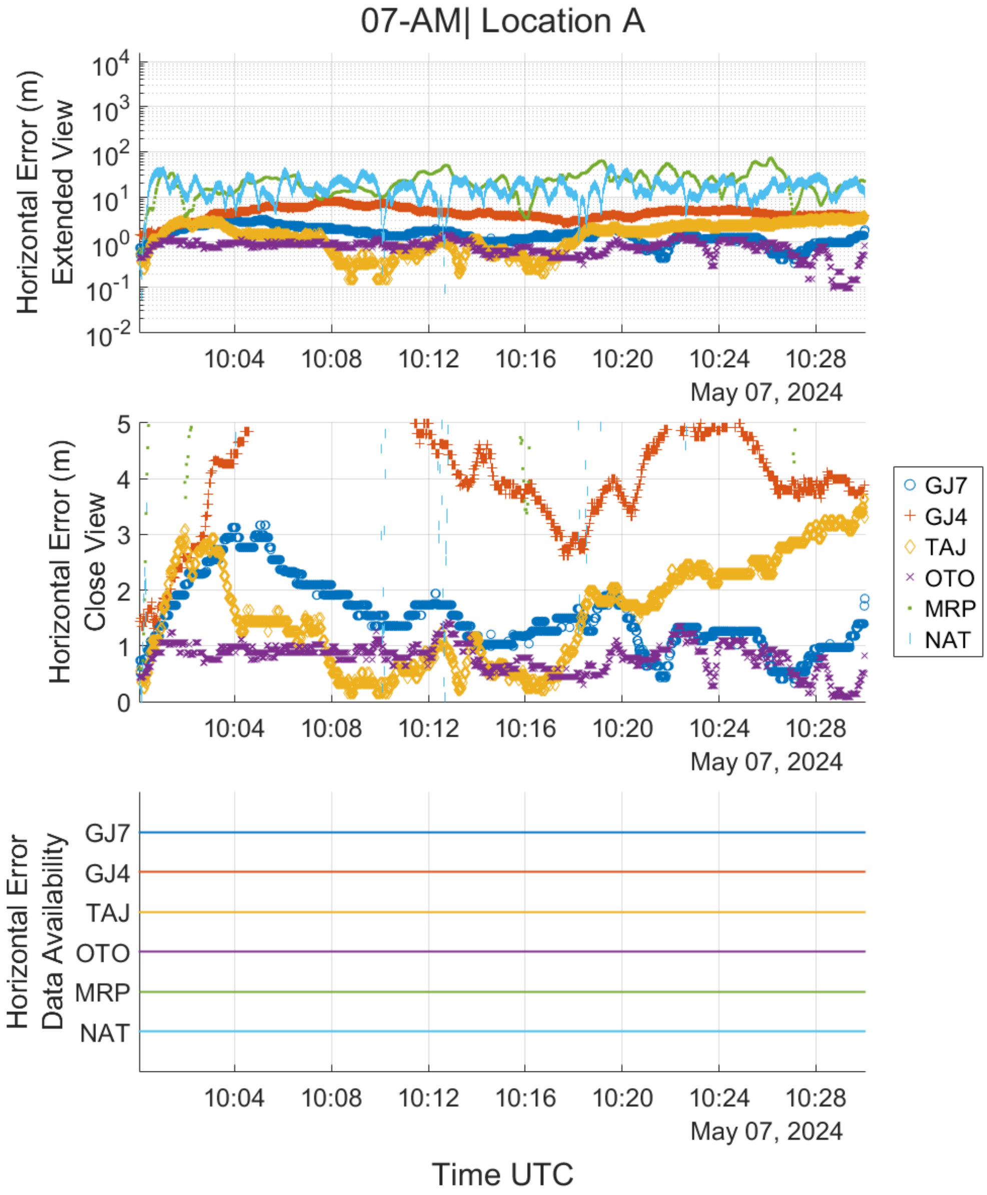


Figure 44. Horizontal position errors during scenario 07-AM

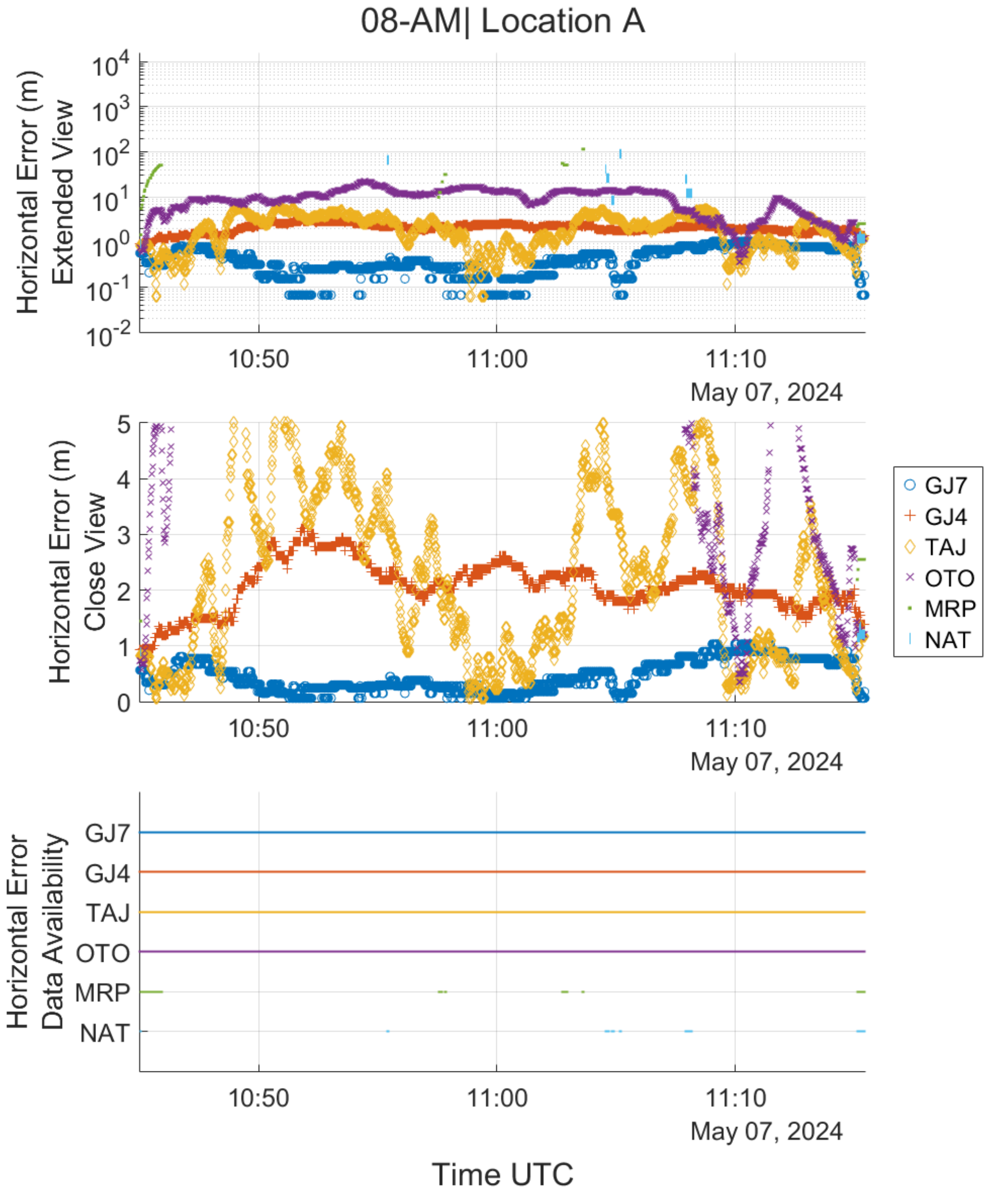


Figure 45. Horizontal position errors during scenario 08-AM

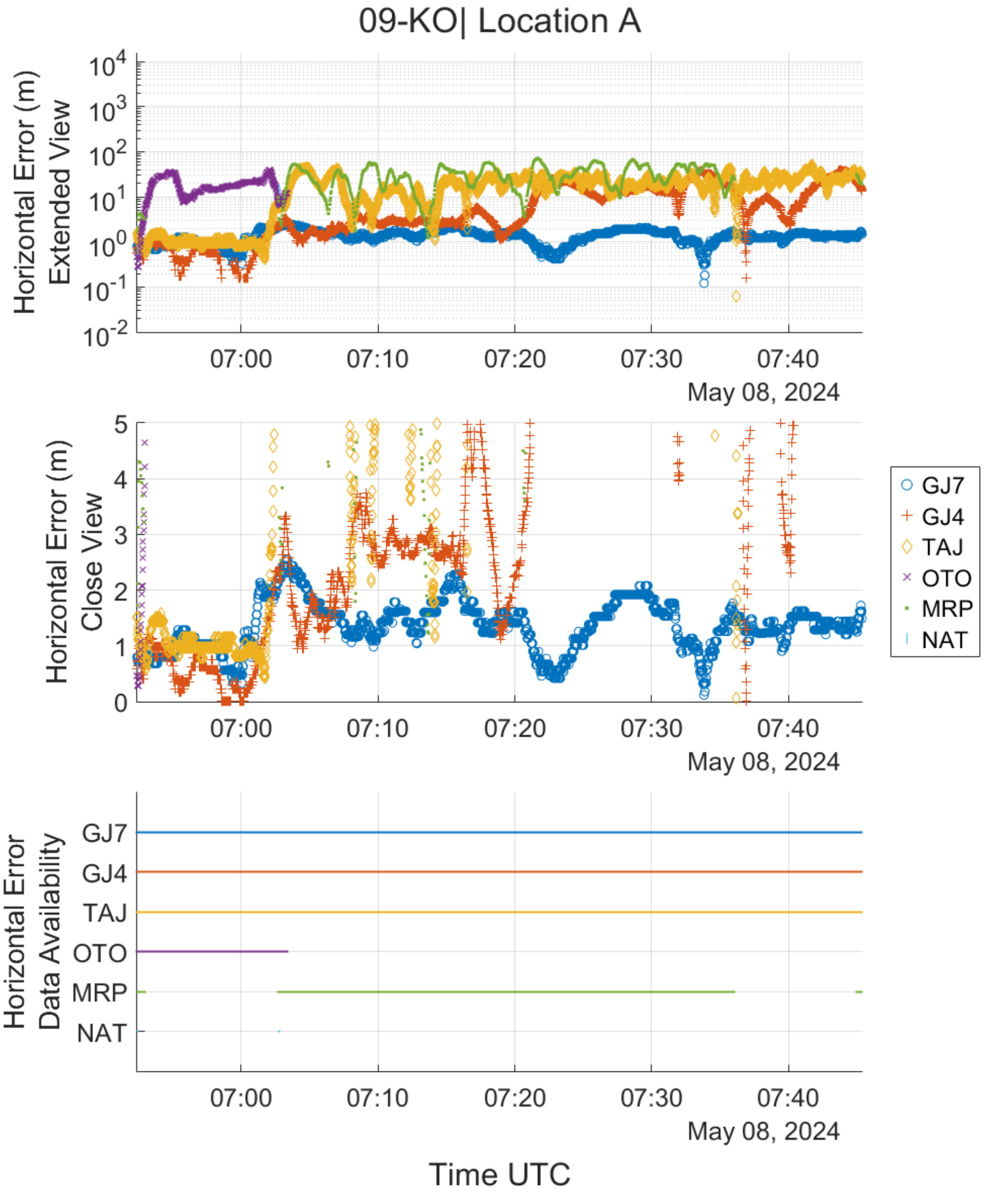


Figure 46. Horizontal position errors during scenario 09-KO

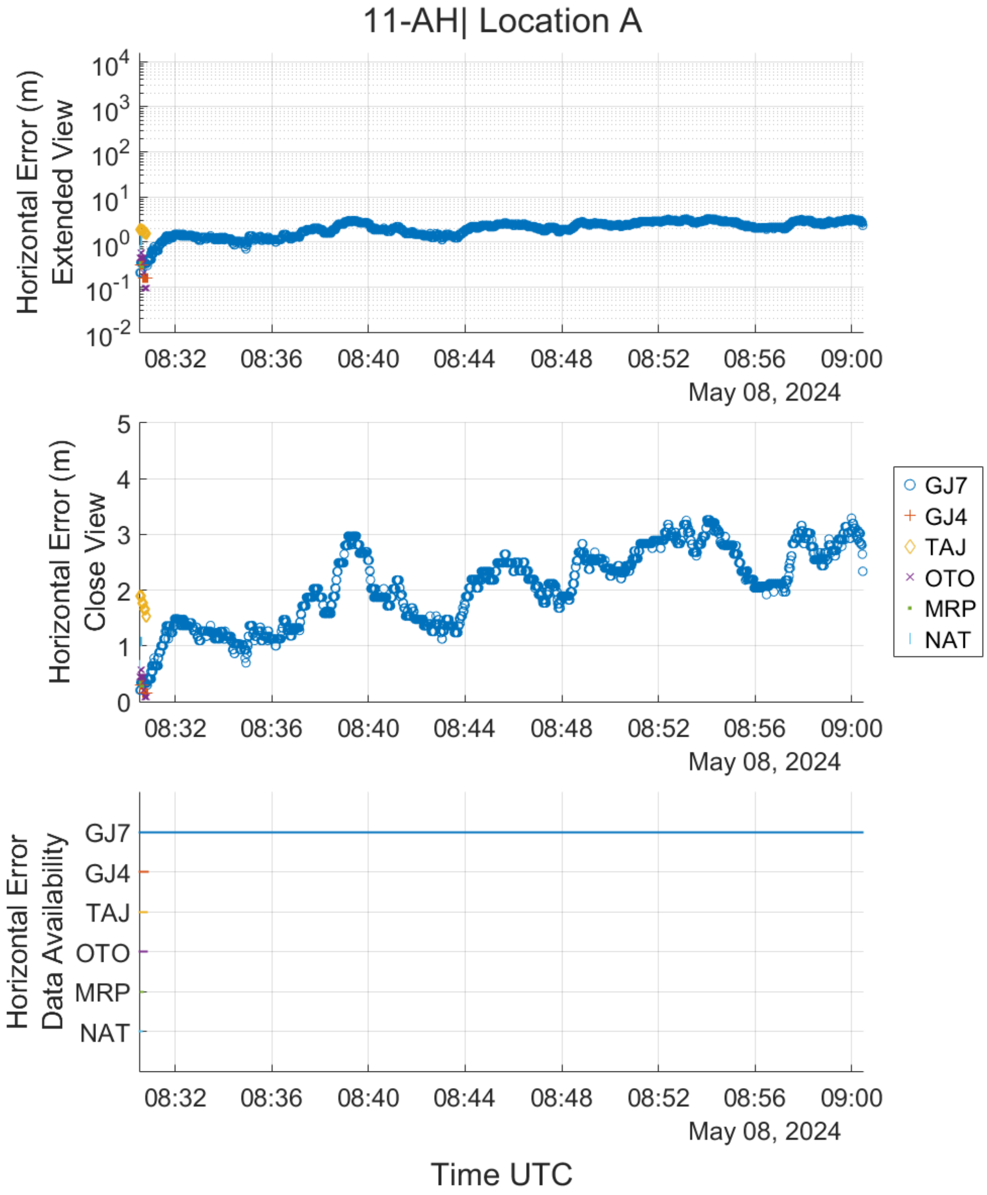


Figure 47. Horizontal position errors during scenario 11-AH

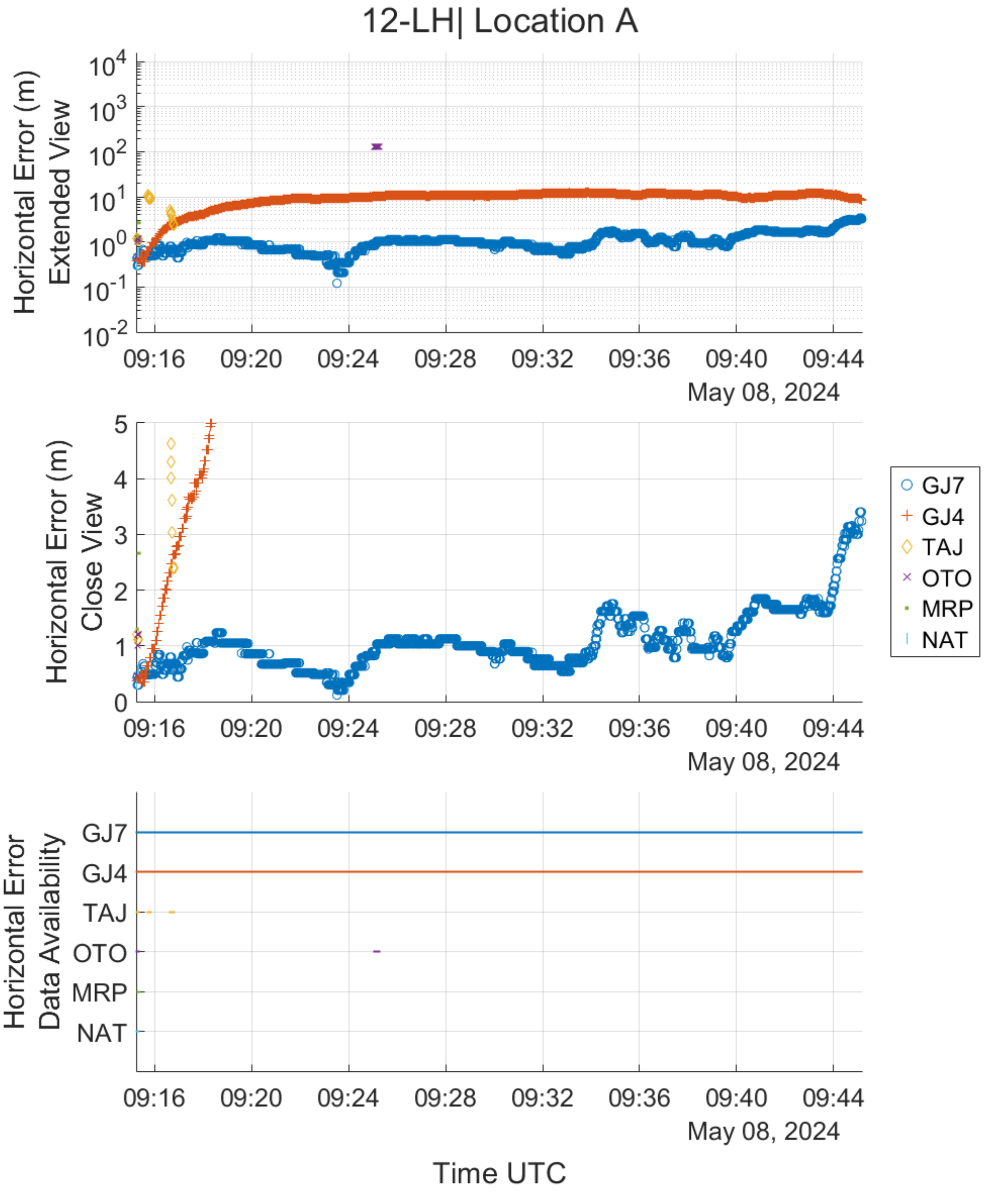


Figure 48. Horizontal position errors during scenario 12-LH

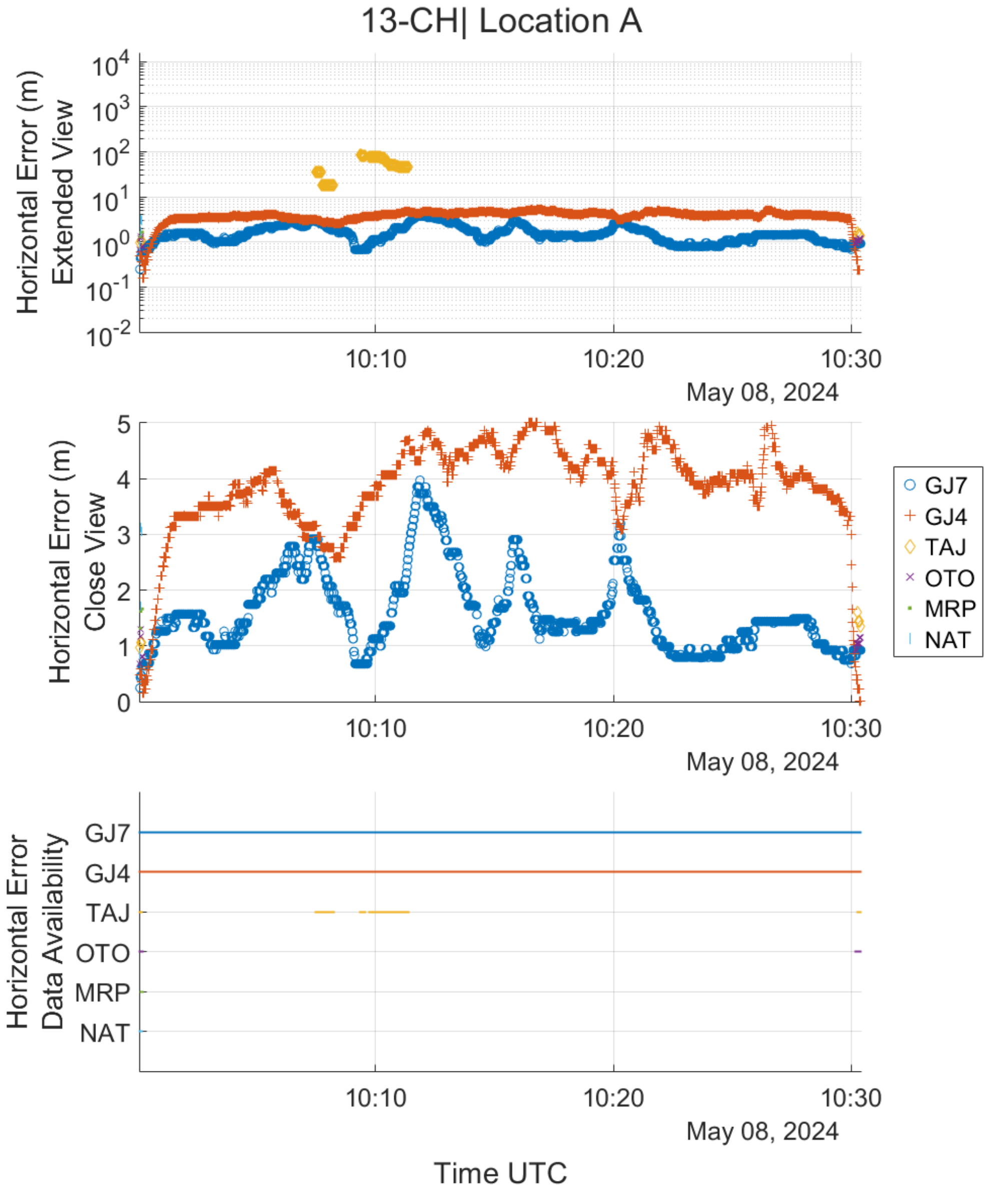


Figure 49. Horizontal position errors during scenario 13-CH

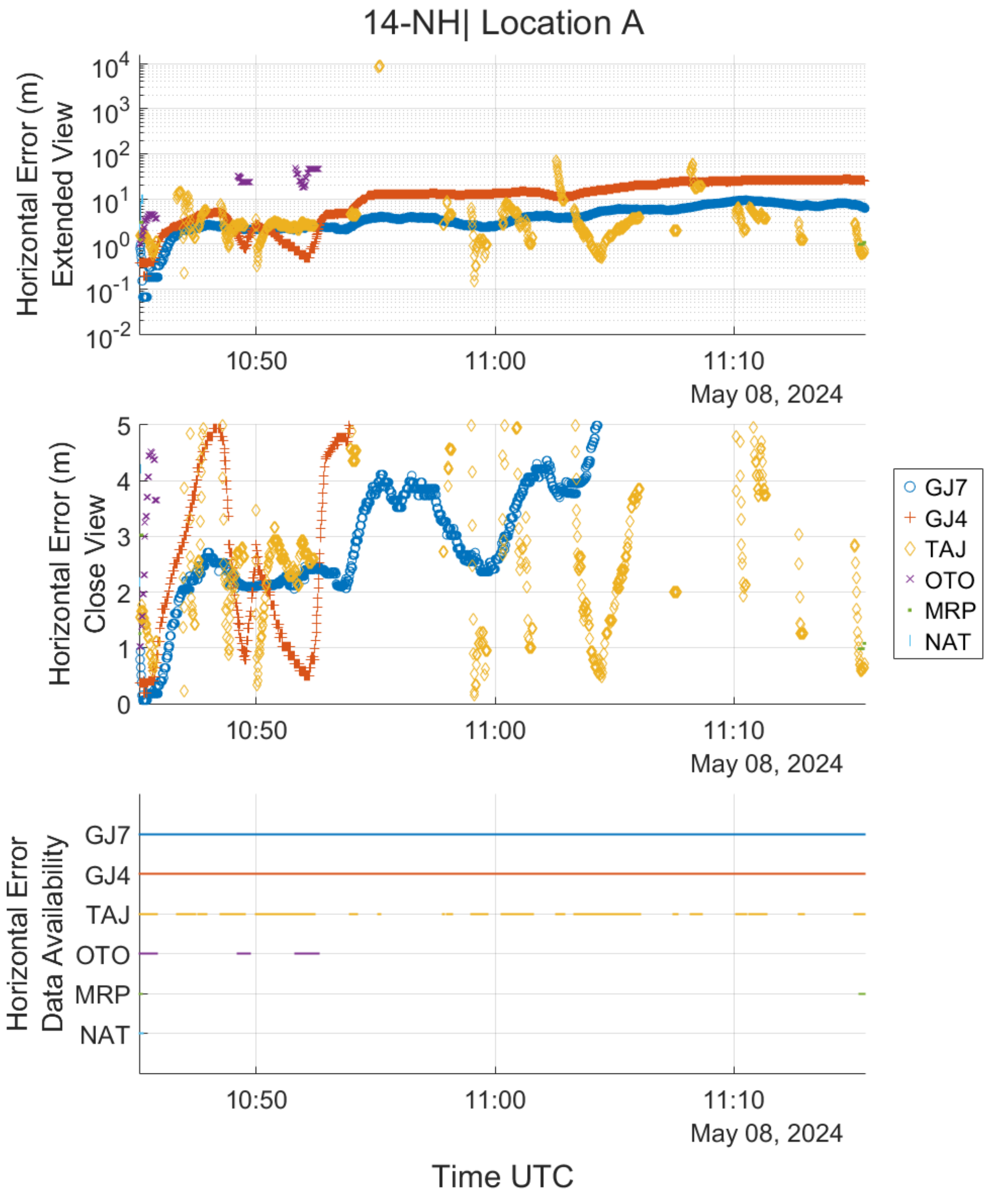


Figure 50. Horizontal position errors during scenario 14-NH

