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

Final Report

Final Report — March 2023

DOT-VNTSC-OSTR-23-02

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

(Cover photo credit: Volpe Center)

U.S. Department of Transportation
Volpe Center

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
March 2023	Updated Final Report	

4. TITLE AND SUBTITLE
DOT Pilot Program - MARAD

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Stephen Mackey, Andrew Hansen, Hadi Wassaf, George Mantis, Eric Wallischeck, Christopher Scarpone, Karl Shallberg, John Flake, Roger Ishimoto

5d. PROJECT NUMBER
51OS92A421 / 51OS92A421

5e. TASK NUMBER
UM175 / VM175

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Department of Transportation
John A Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142-1093

8. PERFORMING ORGANIZATION REPORT NUMBER
DOT-VNTSC-OSTR-23-02

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of the Assistant 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)
OST-R

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.

15. SUBJECT TERMS
NISTIR 8283

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			George Mantis
			SAR	115	**19b. TELEPHONE NUMBER** *(include area code)* 617-494-2732

Standard Form 298 (Rev. 8-98)

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

Abbreviations, Acronyms, and Initialisms

Abbreviation	Term
1PPS	One pulse-per-second
3D	Three dimensional
AGC	Automatic gain control
AIS	Automatic Identification System
BGAN	Broad Global Area Network
C/A	Coarse/Acquisition
CMCI	Carrier Range Corrected for Ionosphere
COTS	Commercial off-the-shelf
CPNT	Complementary positioning, navigation, and timing
CRPA	Controlled reception pattern antenna
CRUCIBLE	Federal data repository of suspected cases of GNSS purposeful interference
C/N_O	Carrier to noise ratio
CSF	Cybersecurity framework
DHS	U.S. Department of Homeland Security
DME	Distance measuring equipment
ECDIS	Electronic chart and information display system
EMCON	Emissions control
EO	Executive Order
EPIRB	Emergency Positioning Indicating Radio Beacon
GET-CI	GPS Equipment Testing for Critical Infrastructure
GIS	Geographic Information System
GLONASS	GLObal NAvigation Satellite System
GMDSS	Maritime Distress and Safety Systems
GNSS	Global navigation satellite system
GPS	Global Positioning System
IMU	Inertial measurement unit
LEO	Low Earth orbit
MARAD	Maritime Administration
MSC	Military Sealift Command
NATO	North Atlantic Treaty Organization
NGO	Non-Governmental Organization
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Internal Report
OST-R	Office of the Assistant Secretary of Transportation for Research and Technology
PIDC	Power injector data converter
PIRT	Purposeful Interference Response Team
PNT	Positioning, navigation, and timing
PPP	Precise Point Positioning
PRN	Pseudorandom noise
R&D	Research and Development
RF	Radio frequency
RRF	Ready Reserve Force

Abbreviation	Term
SBAS	Satellite-based augmentation system
SDR	Software defined radio
SS	Steam ship
STL	Satellite time and location
SRMA	Sector Risk Management Agency
TA	Turbo activation
TACAN	Tactical Air Navigation
TIC	Timing Interval Counter
TOA	Time of arrival
USDOT	U.S. Department of Transportation
USTRANSCOM	U.S. Transportation Command
UTC	Coordinated Universal Time

This page is intentionally blank to support duplex printing.

Executive Summary

The Role of GPS in Transportation

The U.S. Global Positioning System (GPS) was originally developed by the U.S. Department of Defense to improve en route navigation and positioning for military purposes. The first GPS satellites were launched in 1978, with the full 24-satellite constellation declared operational in April 1995. The "selective availability" feature—which intentionally degraded the quality of the GPS signal available to civilian users by introducing errors of 50 to 100 meters—was turned off in 2000, increasing the precision of GPS position and opening the door to its widespread adoption for civilian positioning, navigation, and timing, (PNT) applications.

Although GPS was conceived as a military PNT system, its potential for civilian applications system was apparent form the start. The first commercially available GPS receiver was introduced in 1981. At nearly 59 pounds, it was hardly "portable," took nearly 20 minutes to initially acquire a position, and cost over $119,000, putting it out of reach of most users. Subsequent advances in miniaturization of GPS receiver technology, along with a revolution in the development of computer-based geographic information system (GIS) applications—whether mapping, surveying, routing, fleet management, asset recovery, or package tracking—encouraged innovation, spurred growth, and opened new markets beyond basic point-to-point navigation.