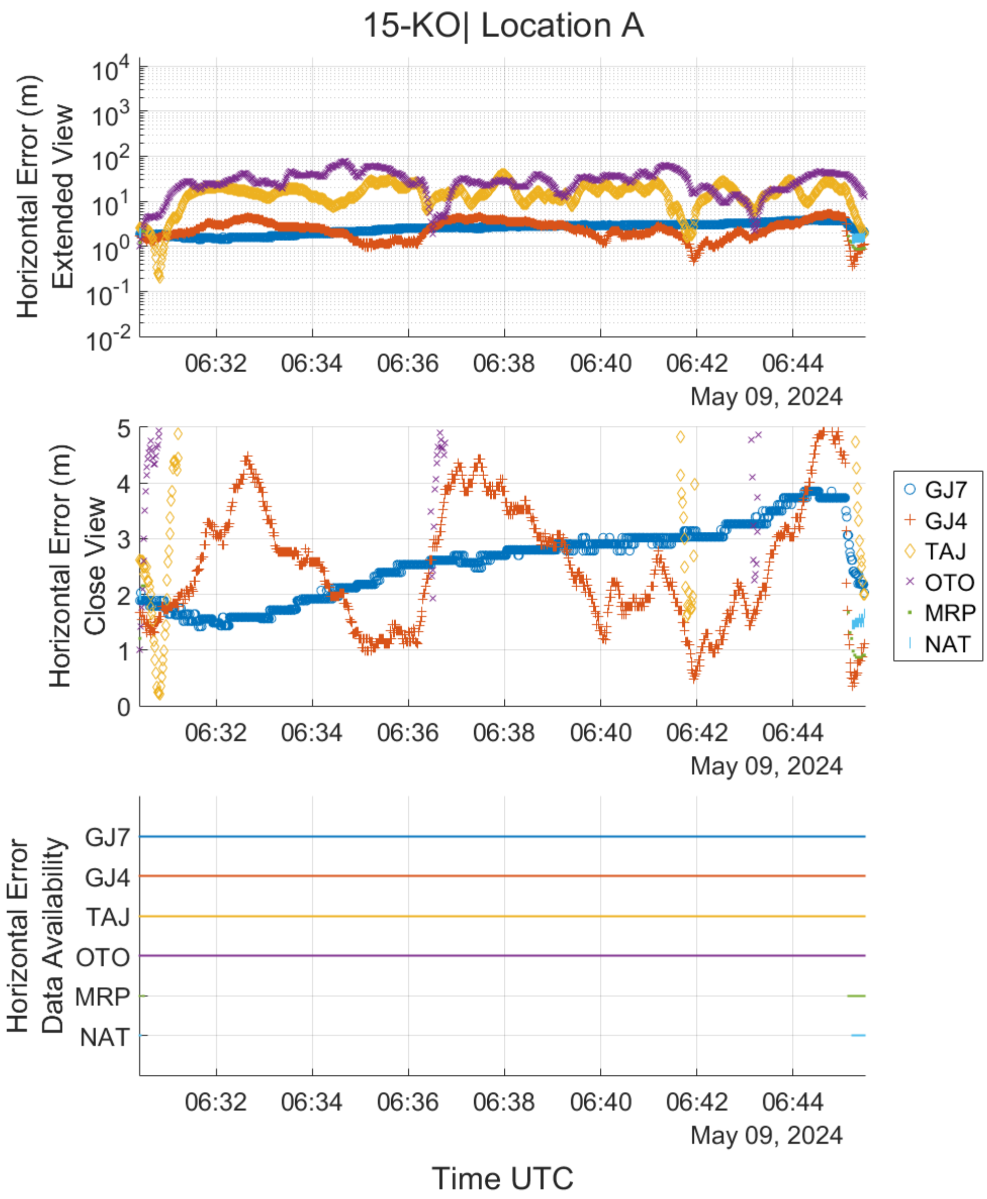


Figure 51. Horizontal position errors during scenario 15-KO

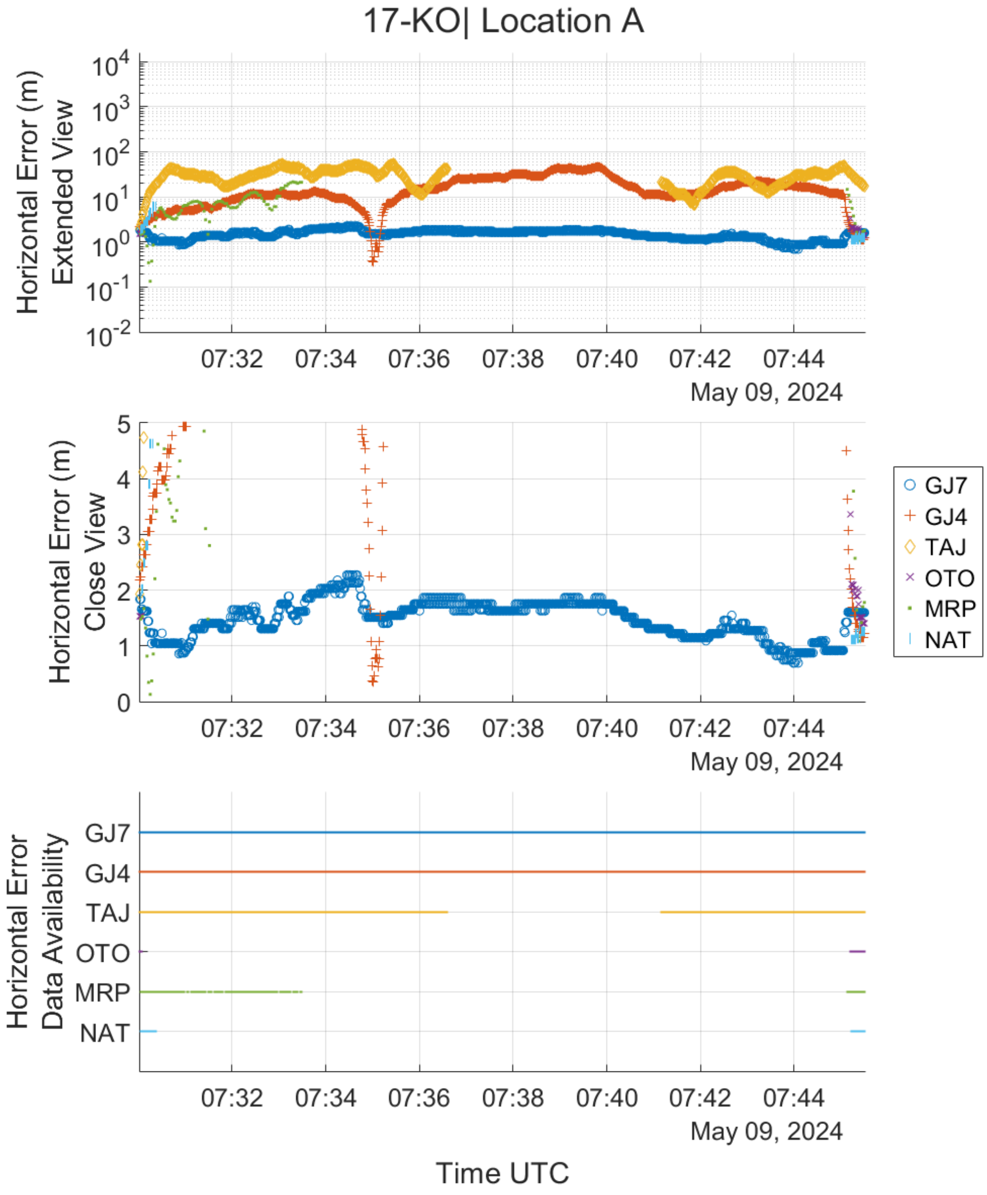


Figure 52. Horizontal position errors during scenario 17-KO

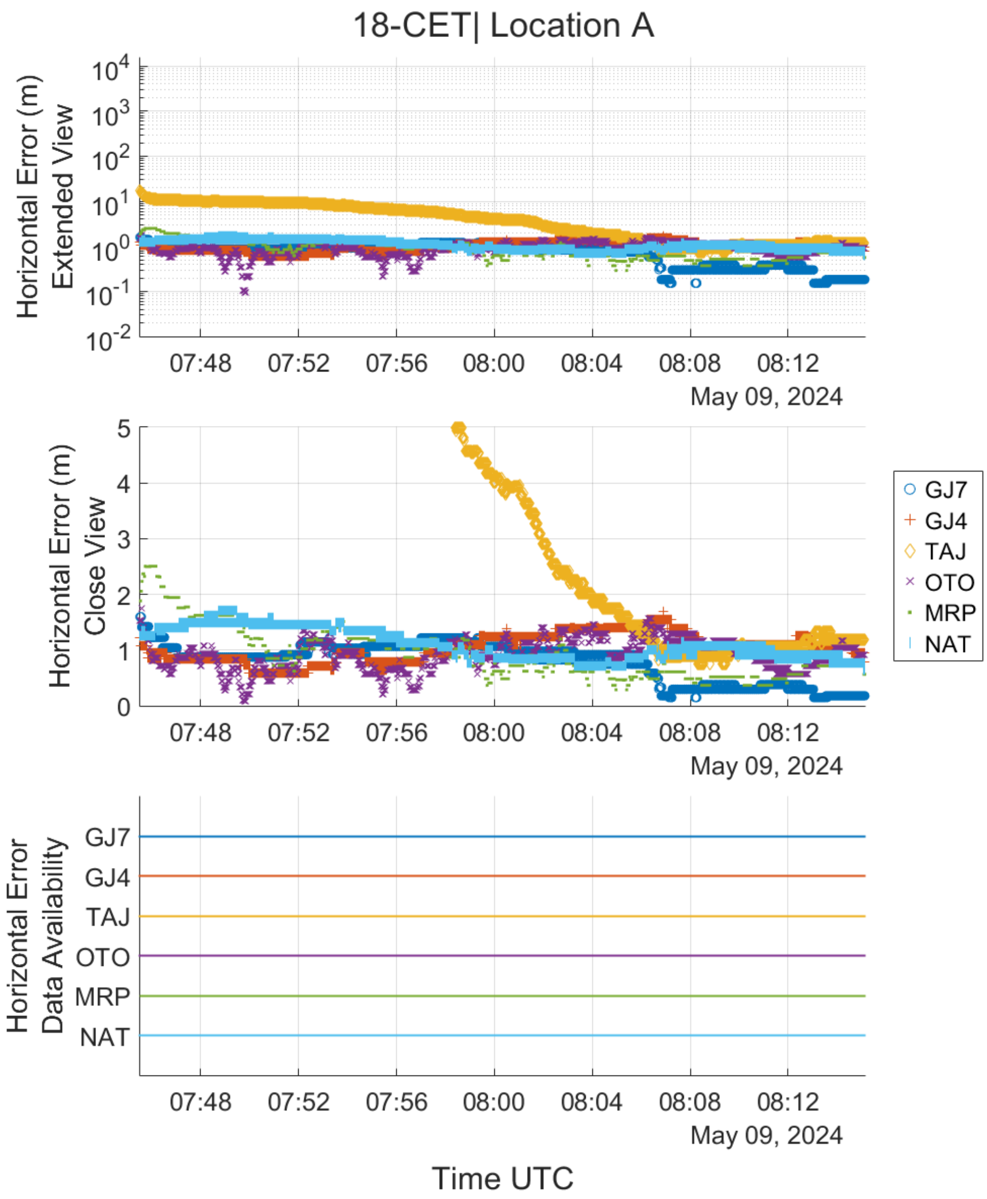


Figure 53. Horizontal position errors during scenario 18-CET

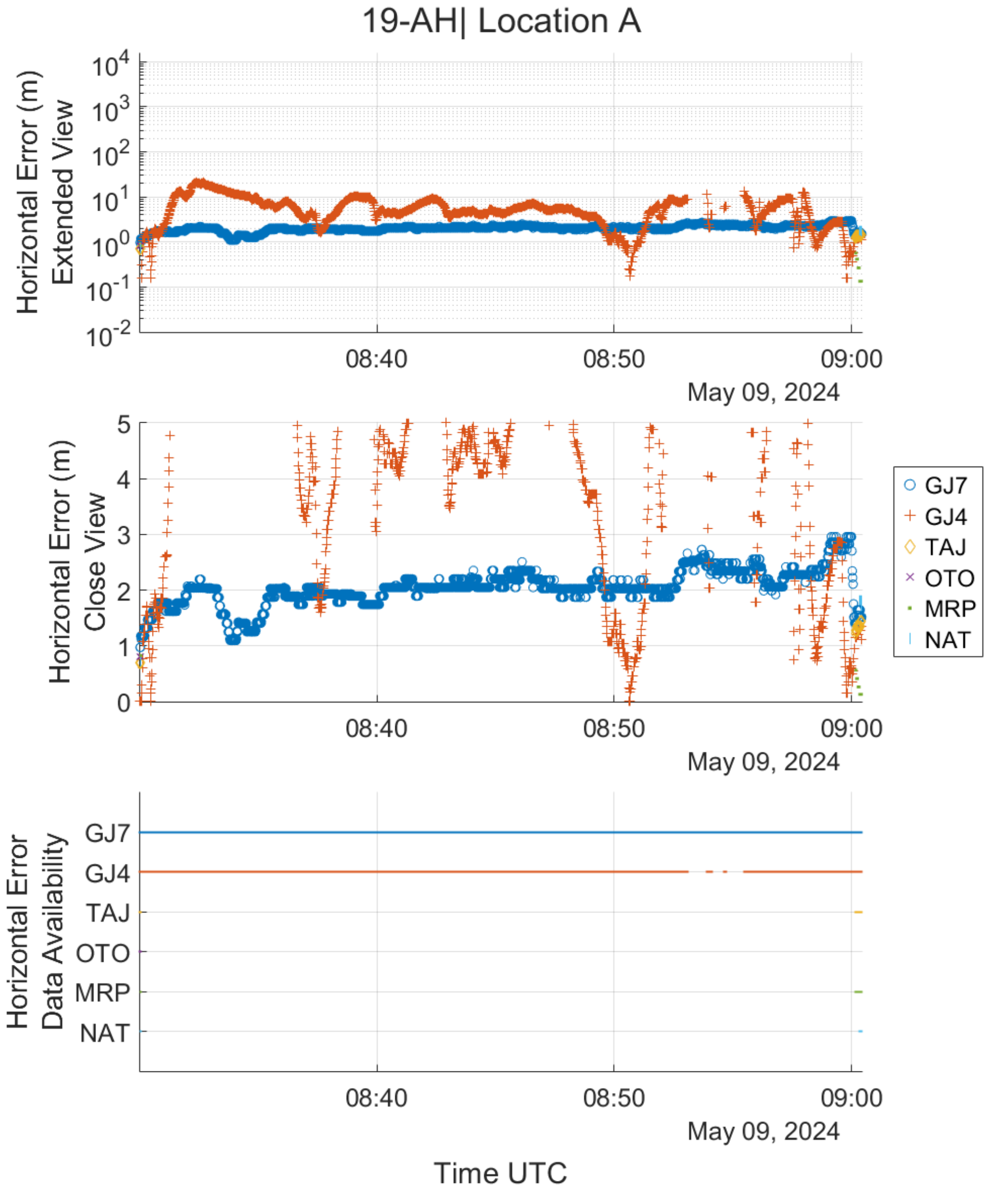


Figure 54. Horizontal position errors during scenario 19-AH

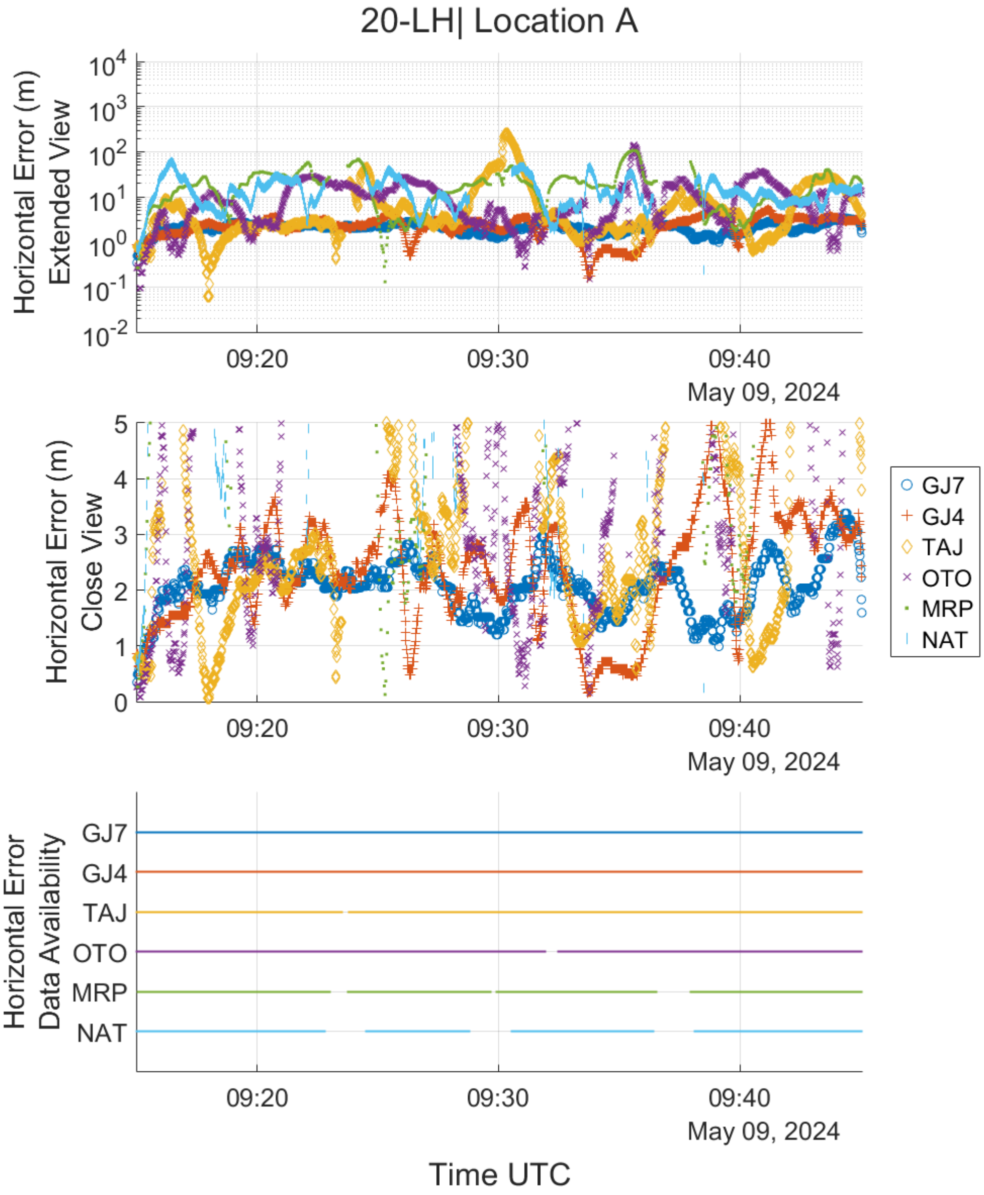


Figure 55. Horizontal position errors during scenario 20-LH

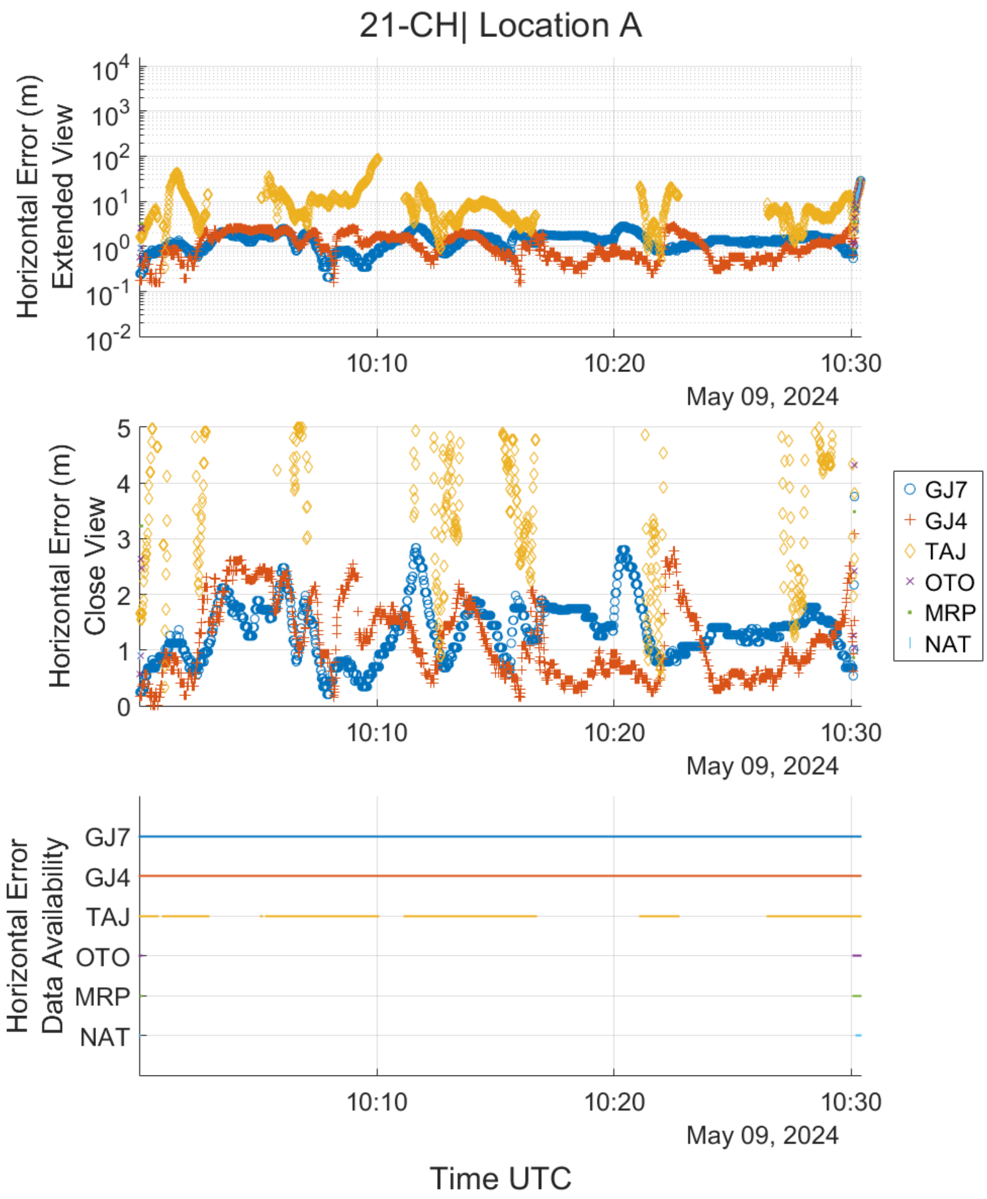


Figure 56. Horizontal position errors during scenario 21-CH

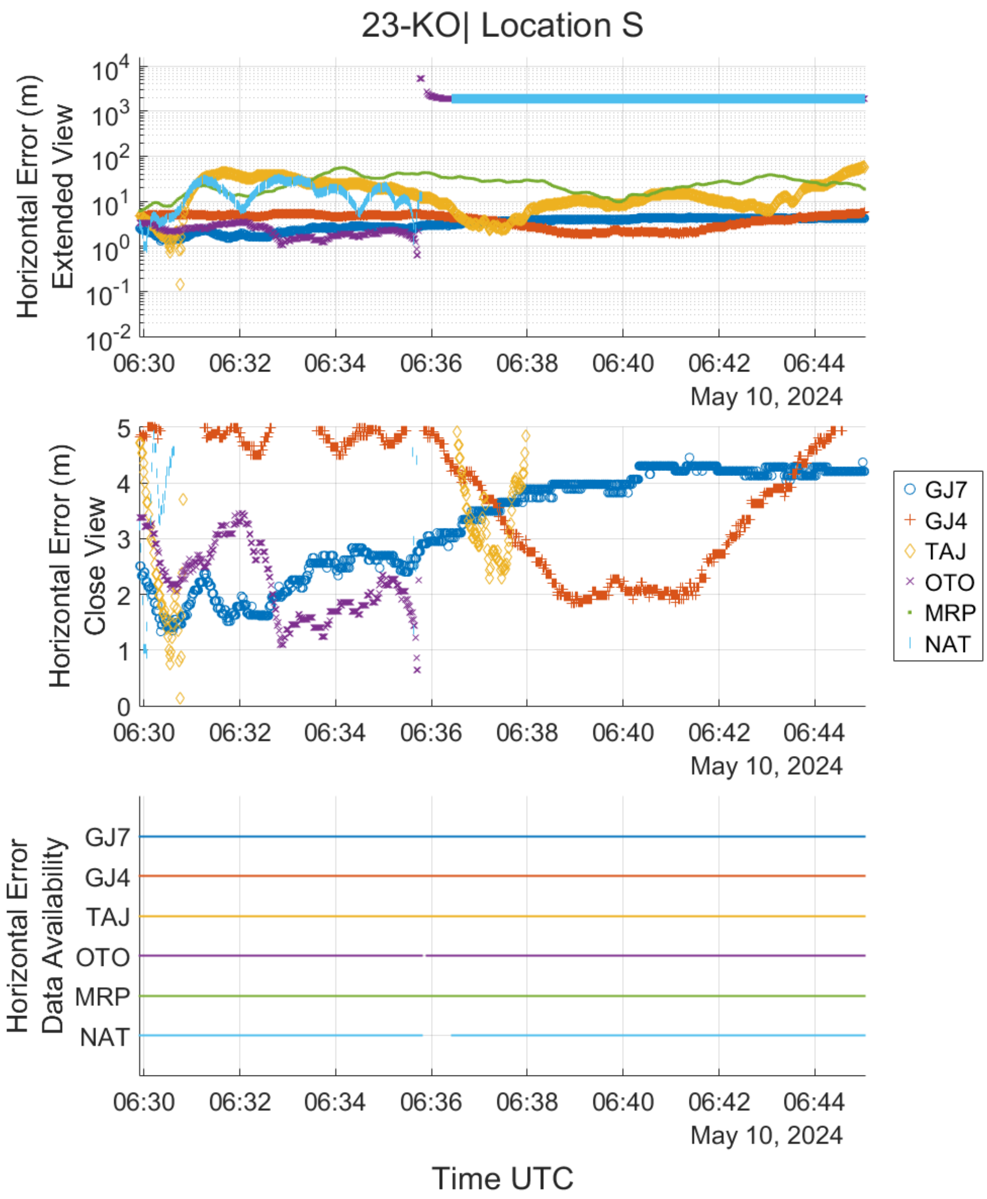


Figure 57. Horizontal position errors during scenario 23-KO