Today, GPS has become the ubiquitous global navigation satellite system (GNSS), and the gold standard for PNT services 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 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. 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 Pilot Program sought to raise awareness of the extent to which maritime vessels depend on PNT services; identify approaches for maritime operations to withstand disruption or manipulation of those services; and to engage the maritime community to promote the responsible use of PNT services. In December 2020, USDOT hosted a workshop, "GPS Jamming and Spoofing in the Maritime Environment," which featured speakers from government, industry, and non-profit PNT organizations. The objective of this 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 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, 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 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 and backup services that could serve as mitigations to operational impacts. Subsequent sections of the report expand on the technical aspects of the three areas.

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. Extension of complementary PNT demonstration evaluations to low Earth orbit (LEO) PNT services with Government furnished equipment.

The data-gathering effort MARAD determined that RRF ships typically have two or three GPS units installed—commonly the Furuno GP170 or Furuno GP150—with a few exceptions. The GPS unit supplies PNT information to the vessel's electronic chart display and information system (ECDIS), which also relies on other GPS units as backup PNT sources. This system design represents a vulnerability to the RRF vessels by being reliant on GPS alone for PNT data. PNT information derived from the GPS receivers is utilized by several downstream situational awareness and safety-critical systems, including automatic identification systems (AIS), emergency positioning indicating radio beacons (EPIRBs), and Global Maritime Distress and Safety Systems (GMDSS).

During the period August 28–September 2, 2021, the study team embarked aboard the SS *Antares* during a Turbo Activation event (an annual activation of vessels in the U.S. Transportation Command Organic Surge Fleet) that involved 18 ships (17 MARAD RRF ships and 1 Military Sealift Command (MSC) vessel). The *Antares* crew conducted a number of required demonstration activities in port, followed by several specific maneuvers at sea over the course of the exercise. During the exercise aboard the *Antares*, GNSS measurement and positioning performance data was collected and evaluated. The technical team performed a radio frequency (RF) and GPS measurement survey to characterize

emissions and GPS performance in a typical maritime operational environment. The purpose of this evaluation was to provide insight on typical GPS performance in the maritime environment, to support recommendations being developed to improve maritime PNT resiliency.

A survey-grade dual GPS receiver (multi-frequency, multi-constellation GNSS receiver) with an internal inertial measurement unit (IMU) was installed on the *Antares* as part of the testing equipment. A spectrum analyzer was used to sweep GPS frequency bands to capture spectrum transmissions in and near the GPS bands (L1, L2, and L5) and to collect GPS measurement data. The GPS spectral data was inspected to determine emitters close to the GPS band, while the wider-band spectral data revealed potential RF spectrum conflicts with PNT technologies and other existing systems. The GPS signal collection enabled characterization of the ship's multipath conditions and provided data useful for investigating shipboard GPS interference.

The Pilot Project also evaluated two elements of a comprehensive resilient solution: a protected primary GPS receiver and use of an alternate PNT source. The primary PNT receiver was protected by enhancing the existing system with a capability to monitor and mitigate GPS signal disruptions by replacing the native GPS antenna with a multi-element nulling antenna capable of suppressing GPS jamming and spoofing signals, as well as unintentional interference signals in the GPS L1 band. The second element investigated the use of a non-GNSS source to provide a form of complementary PNT technology to assist with jamming and spoofing detection. The Project Team selected a system using satellite time and location (STL), a proprietary time-of-arrival (TOA) multilateration system designed by Satelles, Inc. (Reston, VA) offering three-dimensional (3D) positioning and timing using dedicated satellite signals of the Iridium satellite communication system.