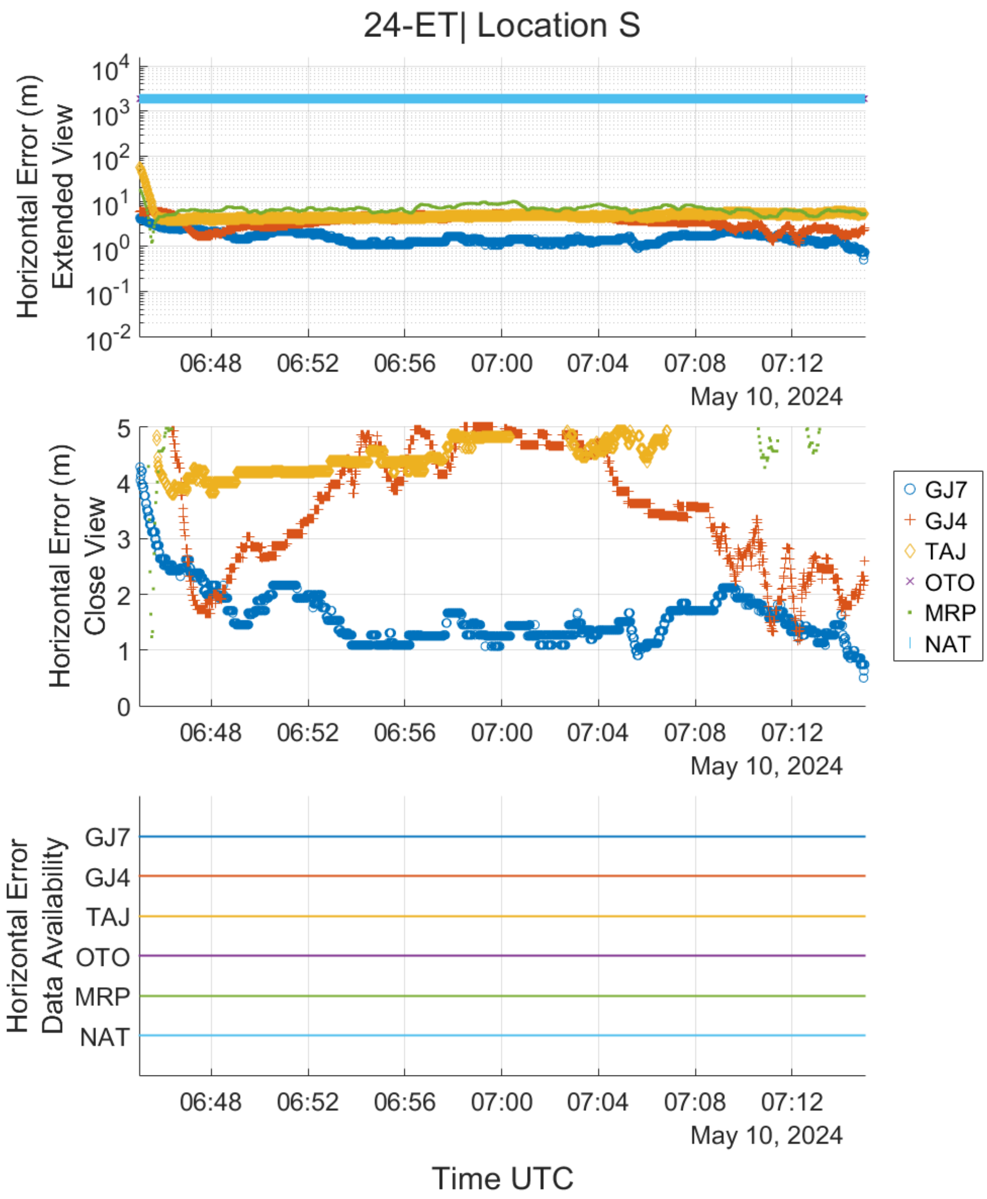


Figure 58. Horizontal position errors during scenario 24-ET

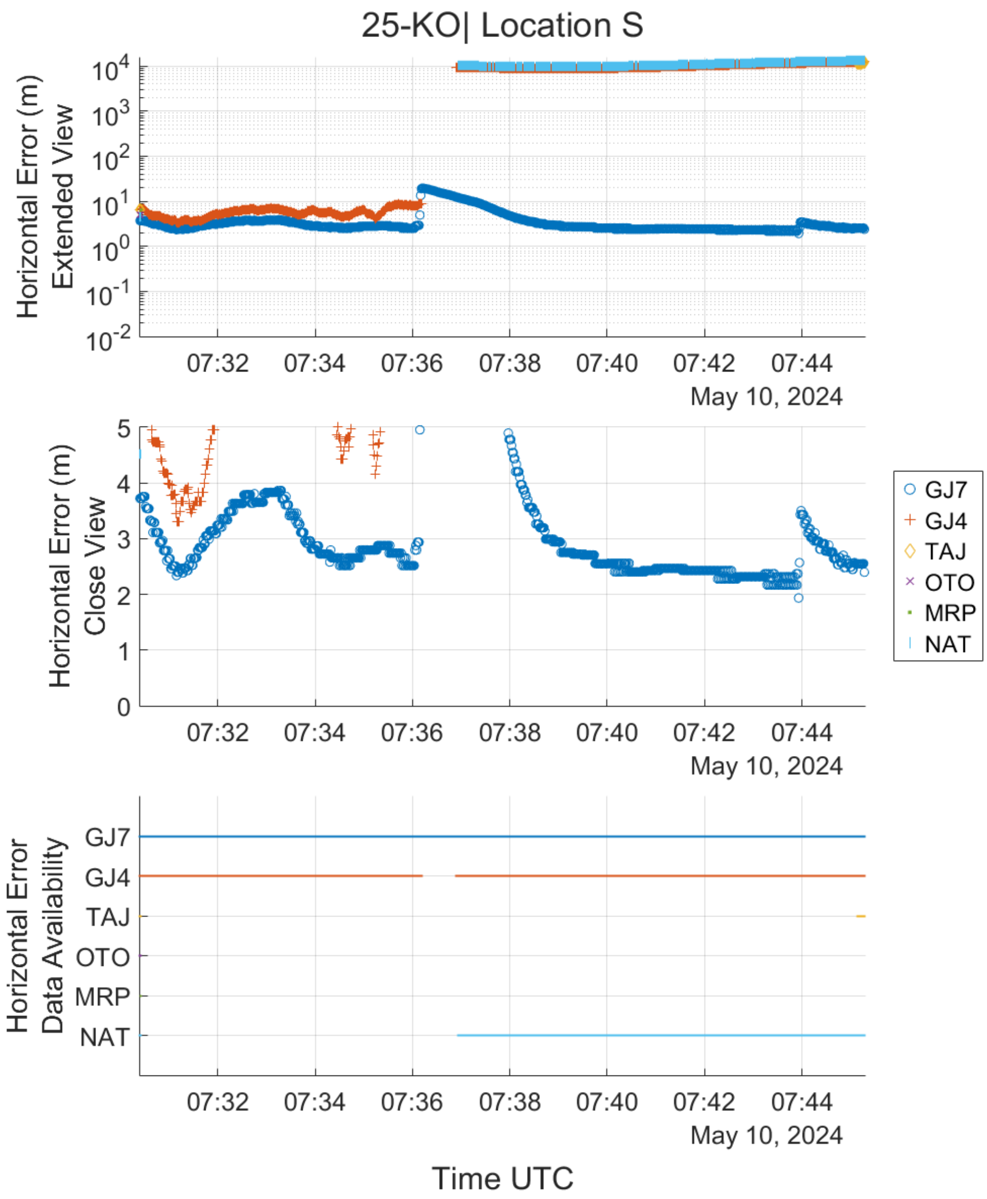


Figure 59. Horizontal position errors during scenario 25-KO

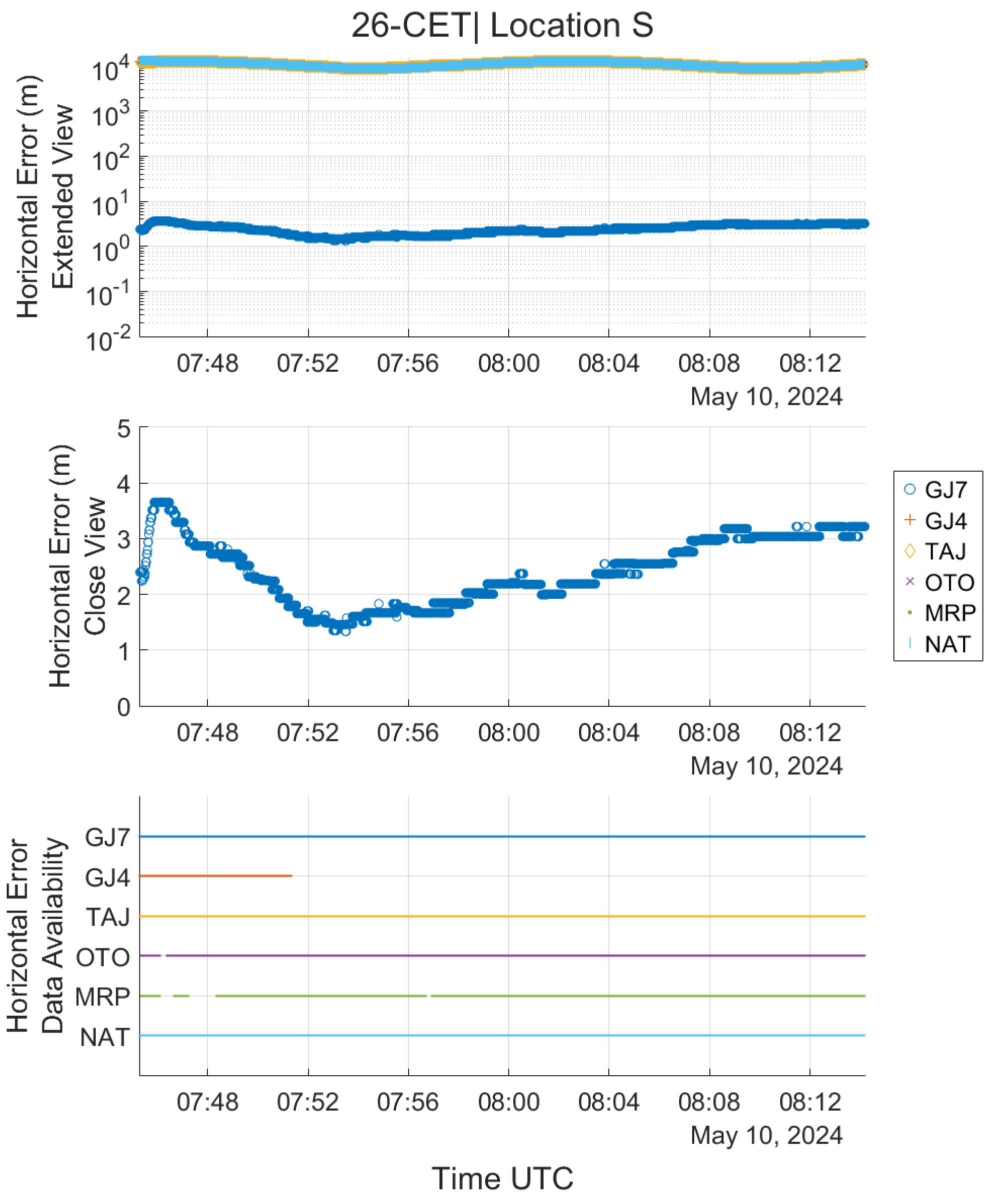


Figure 60. Horizontal position errors during scenario 26-CET

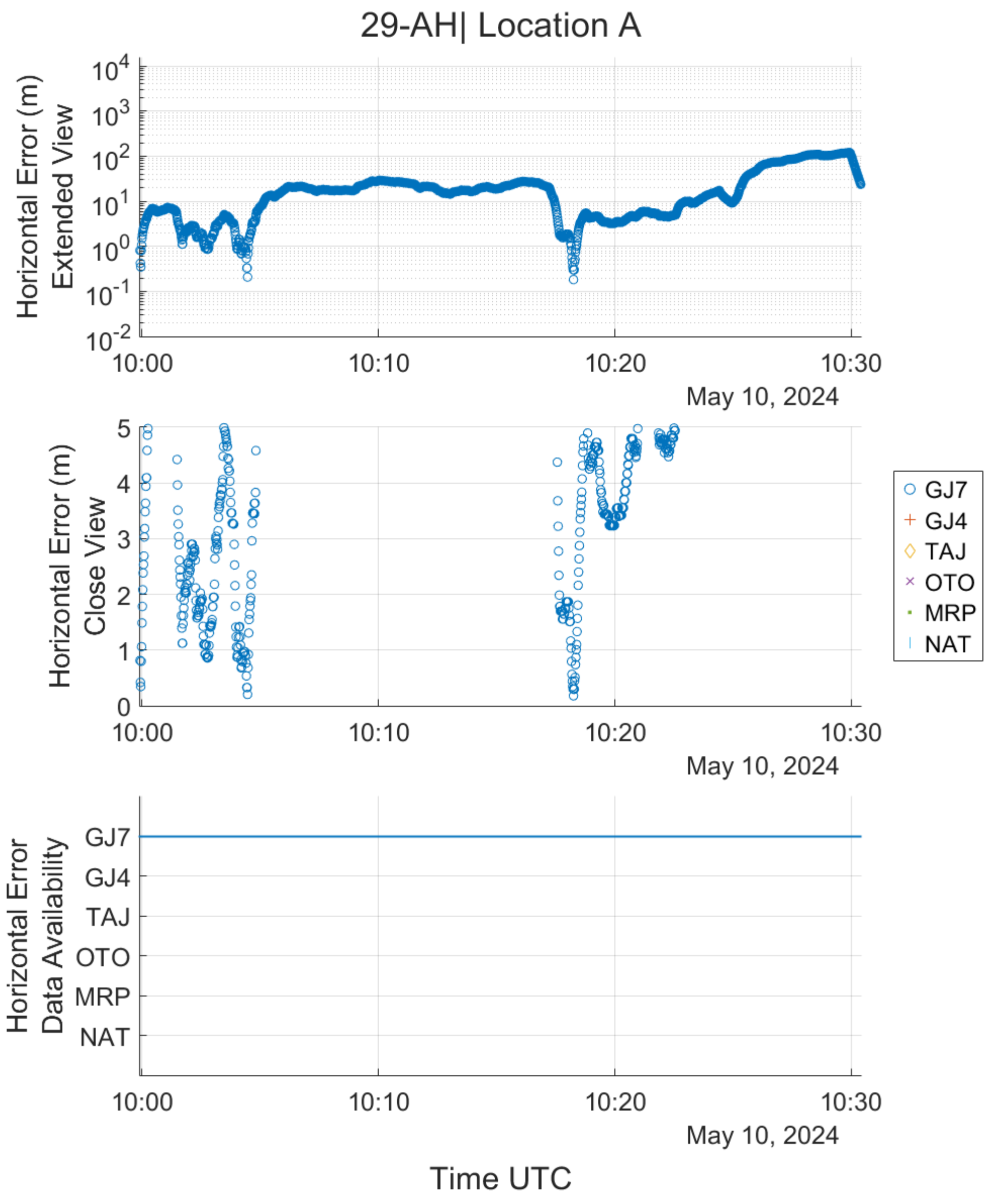


Figure 61. Horizontal position errors during scenario 29-AH

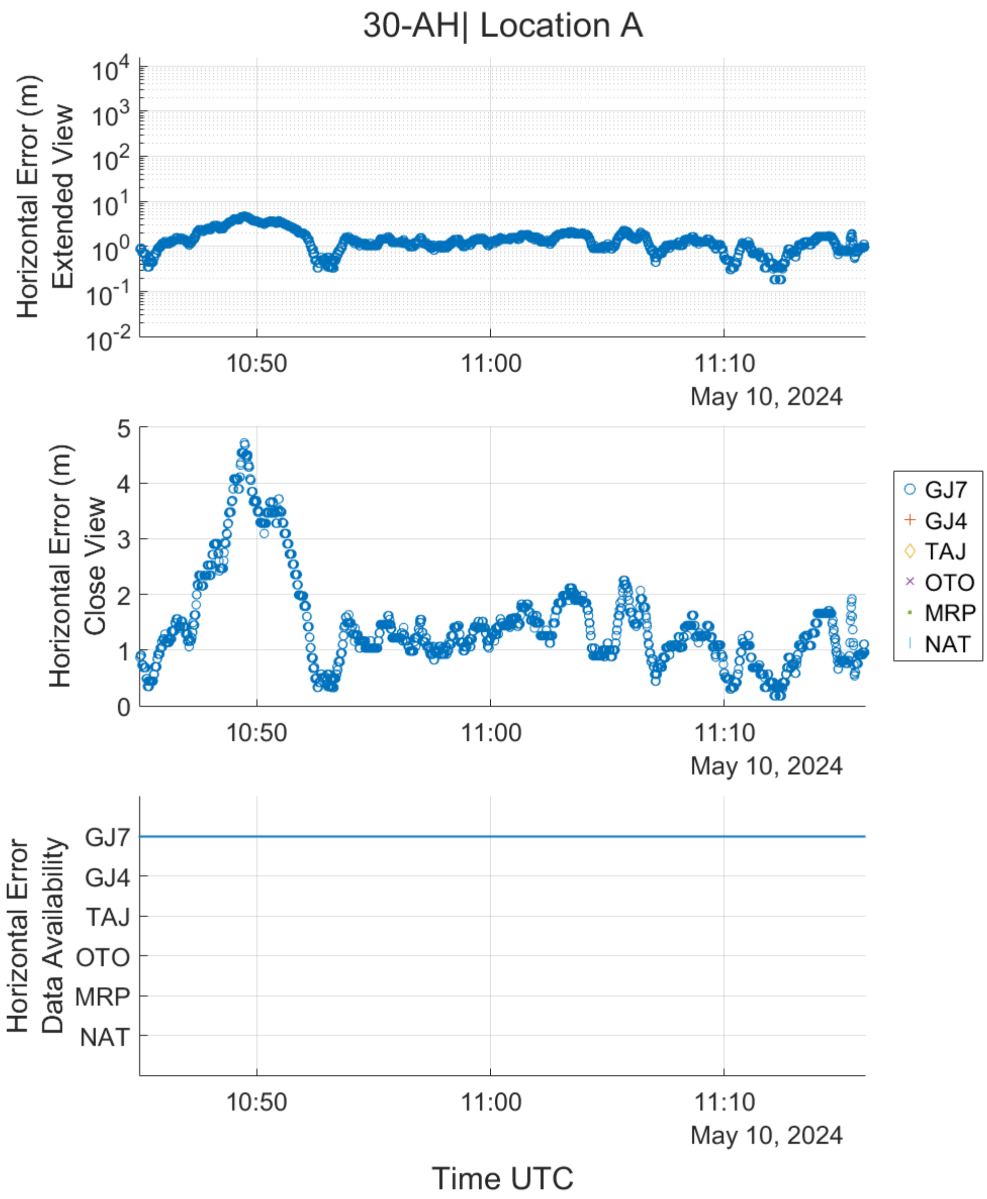


Figure 62. Horizontal position errors during scenario 30-AH

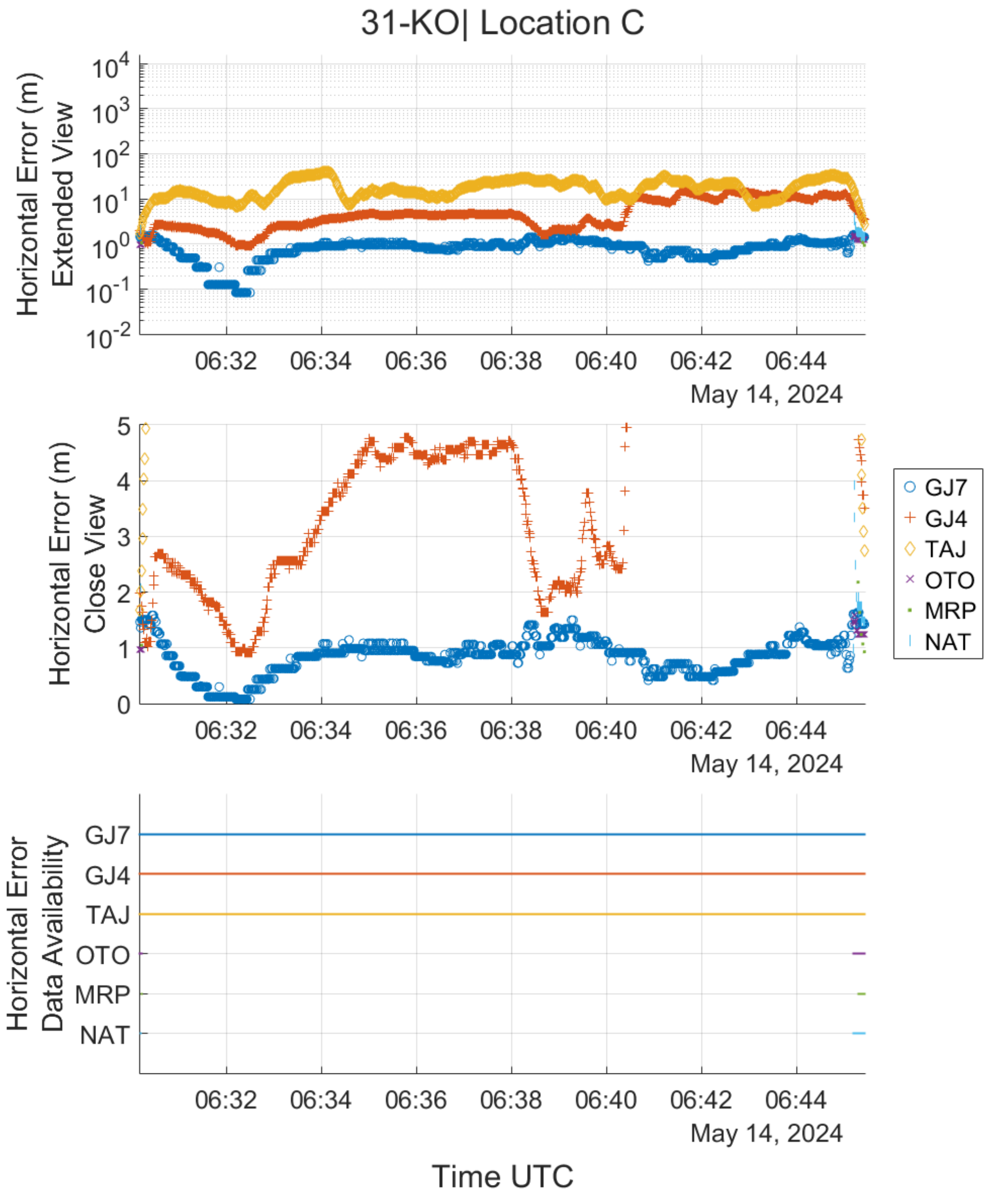


Figure 63. Horizontal position errors during scenario 31-KO

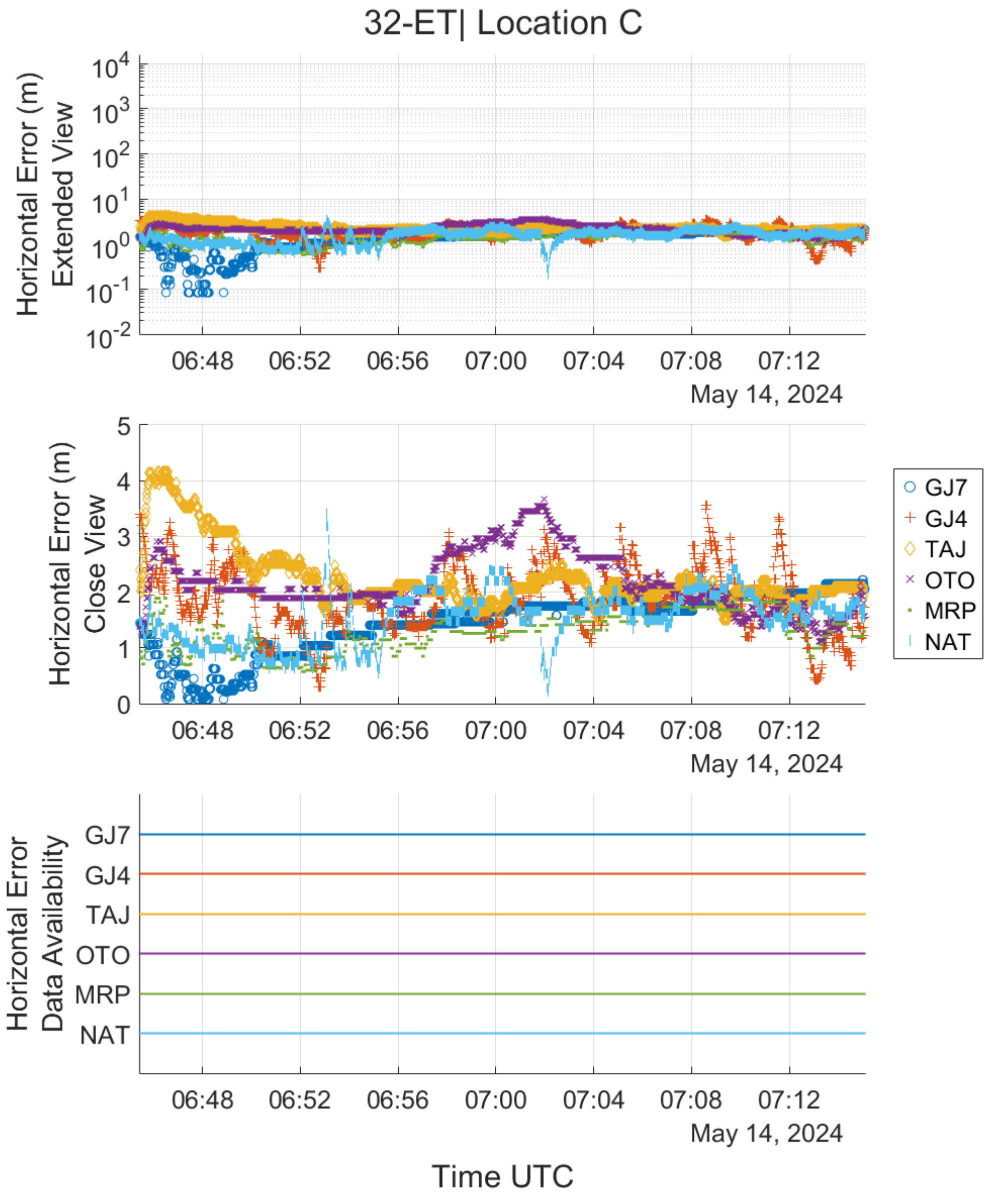


Figure 64. Horizontal position errors during scenario 32-ET