The Furuno GP170 receiver was included in a Department of Homeland Security (DHS) "GPS Testing for Critical Infrastructure" (GET-CI) event held at the Mountain Home Range Complex, Idaho, on June 21–26, 2021. The test was conducted in a live-sky environment, with RF jamming and spoofing signals directed at GPS L1 C/A processing. Twenty-two (22) fixed-infrastructure test scenarios were executed over four days. The tests were designed to elicit different equipment responses and included conditions to cause GPS receiver time-and-position to jump or ramp/walk. Tests were also included to stress receiver processing robustness by transmitting erroneous GPS L1 C/A navigation data. For each test, receivers were allowed a clean RF environment to reach steady state prior to the transmission of any spoofing or jamming signals. The spoofed signals were then transmitted with or without the benefit of knock-off jamming.

During the GET-CI event, the Furuno GP170 receiver dropped the valid L1 C/A signals and was captured by the false signals when using its native Furuno GPA017S antenna. This caused the receiver position to "walk" (with the reported position moving approximately 3.8 km) or "jump" (misrepresenting the reported position by approximately 2.9 km), consistent with scenario intentions. The receiver provided little or no indication it had been captured by these spoofed signals. In contrast, when the Furuno GPA017S native antenna was replaced with a Hexagon GAJT-410ML, four-element controlled reception

pattern antenna, and the receiver subjected to the same spoofed signals, the Furuno GP170 receiver reported position estimates consistent with normal performance (with all positions falling within a locus of 7 meters by 9 meters).

To evaluate the use of a complementary PNT source, the Project Team selected a NAL Research Corporation SHOUT tsA prototype unit, on loan from the U.S. Department of Homeland Security, integrated with a Satelles STL subscription service. The SHOUT/Satelles solution offers the potential of a complementary space-based PNT solution. The SHOUT tsA unit was mounted in a USDOT vehicle and fitted with a roof-mounted Iridium patch antenna. Also installed in the vehicle was a dual-antenna NovAtel PwrPak7D-E2 receiver (PwrPak7) (the same GNSS device installed aboard the *Antares*), which was used to determine the positions used for "truth" in the analysis.

The data collection scenario was a highway drive that offered open sky conditions with few obstructions. Data collection took place in December 2021, along a 92-mile round-trip route on I-66 in Virginia, from Exit 60 to Exit 13 and back. The route was chosen to represent, as best as possible, the sky view and dynamics of an ocean voyage, with some recognized differences: a higher speed of travel, more frequent turns, and potential satellite signal obstructions (e.g., overpasses).

During the data collection process, the SHOUT/Satelles solution demonstrated some anomalous performance, with intermittent location errors ranging from 24.1 meters to 178.0 meters. Given the characteristics of the highway test scenario, additional research, testing, and analysis is necessary to determine the root causes of these errors. Additional evaluation is also needed to determine whether the same range of location errors would be found in an actual maritime environment, where vessels generally operate at slower speeds and have a near-universally-unobstructed sky. Overall, however, the SHOUT/Satelles solution was determined to be a viable complementary space-based PNT data source.

Pilot Project Findings and Recommendations

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

1. Identified specific shipboard systems aboard MARAD's Ready Reserve Force vessels that use or form PNT data.
2. Identified a complementary PNT data source suitable for the maritime operating environment to diversify acquisition of PNT data from a non-GPS source—through operational testing and data collection.
3. Detected the disruption and manipulation of PNT services in actual and simulated marine 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 to manage the associated risks to the shipboard systems, networks, and assets dependent on PNT services—by identifying 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 Pilot Program, the findings above 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 results described in this report demonstrate that these solutions should be further evaluated with respect to the full set of operational requirements for a platform such as the MARAD Ready Reserve Force. However, from the PNT Profile perspective, the USDOT Pilot Program findings lead to two 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 paired with the GAJT nulling antenna, the GPS receiver will be unable to demodulate the spoofing data therefore protecting the receiver from the vast majority of both signal and data spoofing attacks. This solution, if desired, does have the capability to serve further a detect-and-characterize function (power and direction of arrival) on interfering signals. Further, a dual antenna/receiver pair can be used to detect a spoofing attack through self-differential means.
2. Augment shipboard equipage in the RRF with LEO-based timing and, potentially, positioning technology. Solutions such as the SHOUT/Satelles STL service can be added with minimal integration (human in the loop procedures) to provide both a check of GPS-based PNT outputs and a complementary space-based PNT source for ship management equipage.