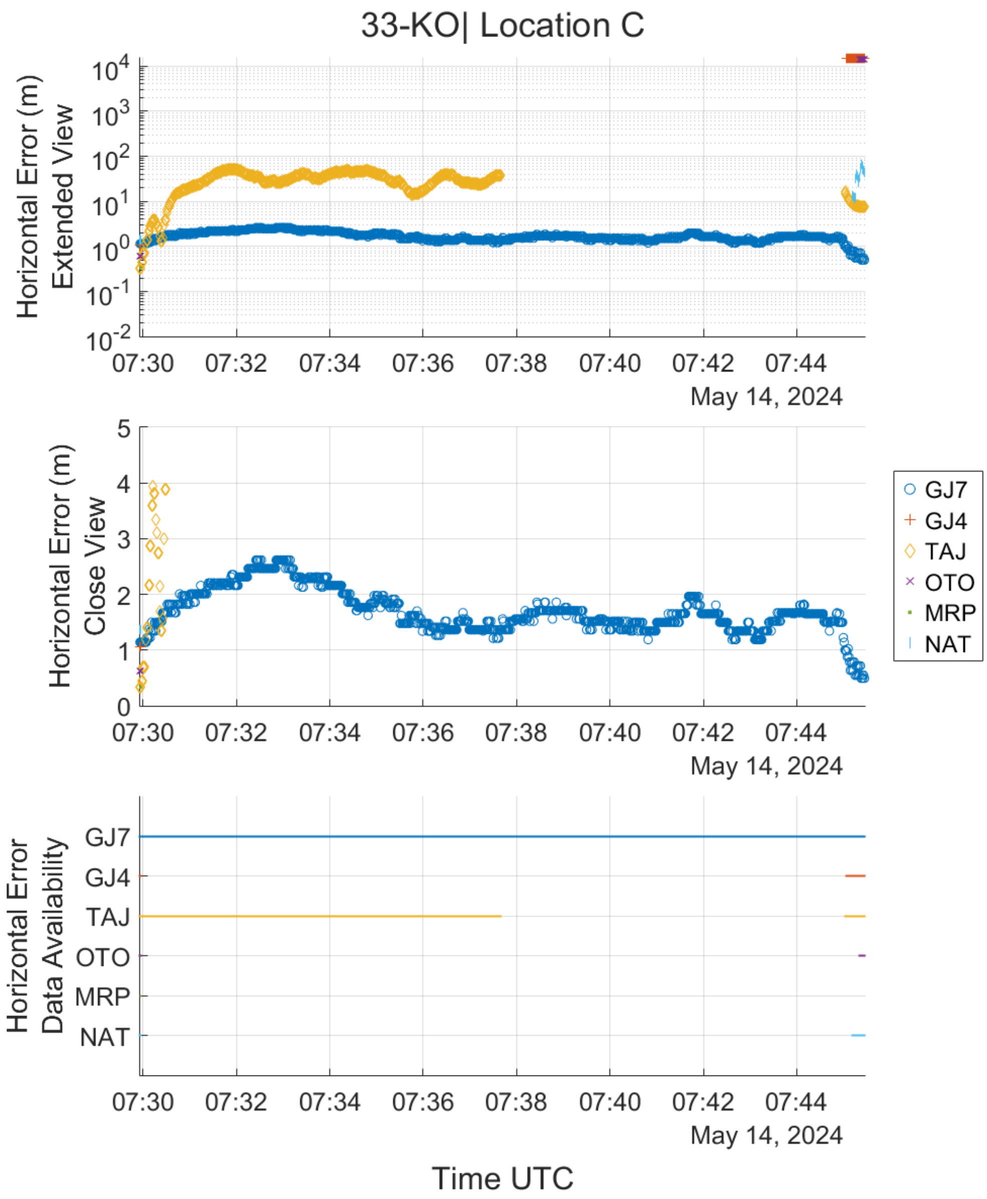


Figure 65. Horizontal position errors during scenario 33-KO

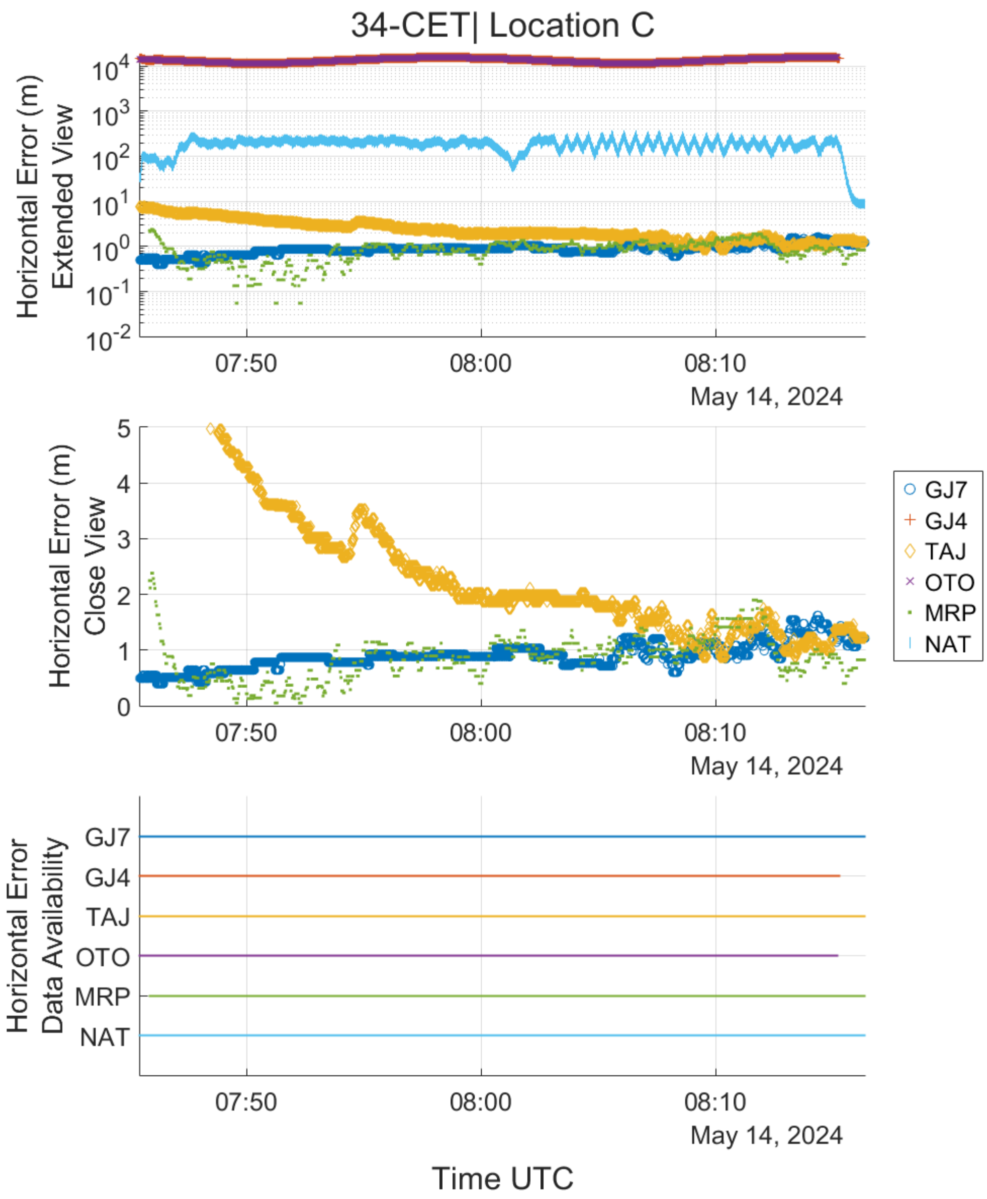


Figure 66. Horizontal position errors during scenario 34-CET

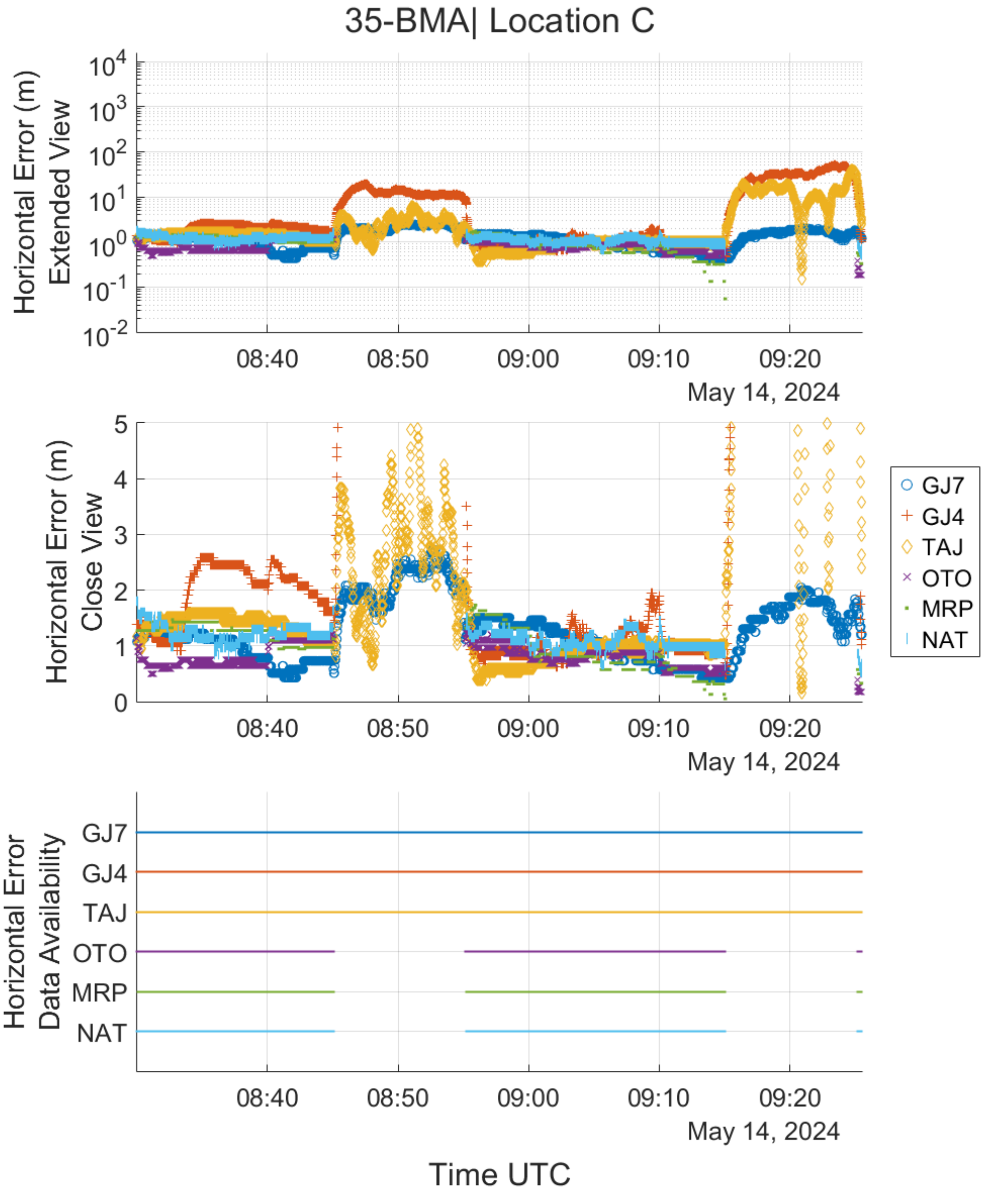


Figure 67. Horizontal position errors during scenario 35-BMA

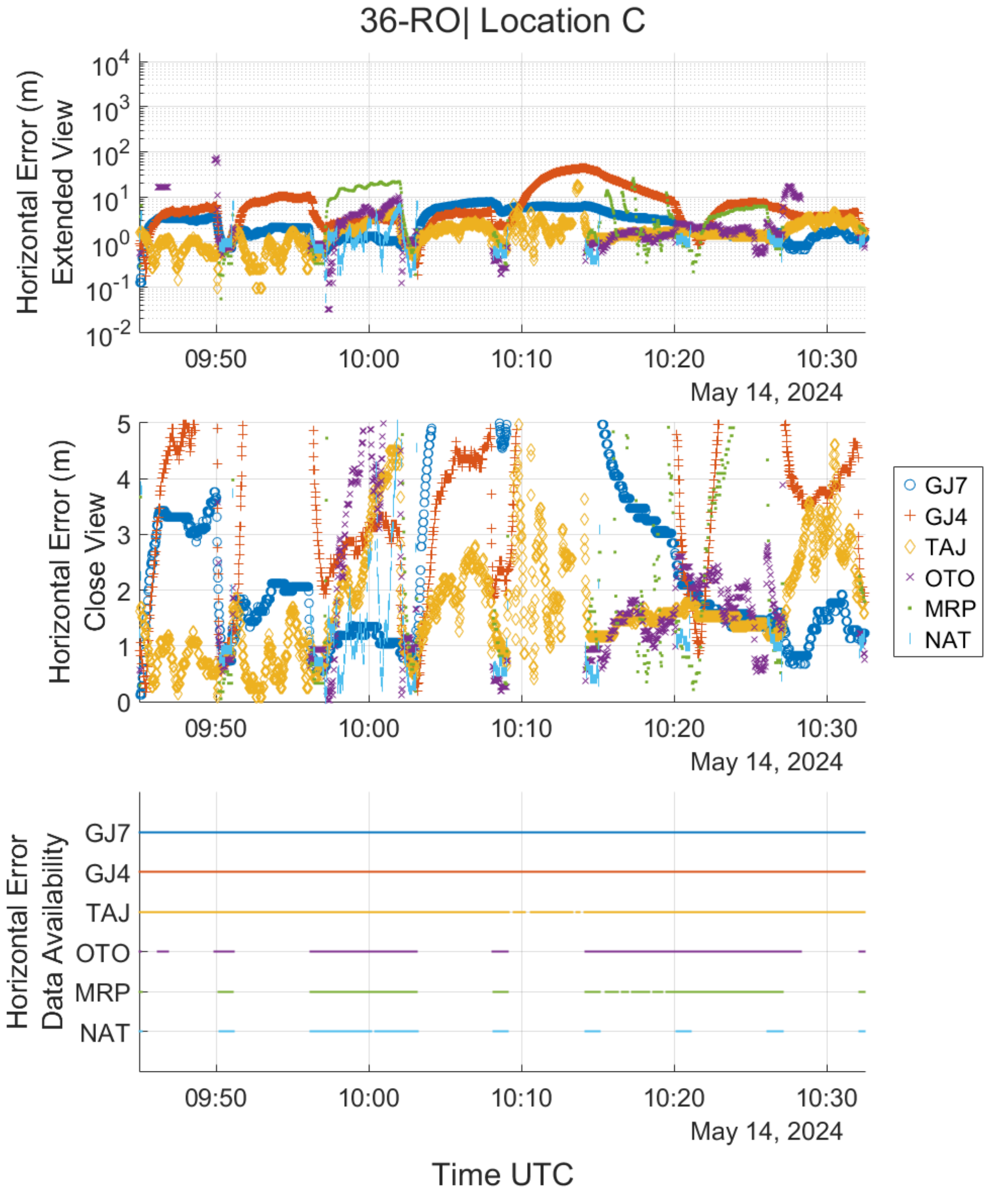


Figure 68. Horizontal position errors during scenario 36-RO

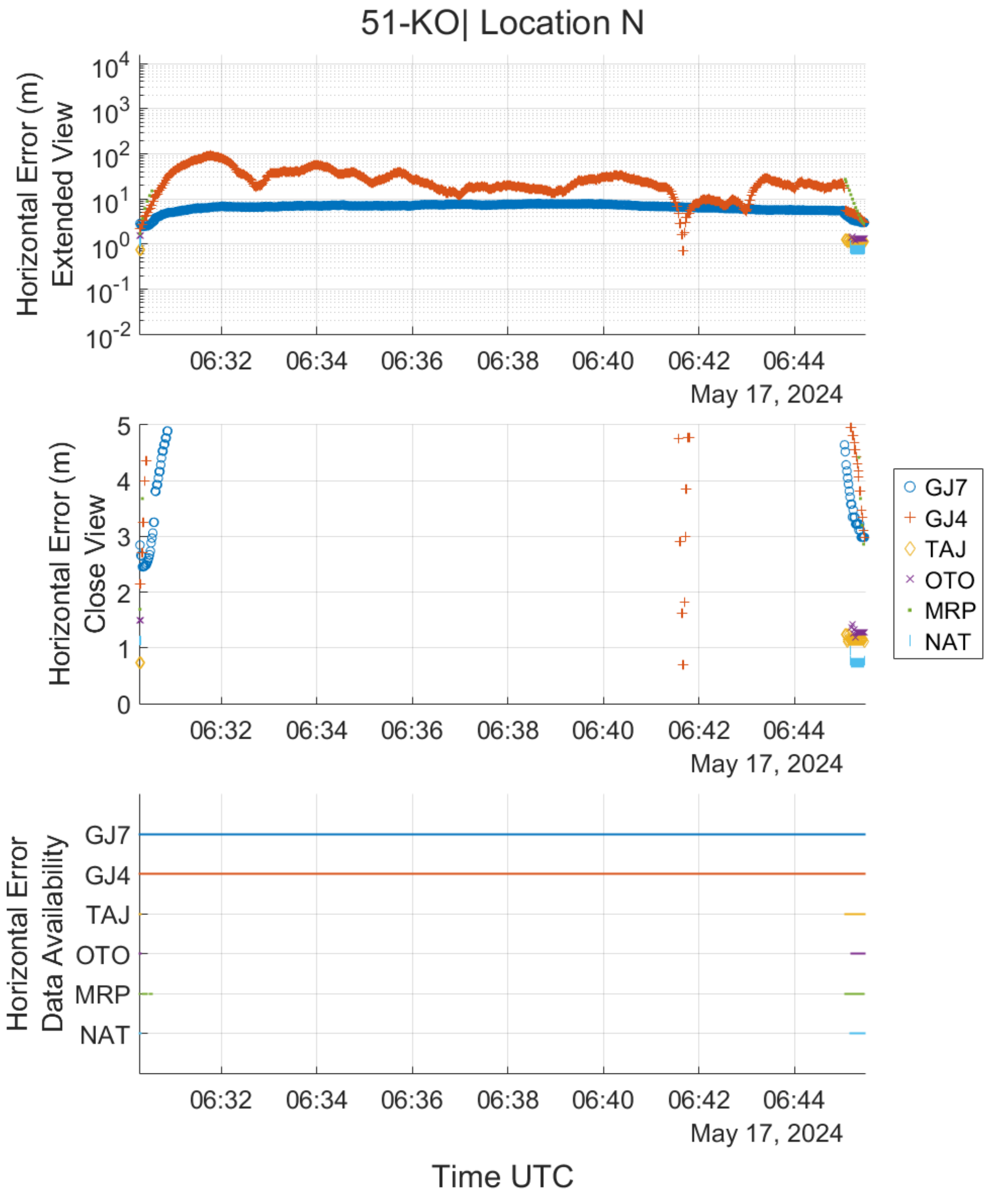


Figure 69. Horizontal position errors during scenario 51-KO

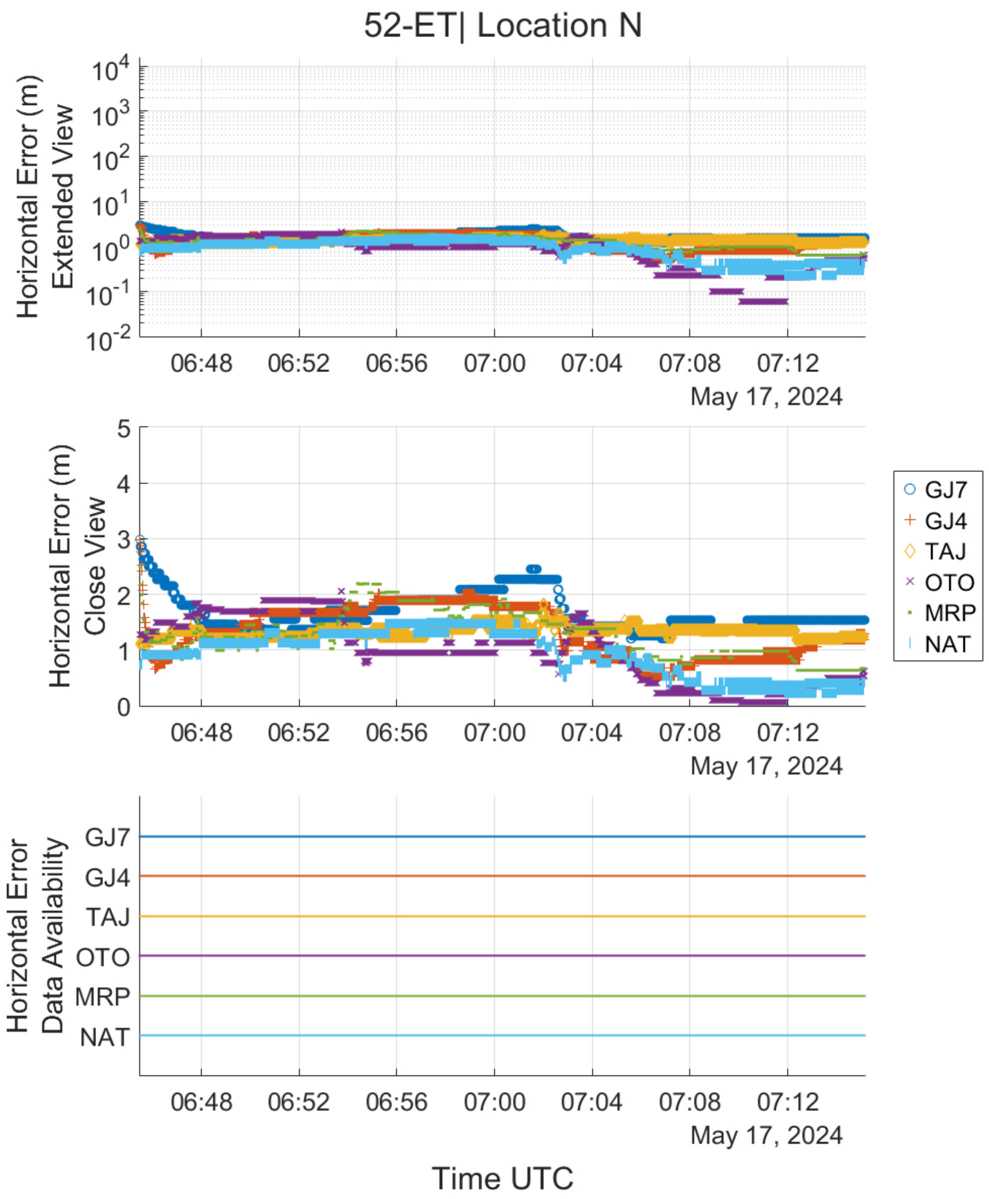


Figure 70. Horizontal position errors during scenario 52-ET

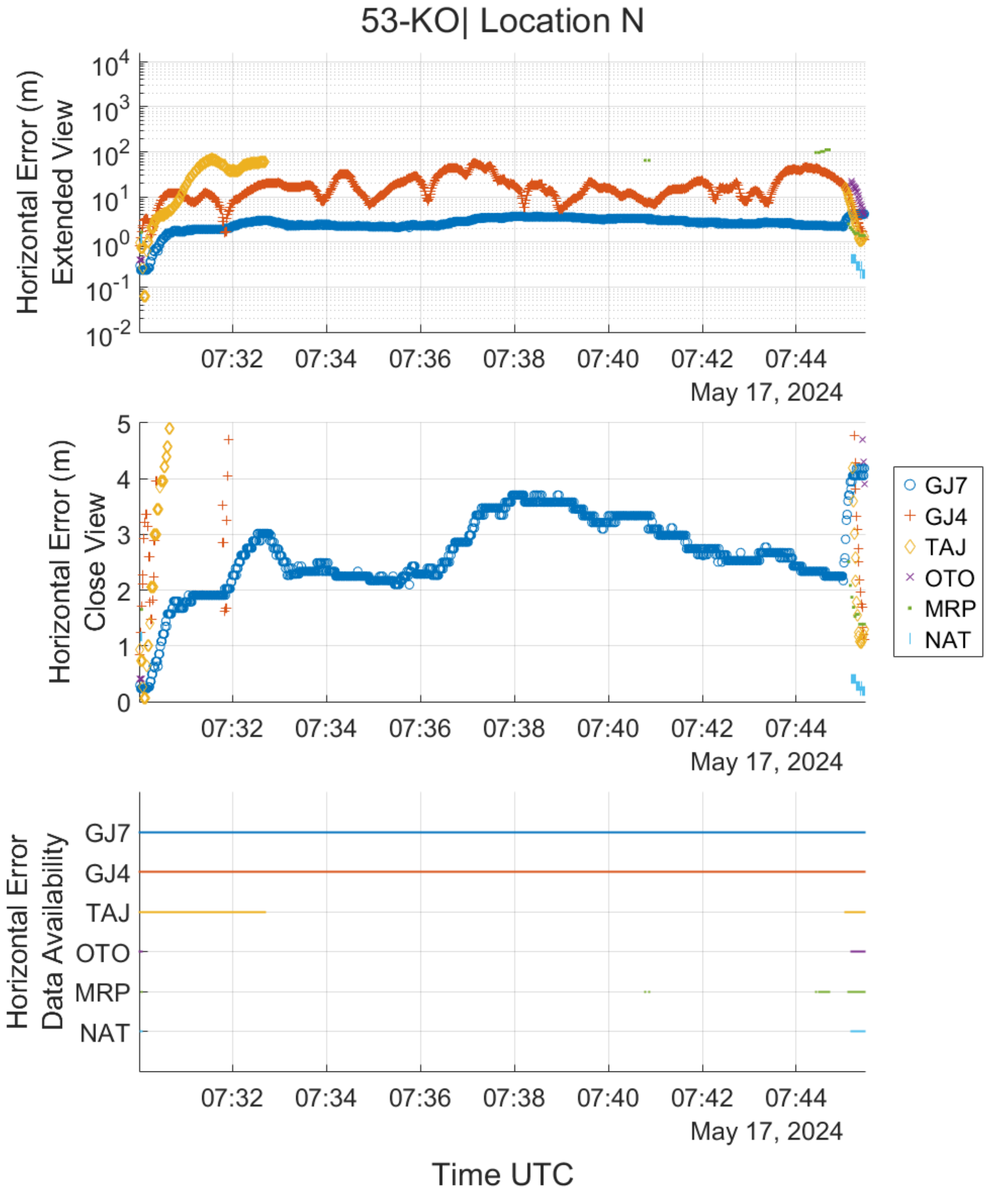


Figure 71. Horizontal position errors during scenario 53-KO

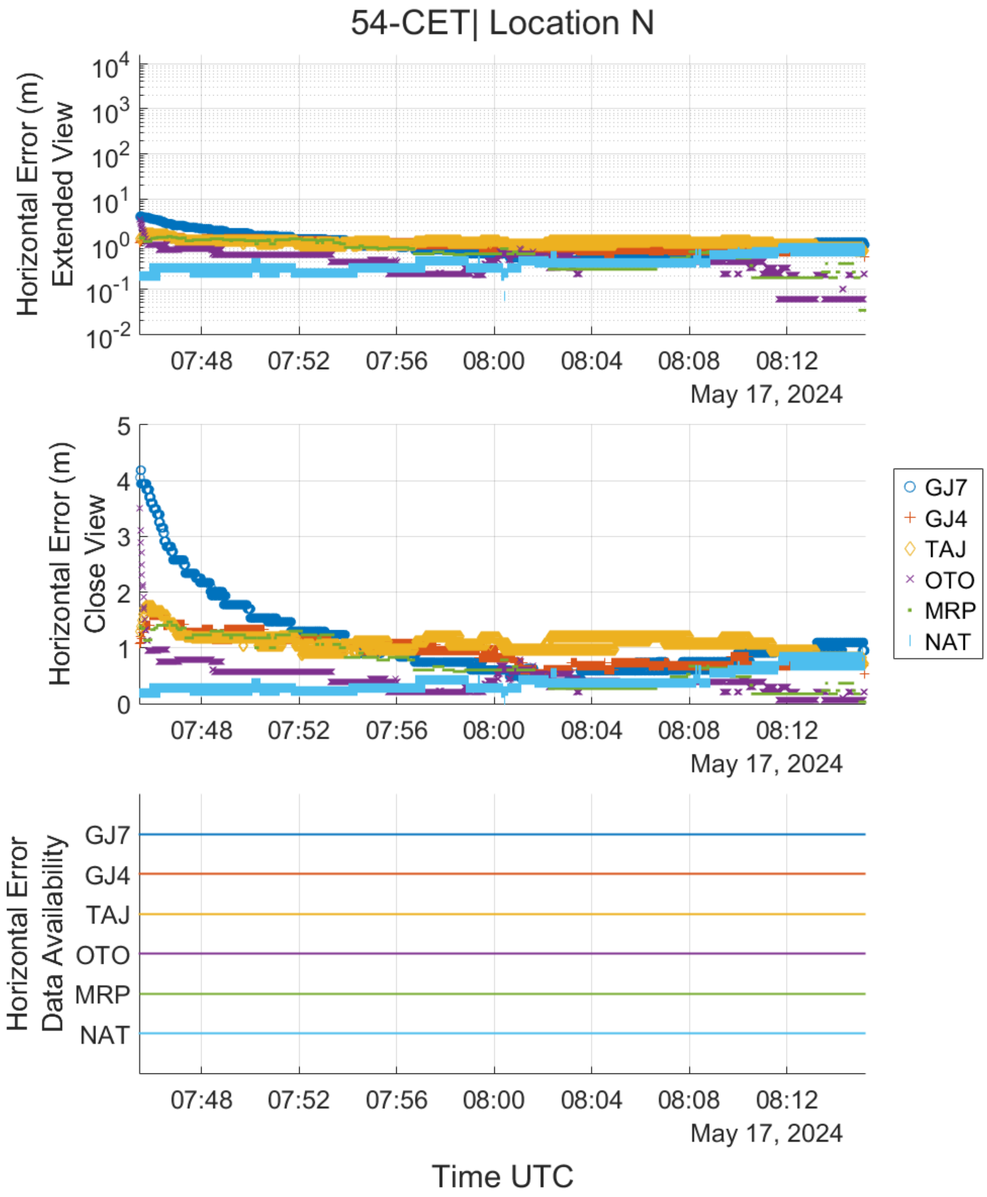


Figure 72. Horizontal position errors during scenario 54-CET

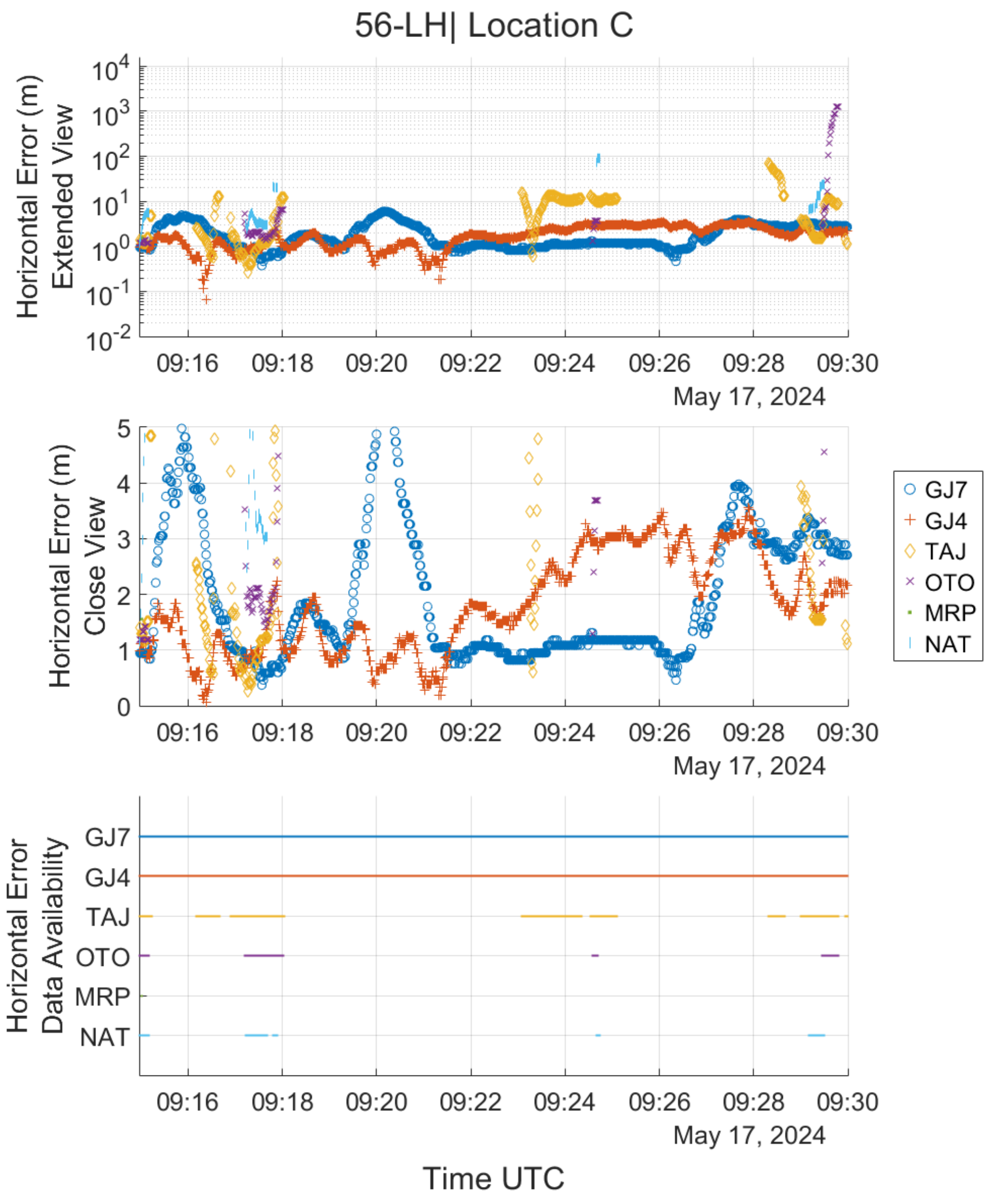


Figure 73. Horizontal position errors during scenario 56-LH

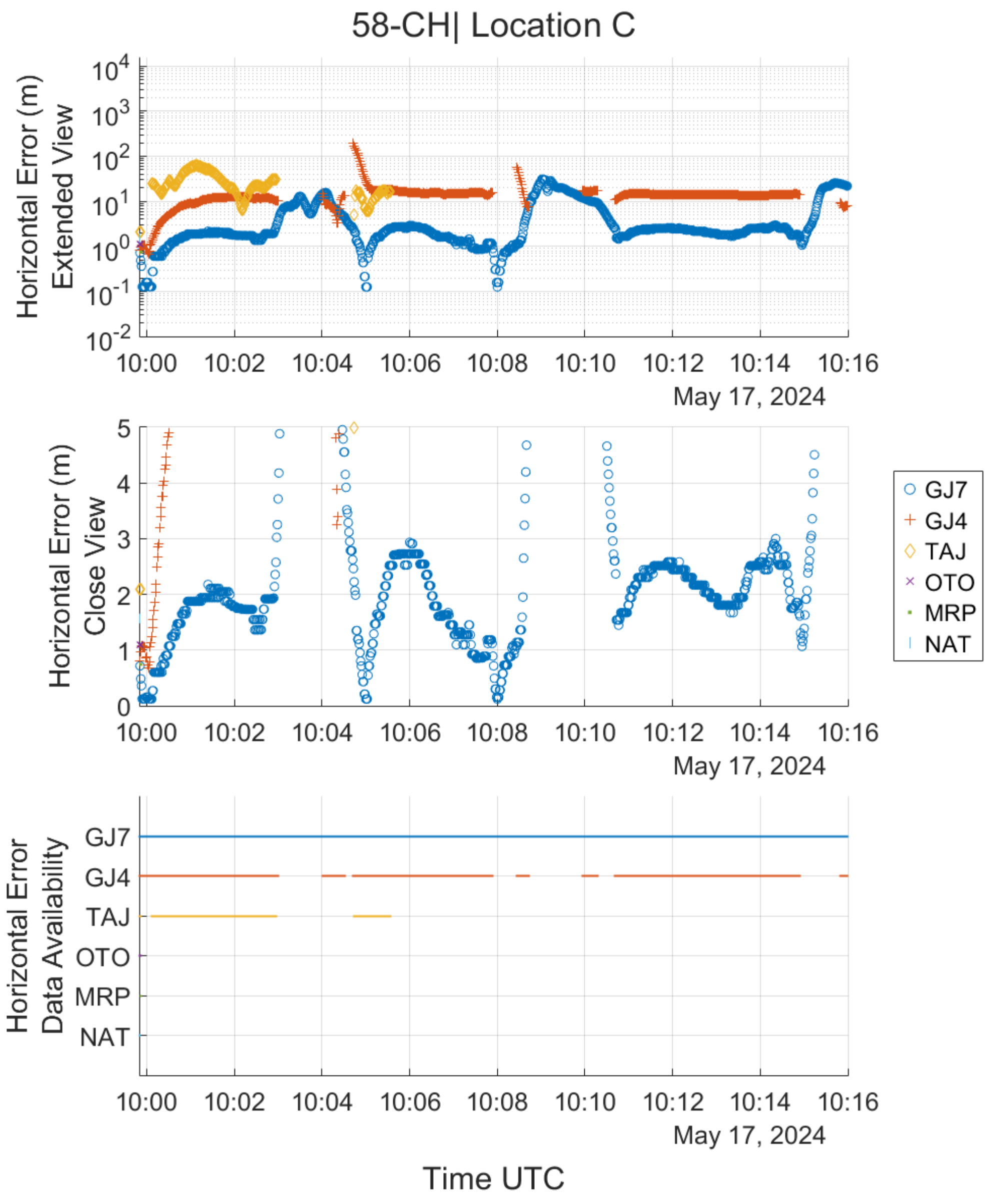


Figure 74. Horizontal position errors during scenario 58-CH

11.C: NAVFEST Static Recovery Analysis Time Series Plots

This appendix contains the time series plots for the NAVFEST static recovery analysis. Each plot shows the horizontal position errors starting near the end of a scenario and extending through the recovery window. All plots are included, regardless of whether the device recovered within the recovery window.

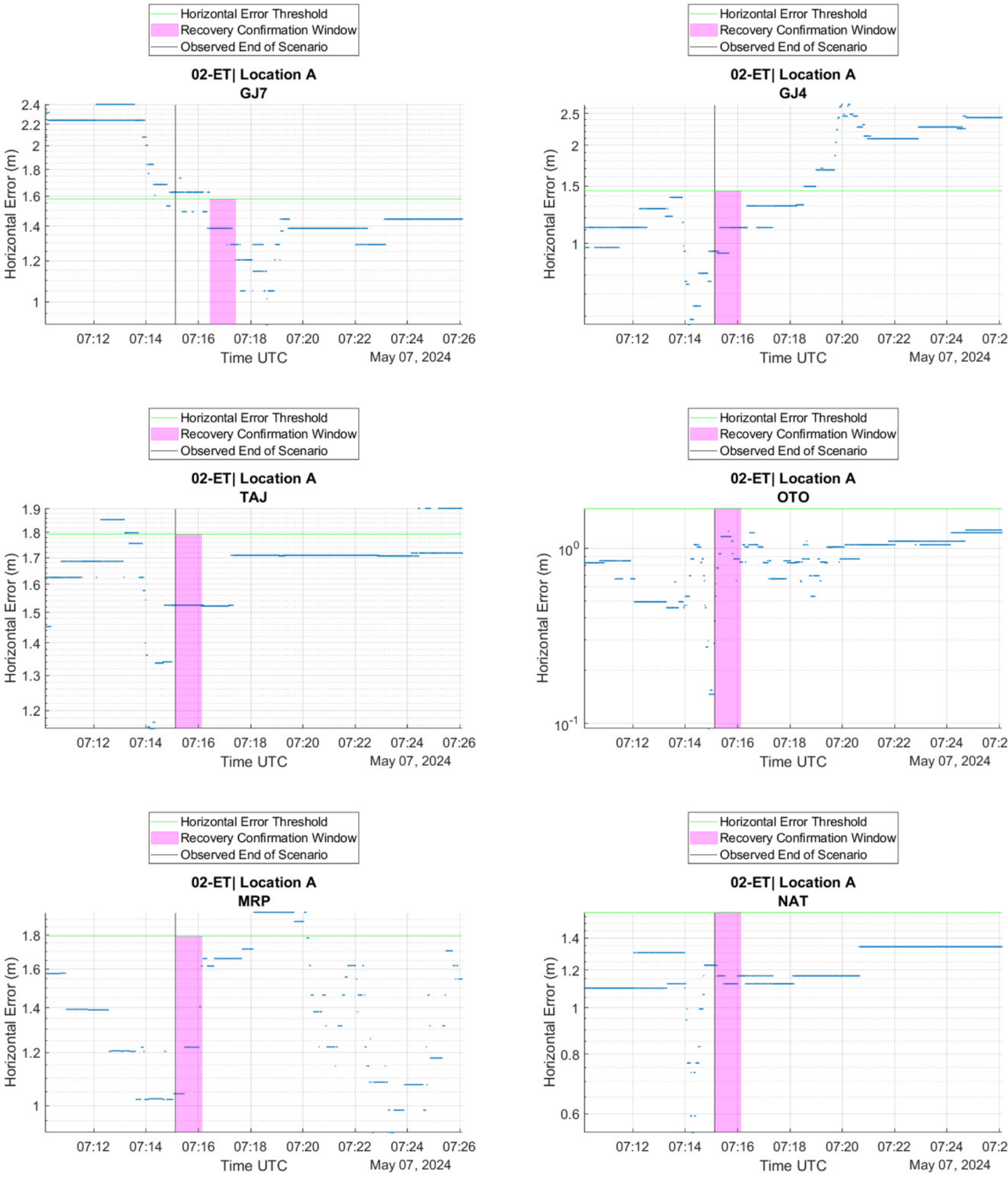


Figure 75. Static recovery analysis time series plots for scenario 02-ET

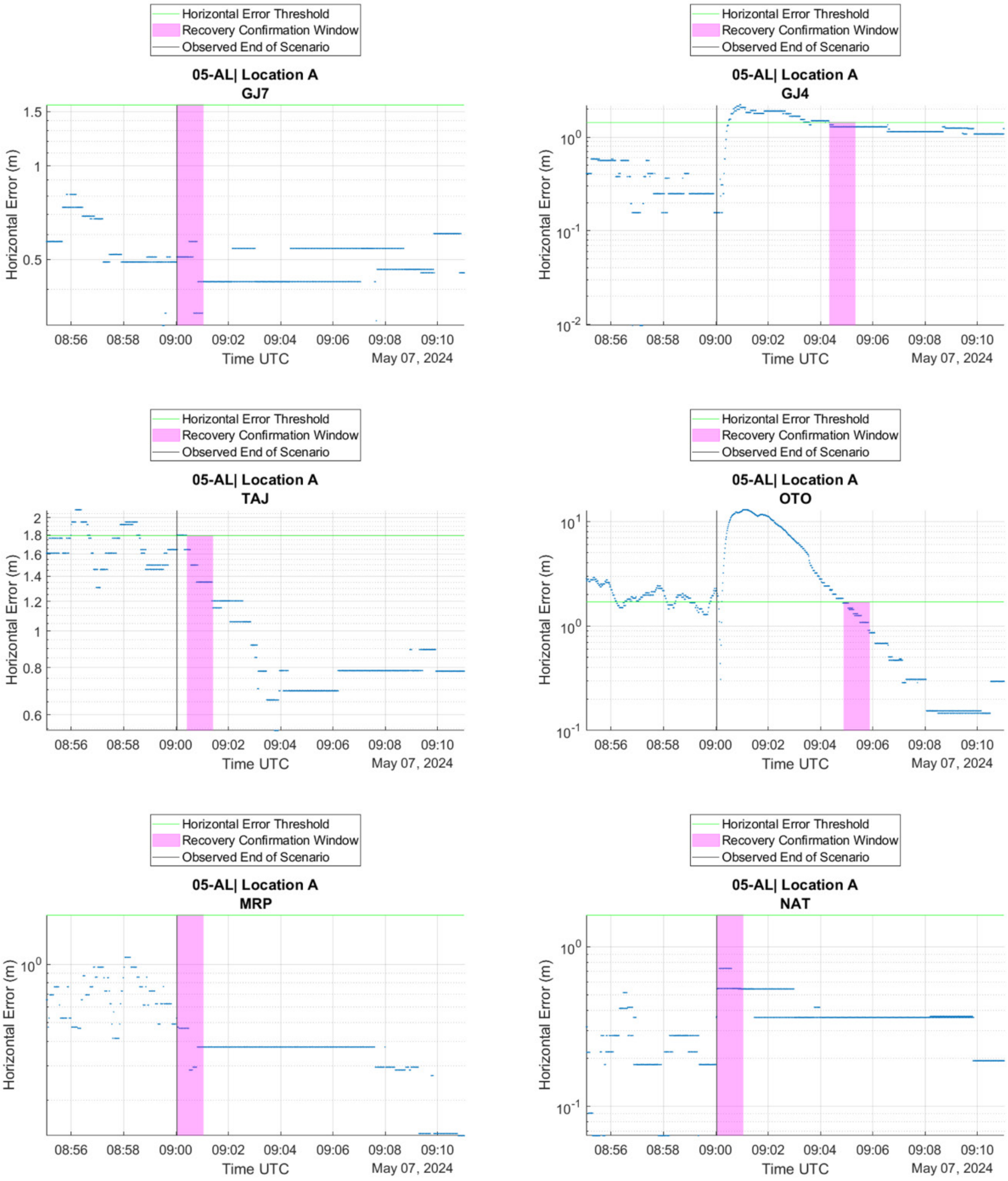


Figure 76. Static recovery analysis time series plots for scenario 05-AL

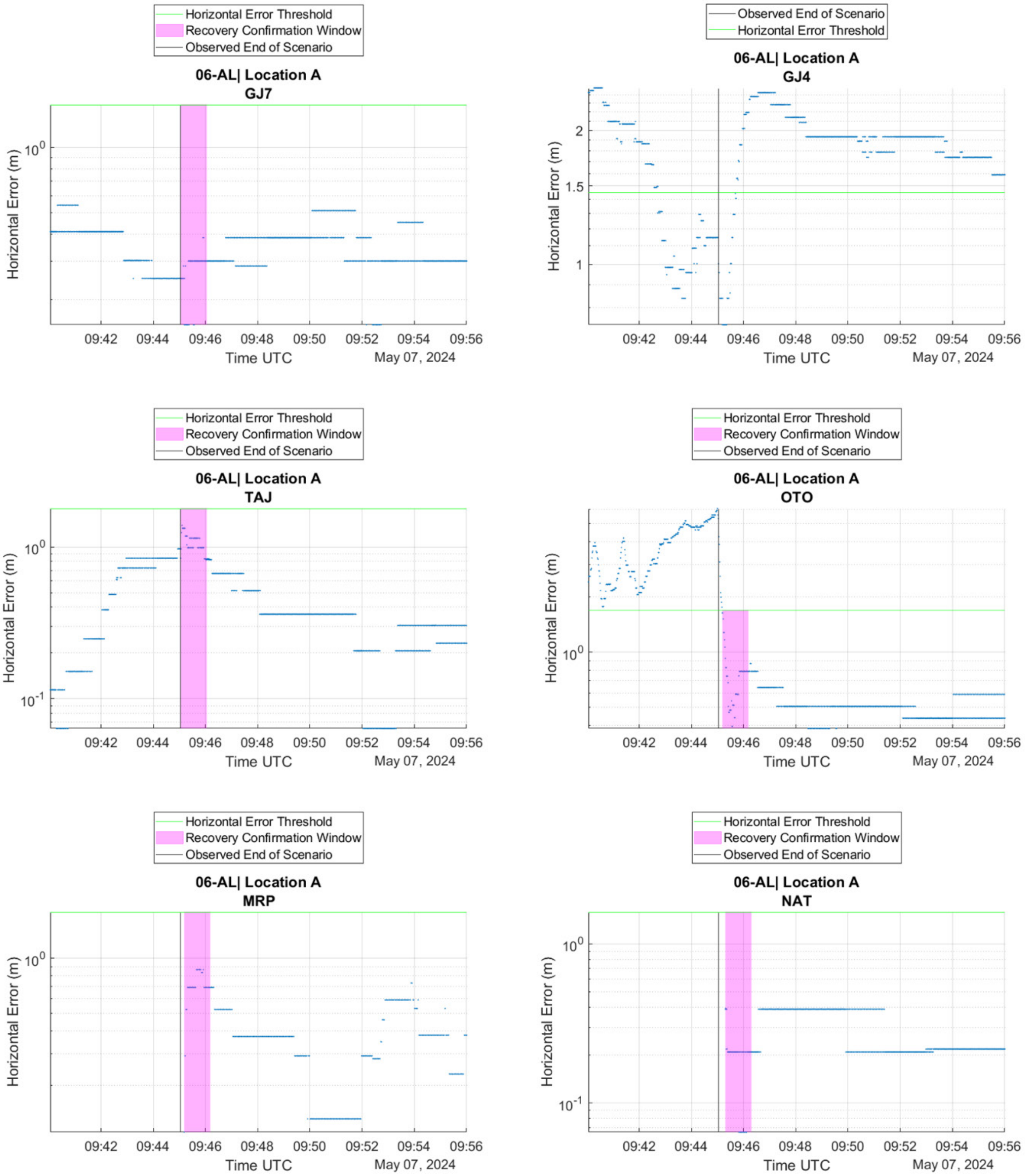


Figure 77. Static recovery analysis time series plots for scenario 06-AL

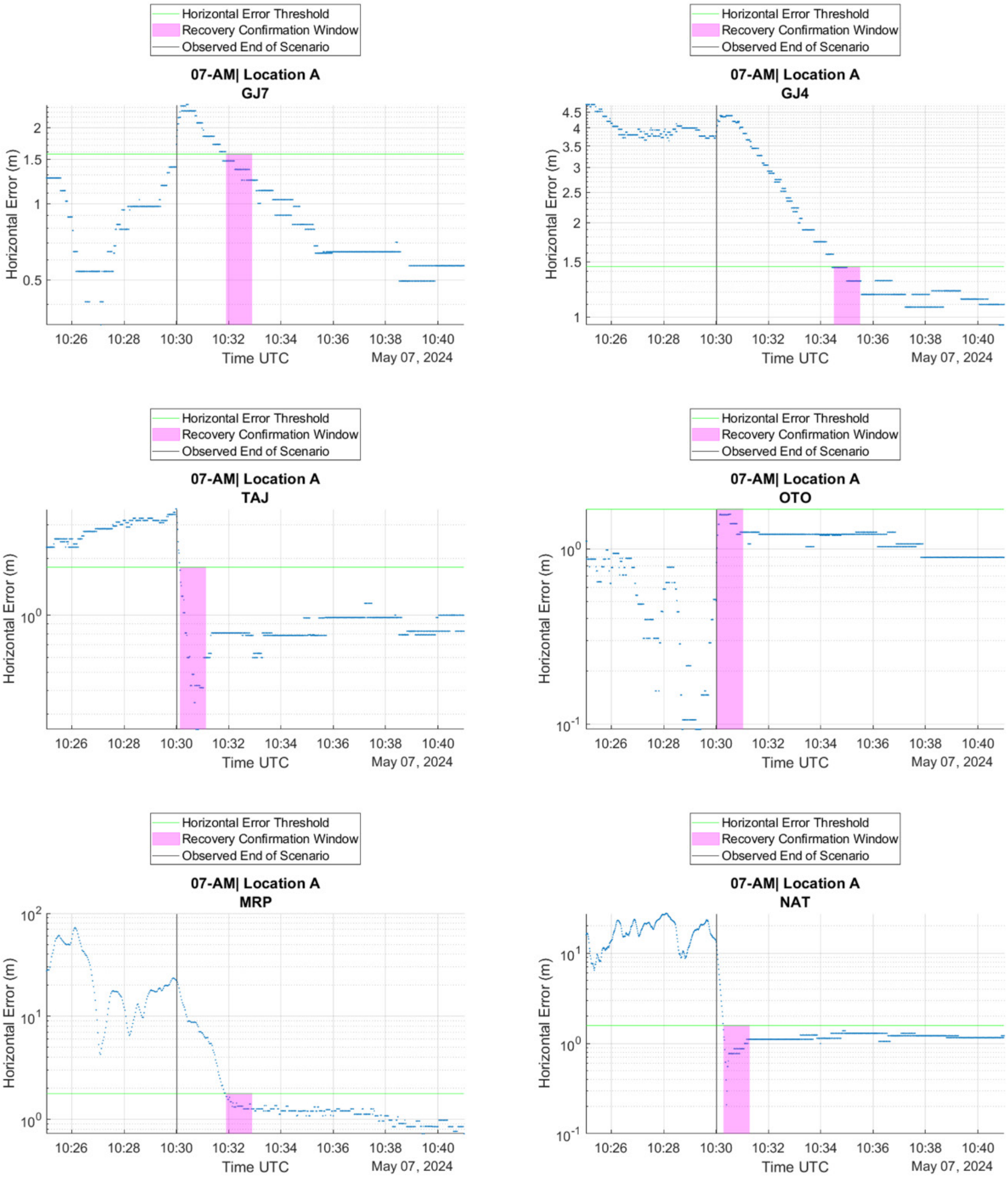


Figure 78. Static recovery analysis time series plots for scenario 07-AM

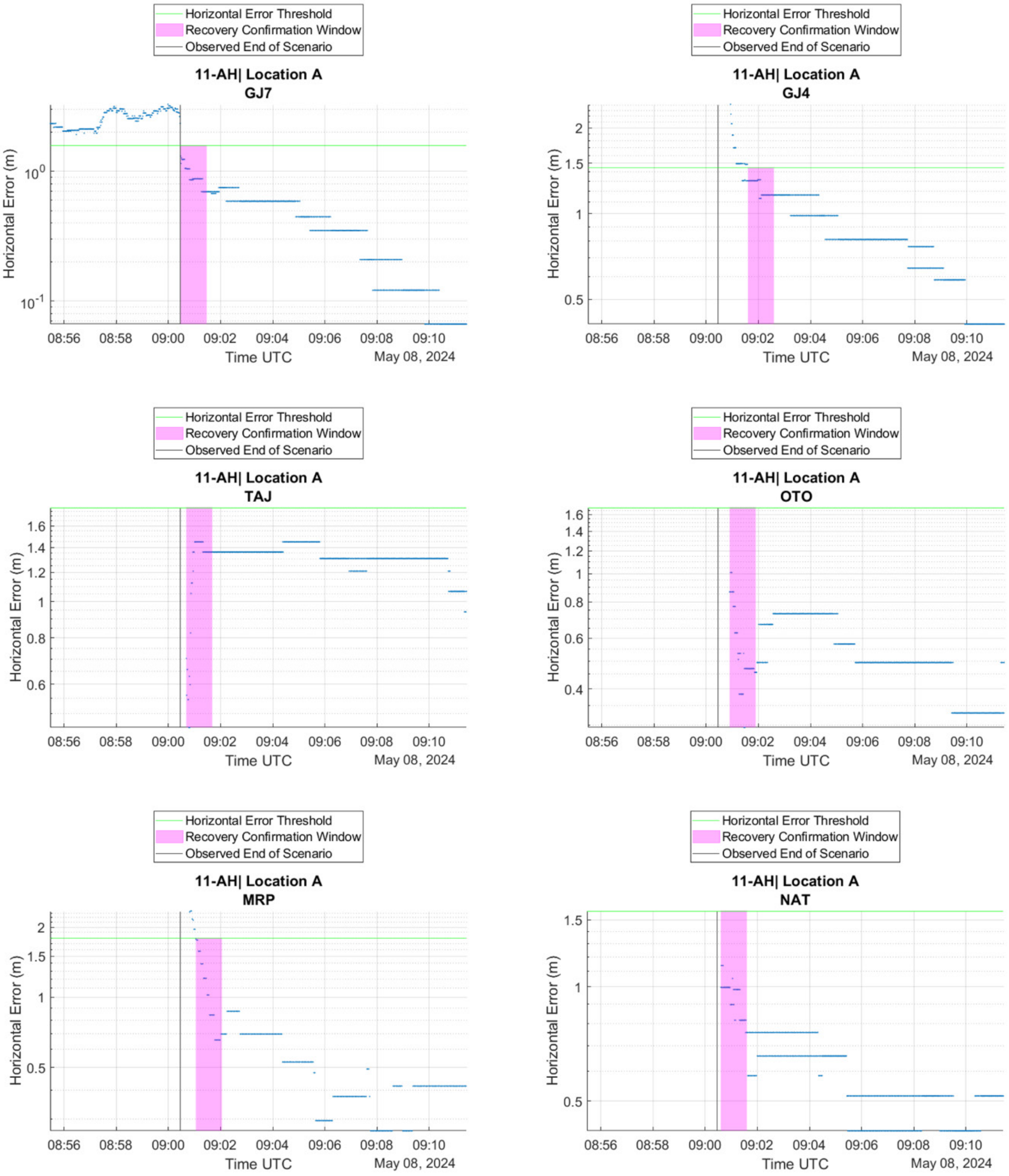


Figure 79. Static recovery analysis time series plots for scenario 11-AH

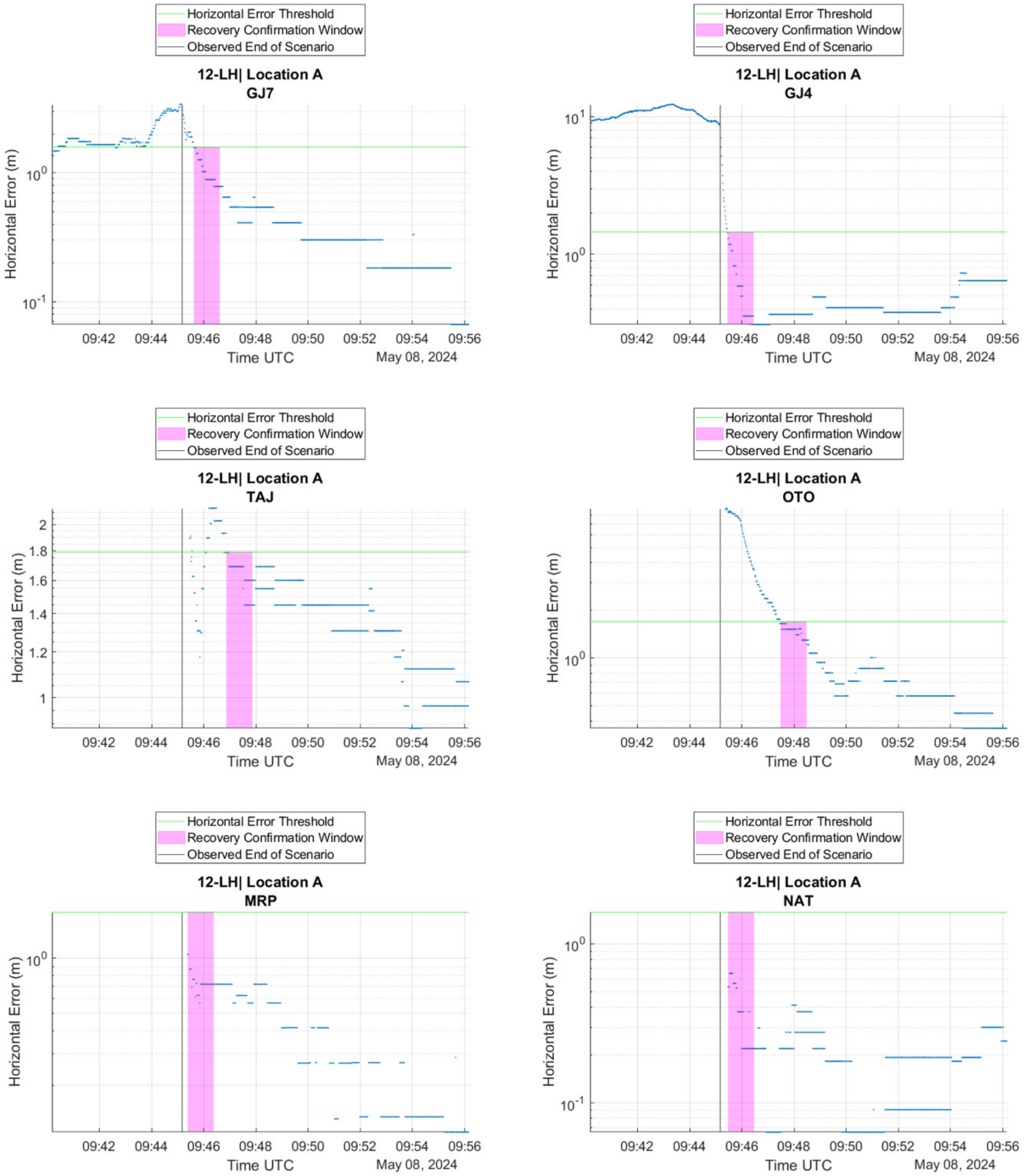


Figure 80. Static recovery analysis time series plots for scenario 12-LH

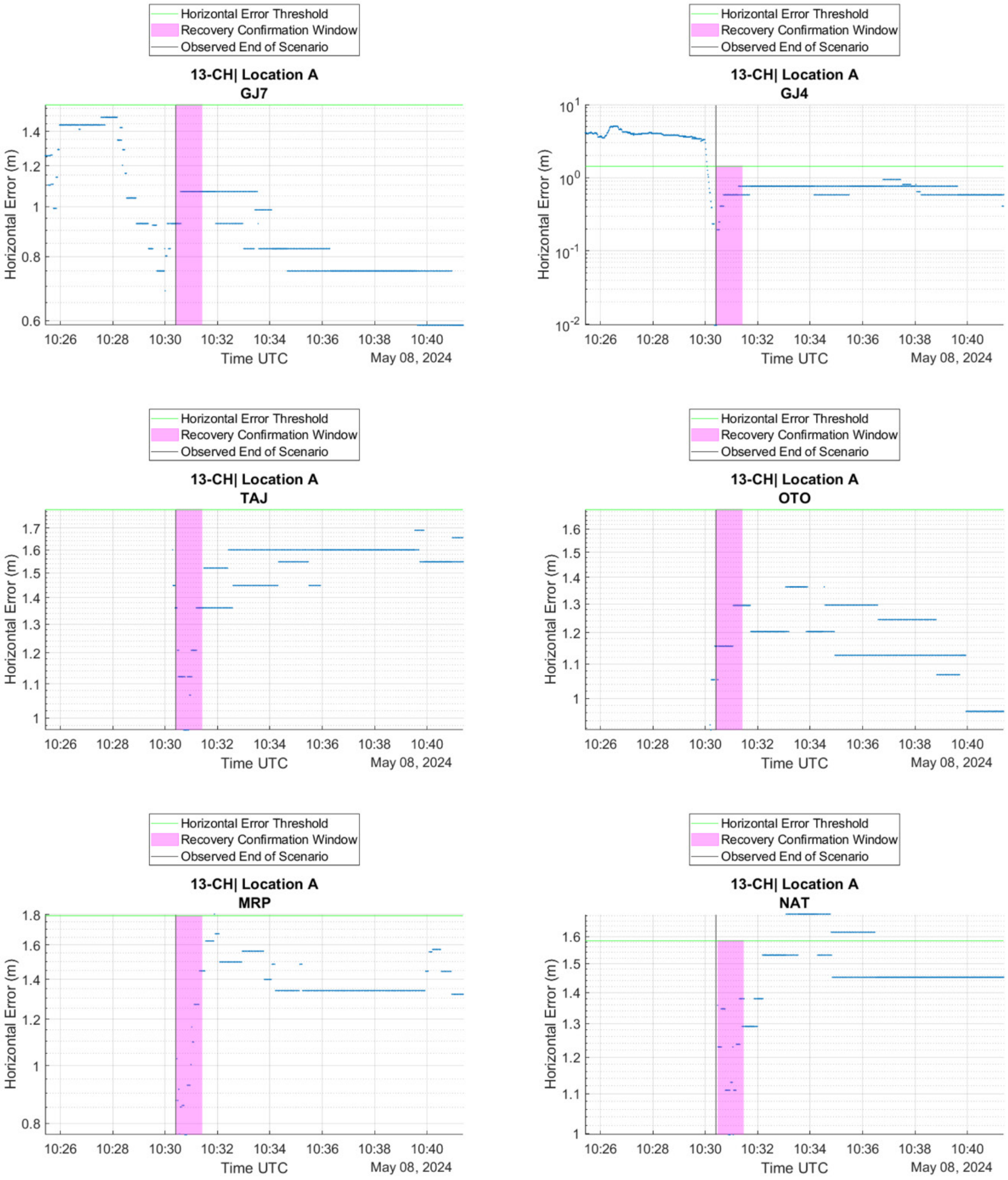


Figure 81. Static recovery analysis time series plots for scenario 13-CH

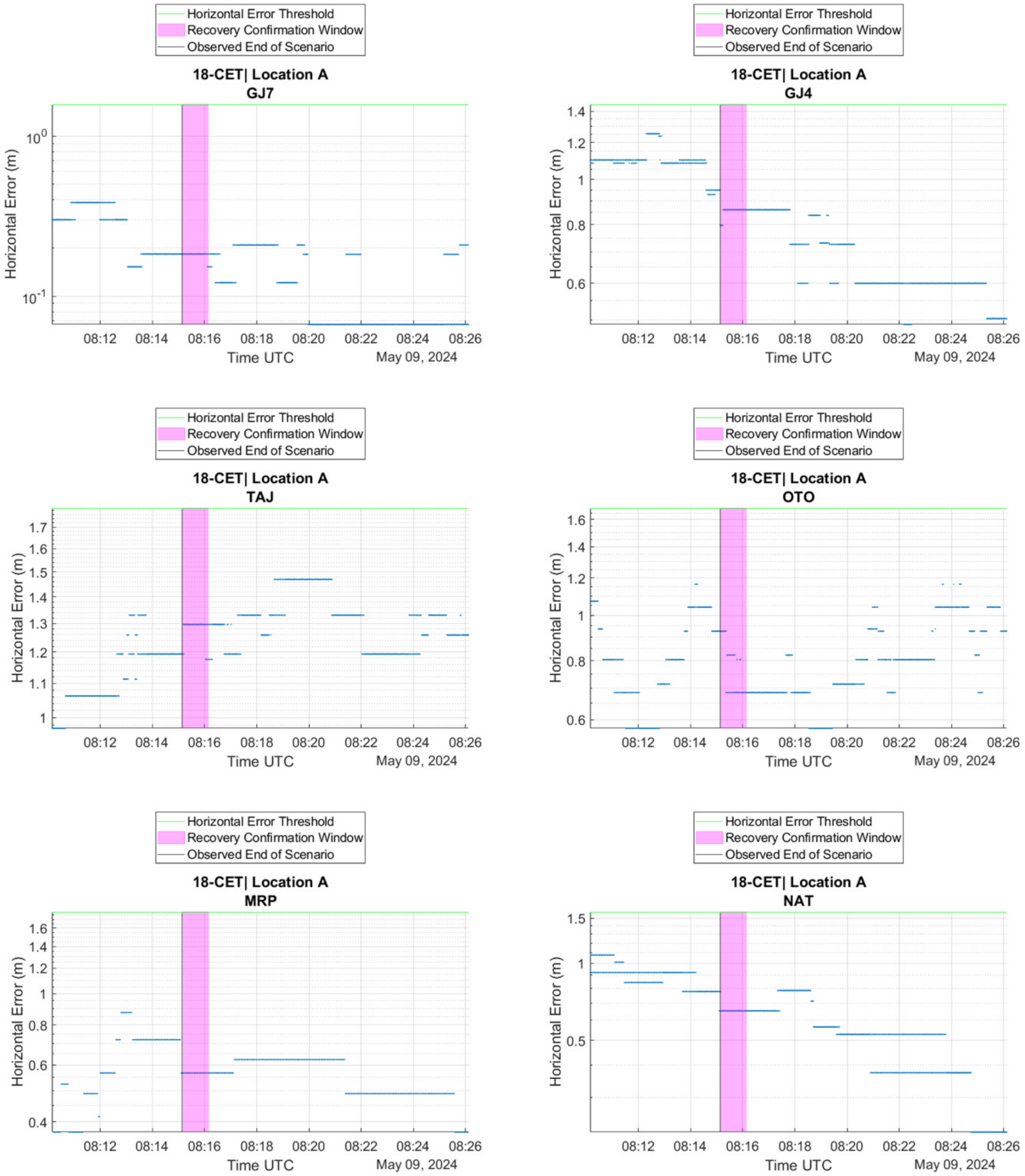


Figure 82. Static recovery analysis time series plots for scenario 18-CET

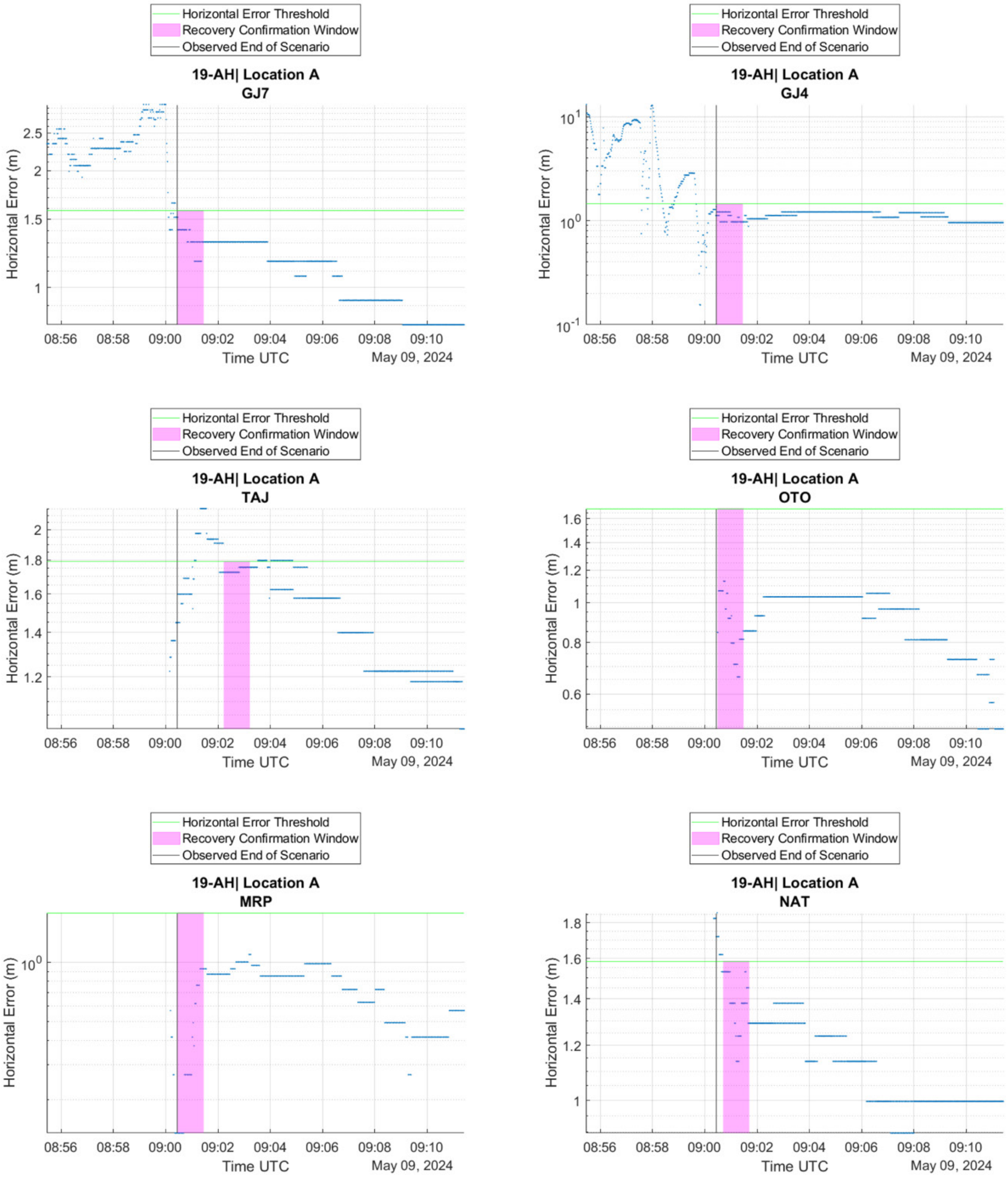


Figure 83. Static recovery analysis time series plots for scenario 19-AH

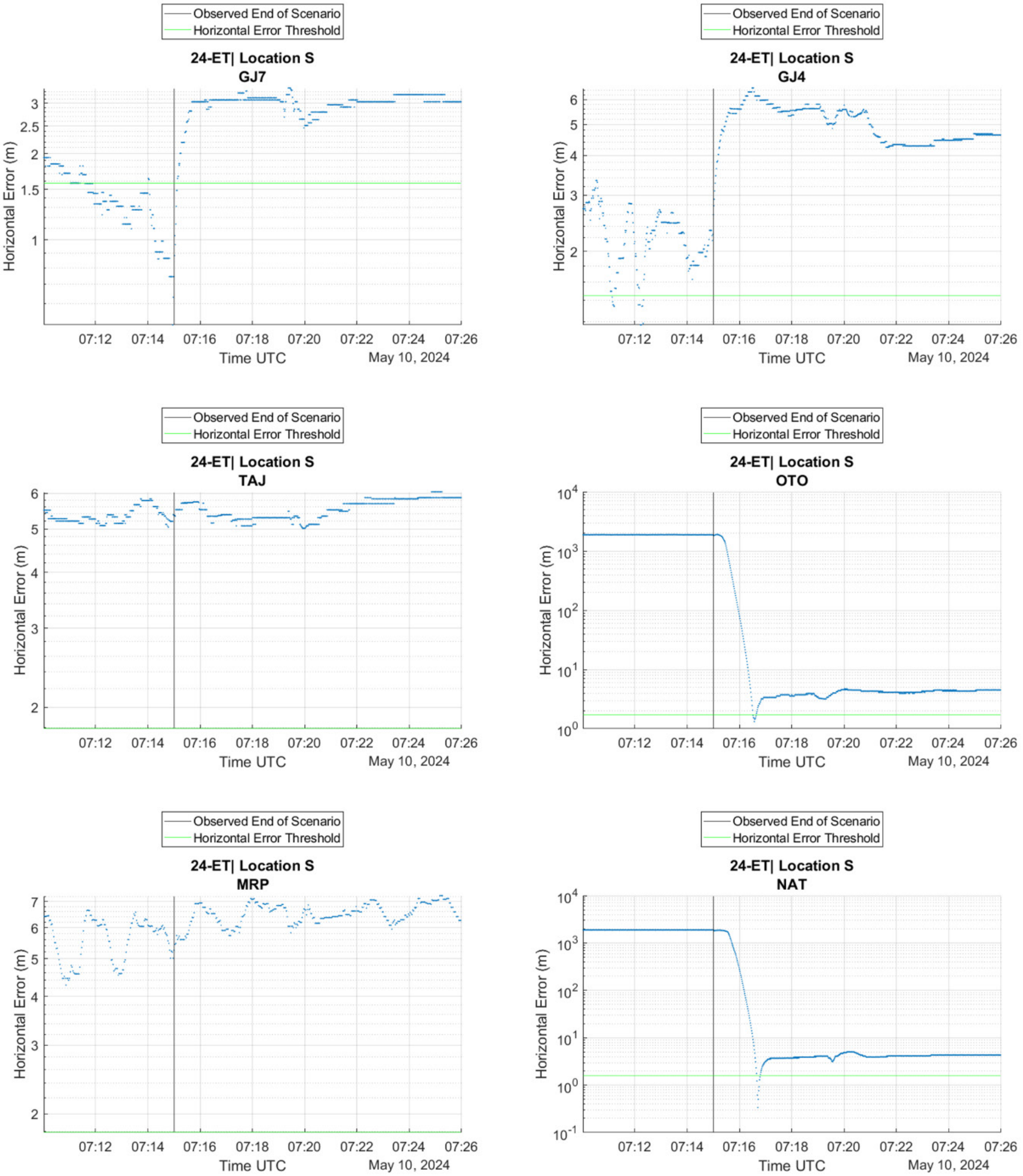


Figure 84. Static recovery analysis time series plots for scenario 24-ET

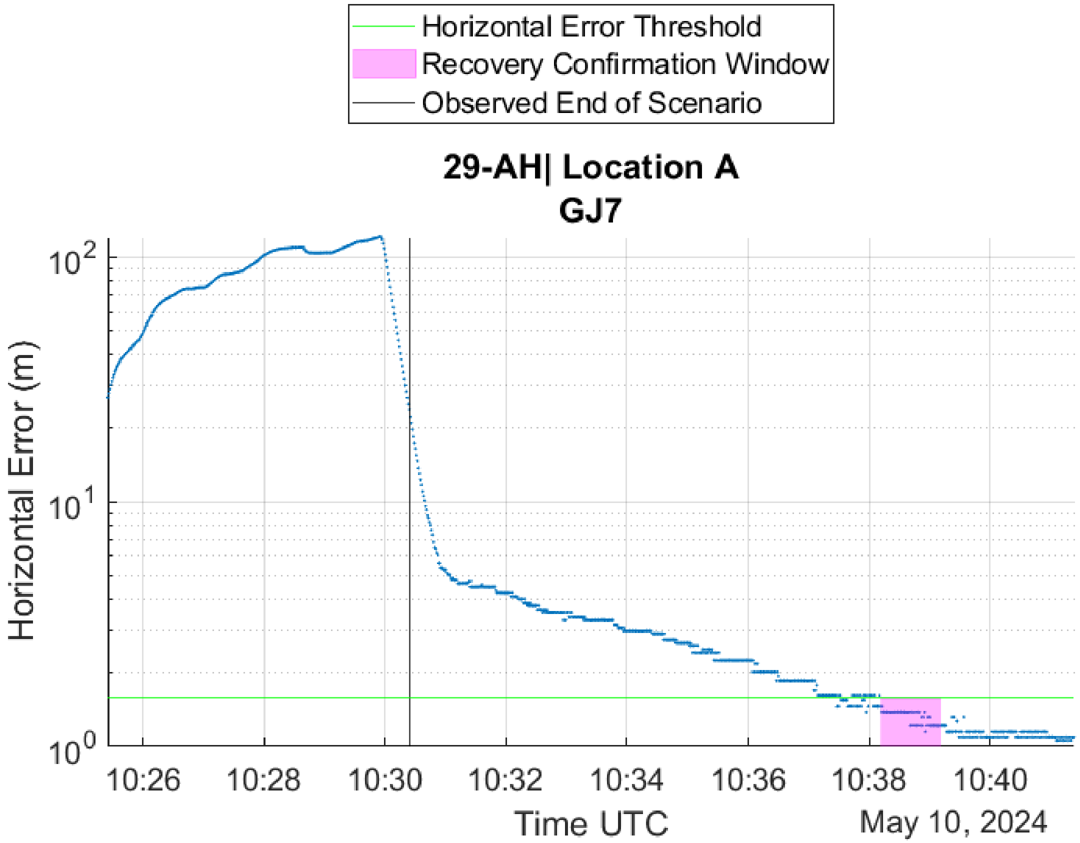


Figure 85. Static recovery analysis time series plots for scenario 29-AH.

(All devices other than GJ7 were excluded due to disruptions during data collection)

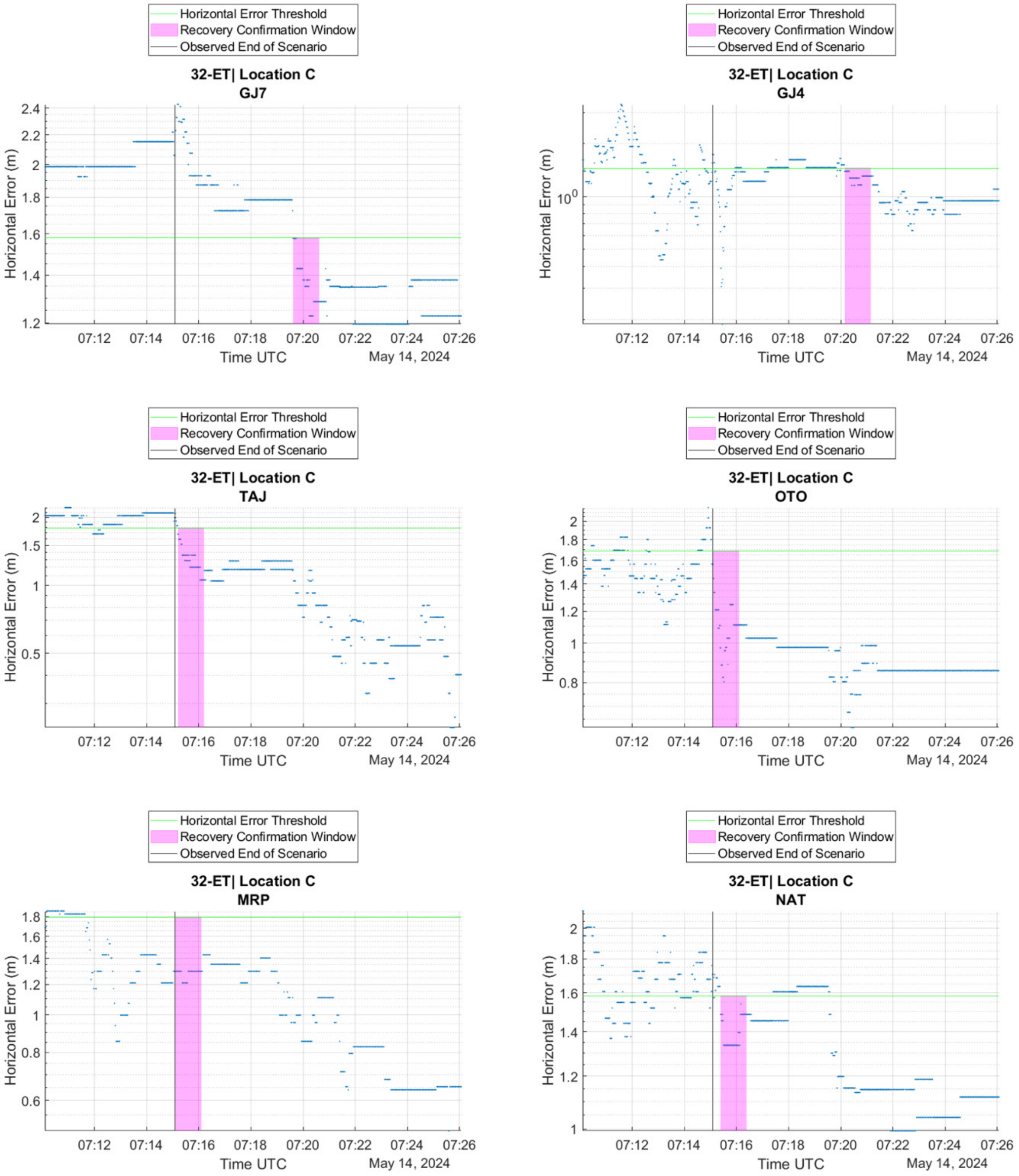


Figure 86. Static recovery analysis time series plots for scenario 32-ET

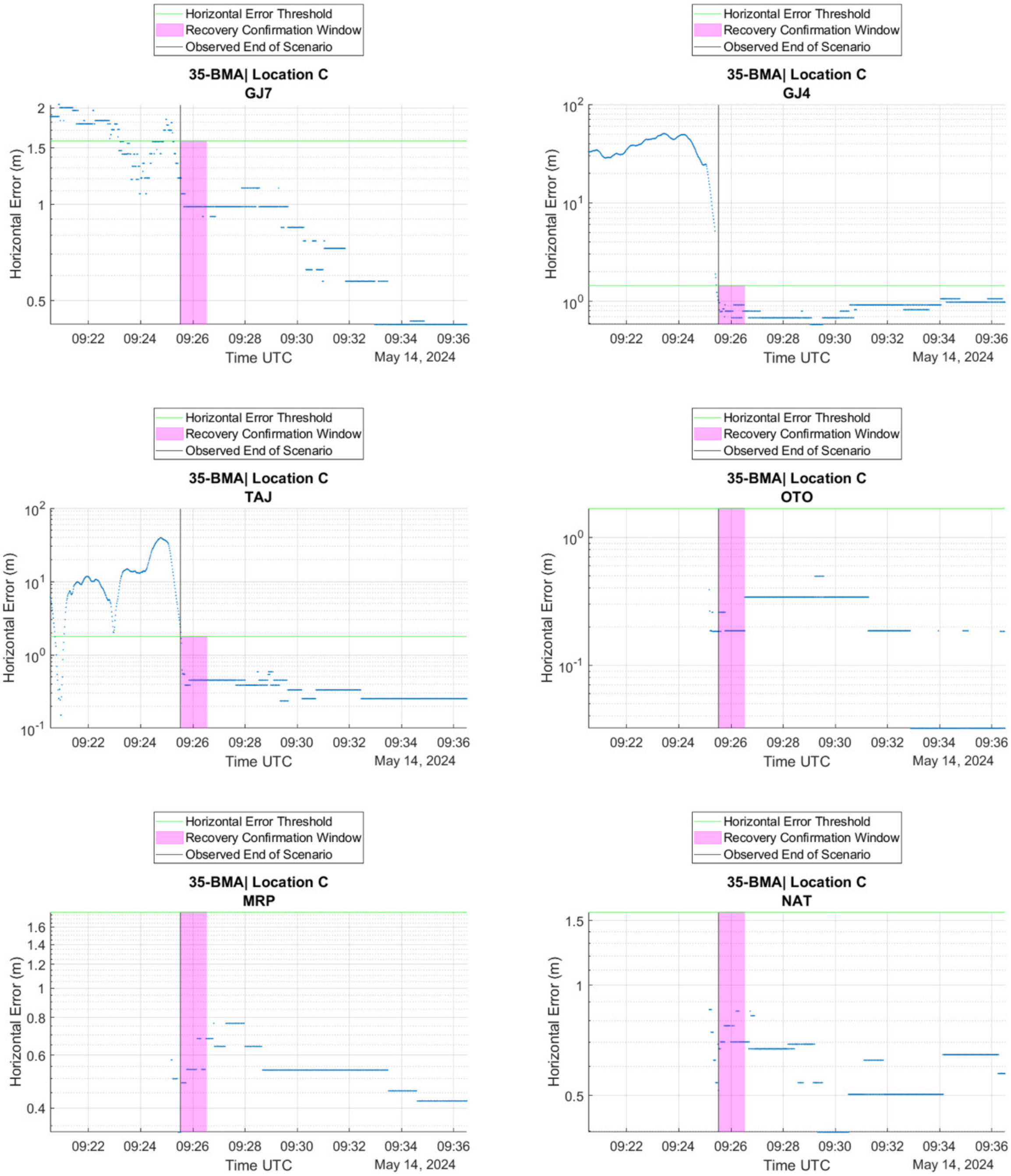


Figure 87. Static recovery analysis time series plots for scenario 35-BMA

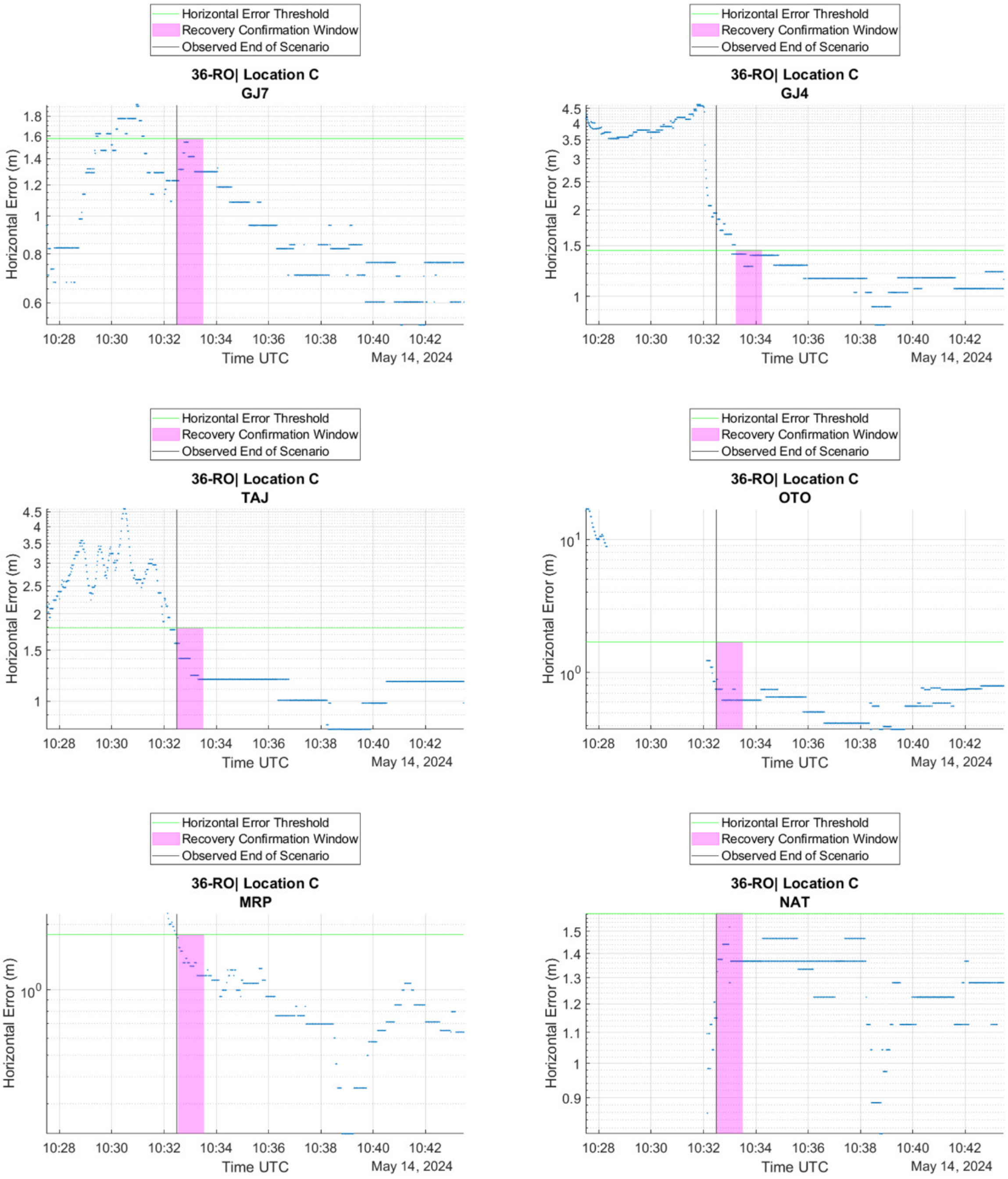


Figure 88. Static recovery analysis time series plots for scenario 36-RO

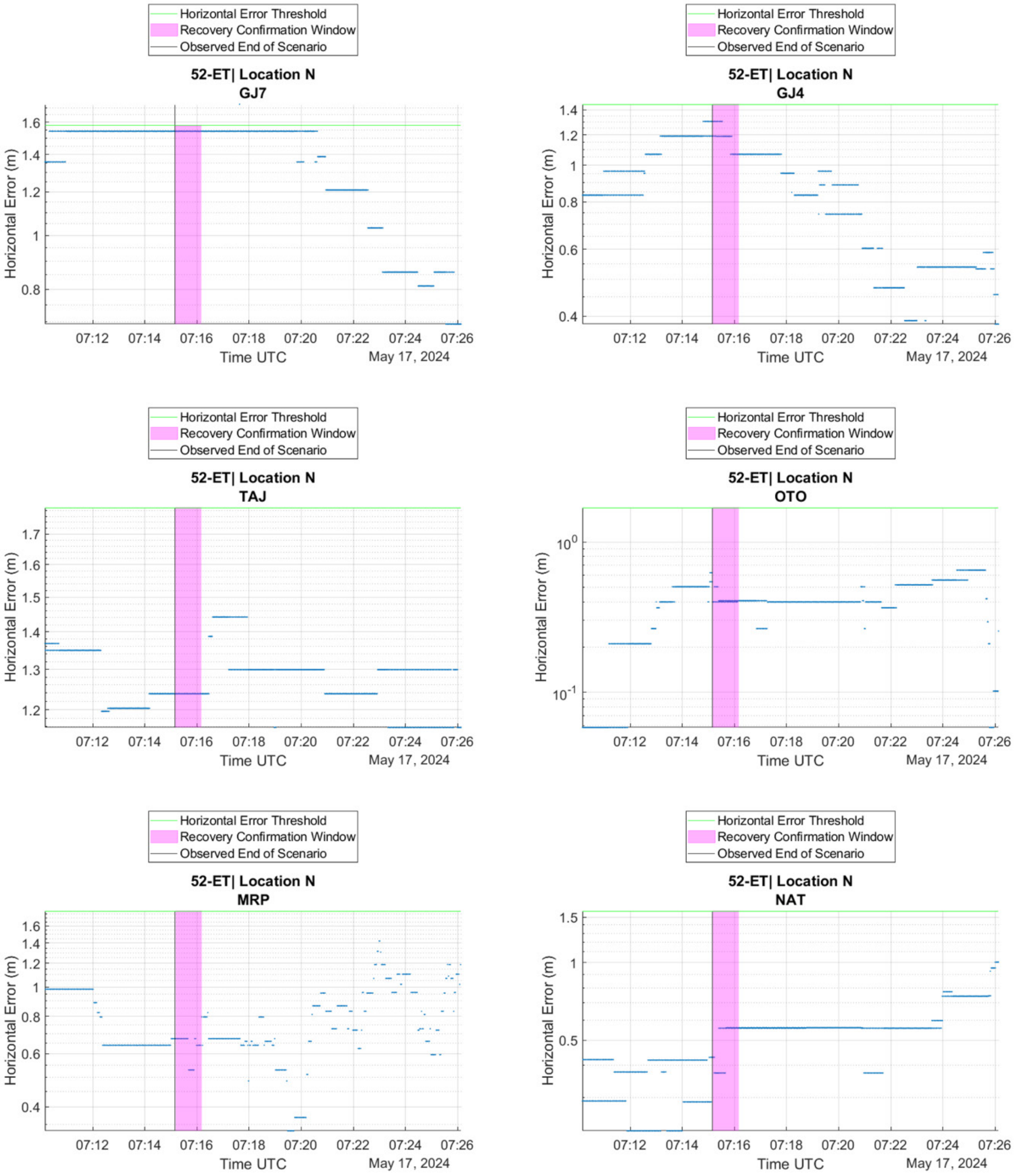


Figure 89. Static recovery analysis time series plots for scenario 52-ET

12. Bibliography

https://www.gao.gov/assets/gao-21-320sp.pdf

https://navisp.esa.int/uploads/files/documents/MarRINav-%20Mike%20Fairbanks%20-%20NLA%20International.pdf

https://navi.ion.org/content/68/3/465

https://thedebrief.org/the-u-s-air-force-and-mit-successfully-fly-aircraft-using-jam-proof-ai-enhanced-magnetic-navigation/

https://www.ion.org/publications/abstract.cfm?articleID=18325

https://insidegnss.com/fleshing-out-the-leo-pnt-landscape/

https://arstechnica.com/science/2023/06/scientists-conduct-first-test-of-a-wireless-cosmic-ray-navigation-system/

https://www.skylinenav.com/home

https://www.getvermeer.com

https://www.gps.gov/governance/advisory/meetings/2023-05/murphy.pdf

D Boland, Surepoints – Deep Learning for custom Vision Aided Navigation Descriptors, United States Air Force Research Laboratory. 2023

M Ferguson, C Ito, Self Positioning Off Targeted Anti GPS Emitters (SPOTAGE), Naval Information Warfare Center Pacific (NIWC Pacific), Code 55780, Communications and Networks Department, Presented to: ION Joint Navigation Conference 2021

T Haydon, S Carda, B Conder, Sandia National Labs, A Modern Terrain-Aided Navigation Algorithm, , Presented to: ION Joint Navigation Conference 2021

A Conte, N Saluzzi, J Brodovsky, et al., Navigation Filtering Supported By Magnetic Particle Filtering, Navigation Research and Development Center - The Applied Research Laboratory, Pennsylvania State University, Presented to: ION Joint Navigation Conference 2021

T Stephens, R Merritt, R Compton, et al., Magnetic Anomaly Aided Navigation Operability Recommendations, Honeywell Corporation, Presented to: ION Joint Navigation Conference 2021

R B. Choroszucha, J Landon, T Johnsrud, et al., Ship Based Magnetic Anomaly Navigation and Characterization Test Results, Guidance, Navigation, & Control, Raytheon Technologies, Presented to: ION Joint Navigation Conference 2021

L Bergeron, A Nielsen, Ph.D., Magnetic Anomaly Mapping For Navigation, Air Force Institute of Technology Autonomy and Navigation Technology Center, Presented to: ION Joint Navigation Conference 2021

G Reynolds, C Blankenship, et al., Vision-Based Navigation Integration and Testing on a UAS Army Manned Rotorcraft, US Army CCDC Aviation and Missile Center, Leidos, Presented to: ION Joint Navigation Conference 2021

K Sweeney, H Staack, Z Fisher, A Walker, Honeywell Vision-Aided Navigation: Resiliency For Airborne GPS-Denied Navigation, Honeywell, Presented to: ION Joint Navigation Conference 2021

L Scott, LEO Navigation Systems: A Radio Guy's Perspective, LS Consulting, Presented to: ION Joint Navigation Conference 2021

Evaluation of Diverged Optics for Optical Multilateration, Naval Information Warfare Center – Pacific, Presented to: ION Joint Navigation Conference 2021

M Castleberry, S Gambino, T Mitchell, et al., Ground Vehicle Vision Navigation Map Matching Test Results Using Tactical Army Hardware and Satellite-Derived 3D Geospatial Data, Leidos, Presented to: ION Joint Navigation Conference 2021

A Luong, K Morris, K Cohen, B White, P Jhaveri, Osiris: Simultaneous Localization Mapping Based on RF Signals, Sandia National Laboratories, Presented to: ION Joint Navigation Conference 2021

R Madison, O Mise, Visual-Inertial Navigation in the Dark, Thales, Presented to: ION Joint Navigation Conference 2021

S Moafipoor, B Despres, H Maquet, LEO and PNT Applications: Accuracy Assessment Using Multi-Sensor Fusion, Geodetics Inc., Presented to: ION Joint Navigation Conference 2021

Cornick et al.: Localizing Ground Penetrating RADAR: A Step Toward Robust Autonomous Ground Vehicle Localization, MIT Lincoln Laboratory, Journal of Field Robotics 33(1), 82–102. 2016

Meng, L.; Yang, L.; Yang, W.; Zhang, L. (2022). A Survey of GNSS Spoofing and Anti-Spoofing Technology. Remote Sensing. 14, 4826.
https://doi.org/10.3390/rs14194826

CRFS, (2022, December). How to Deal with GPS Jamming and Spoofing. Retrieved from CRFS: https://www.crfs.com/blog/how-to-deal-with-gps-jamming-and-spoofing/

End Run Technologies. (2022, December). GPS Anti-Jam Antenna. Retrieved from EndRun Technologies: https://endruntechnologies.com/products/antennas-accessories/gps-anti-jam-antenna

Hexagon. (2022, December). Anti-Jam Antenna Systems (GAJT). Retrieved from Hexagon: https://novatel.com/products/anti-jam-antenna-systems-gajt

MARAD. (2022, December). The Ready Reserve Force (RRF). Retrieved from MARAD: https://www.maritime.dot.gov/national-defense-reserve-fleet/ndrf/maritime-administration%E2%80%99s-ready-reserve-force

MARAD. (2022, December). Maritime Security Program (MSP). Retrieved from MARAD: https://www.maritime.dot.gov/national-security/strategic-sealift/maritime-security-program-msp

U.S. NAVY. (2022, December). Military Sealift Command (MSC). Retrieved from U.S. Navy: https://www.msc.usff.navy.mil/About-Us/Mission

Septentrio. (2022, December). OSNMA: the latest in GNSS anti-spoofing security. Retrieved from Septentrio:
https://www.septentrio.com/en/learn-more/insights/osnma-latest-gnss-anti-spoofing-security

Tallysman. (2022, December). Anti-Jam Technology. Retrieved from Tallysman: https://www.tallysman.com/technology/anti-jam-technology/

Furuno Installation Manual GNSS Navigator Model GP-170, pg. v.

https://infinidome.com/otosphere/

https://novatel.com/products/anti-jam-antenna-systems-gajt

Volpe National Transportation Systems Center. (2022, July). U.S. Department of Transportation Maritime Administration PNT Resiliency Pilot Program. Cambridge, MA: U.S. Dept. of Transportation.

U.S. Department of Transportation
John A. Volpe National Transportation Systems Center
220 Binney Street
Cambridge, MA 02142-1093

617-494-2000
www.volpe.dot.gov

DOT-VNTSC-OST-25-04