While these recommendations 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 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

1.1 Background

Executive Order (EO) 13905 "Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services" was issued by the White House on February 12, 2020.[1] The goal of this initiative is to foster responsible use of positioning, navigation, and timing (PNT) services by critical infrastructure users, 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 services 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.

Section 4(g) of EO 13905 states, "Within 180 days of the date of this order, the Secretary of Transportation, Secretary of Energy, and Secretary of Homeland Security shall each develop plans to engage with critical infrastructure owners and operators to evaluate the responsible use of PNT services. Each pilot program shall be completed within 1 year of developing the plan, and the results shall be used to inform the development of the relevant PNT profile and research and development (R&D) opportunities." The initiative to develop PNT resiliency plans for transportation critical infrastructure is broadly organized with the U.S. Department of Transportation (USDOT) as the "USDOT Pilot Program."

The Secretary of Transportation has overall leadership responsibility for civil PNT matters. Within USDOT, the Office of the Assistant Secretary of Research and Technology (OST-R) coordinates PNT initiatives and planning across all modes of transportation, including intermodal engagement. The Maritime Administration (MARAD) is the modal administration within USDOT with responsibilities for waterborne transportation. Its programs promote the use of the maritime transportation system, its integration with other modal segments of the National Transportation System, and to strengthen the overall health of the U.S. Merchant Marine. MARAD works across many areas involving ships and shipping, shipbuilding, port operations, vessel operations, national security, the environment, maritime training, workforce development, and maritime safety. MARAD also maintains a fleet of specialized cargo ships, known as the Ready Reserve Force (RRF), which provide surge sealift during war and national emergencies.

The MARAD RRF fleet was identified as a strong candidate for the U.S. Department of Transportation Pilot Program. This initiative addresses Global Positioning System (GPS) jamming and spoofing that affects maritime vessels, and will consider complementary PNT technologies that could be adopted to

[1] 85 FR 9359, available at https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing

mitigate those impacts.[2] Applicable results and lessons learned from the MARAD Pilot Program will be considered when addressing other modes of transportation (aviation, rail, vehicles, and pipeline) to support PNT resiliency.

1.2 Pilot Project Overview

In response to EO 13905, USDOT, through the Office of the Assistant Secretary for Research and Technology (OST-R) and the Maritime Administration (MARAD), developed a Pilot Program Plan focused on addressing GPS jamming and spoofing in the maritime environment. OST-R put an interagency agreement in place with the Volpe National Transportation System Center (Volpe Center) to support this Pilot Program. A primary goal of the USDOT Pilot Program is to apply the NISTIR 8323 Foundational PNT Profile (discussed in Section 2) through an application-based effort. Specific tasks and outcomes of the USDOT Pilot Program Plan are listed in Table 1.

Table 1. USDOT Pilot Program Plan Tasks and Outcomes

Task	Outcomes
1: Stakeholder Engagement	Identification of Stakeholders
	Outreach to Stakeholders and Virtual Stakeholder Workshop
	Briefing of Results from Stakeholder Engagement
2: Complementary PNT Testing	Complementary PNT Test Plan
	Jamming and Spoofing Detection
	Results of Complementary PNT Testing
3: Report of Results from the USDOT Pilot Program	Report of results from stakeholder engagement, pilot testing and recommendations for PNT profile development

1.2.1 Stakeholder Engagement

A key aspect of the Pilot Program is outreach to stakeholders to understand their operational experience in dealing with GPS jamming and spoofing in the maritime environment. Key stakeholders were identified and included operators within both the Government and the private sector. OST-R (including the Volpe Center) and MARAD identified stakeholders to conduct and participate in interviews, including

[2] As defined by the Department of Homeland Security, jamming is "intentionally produced [radiofrequency] waveforms that have the same effect as interference; the only difference is the intent to degrade or deny a target receiver's operation," while spoofing is "caused by [radiofrequency] waveforms that mimic true signals in some ways, but deny, degrade, disrupt, or deceive a receiver's operation when they are processed." See U.S. Department of Homeland Security, "Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure," no date, https://www.cisa.gov/uscert/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf.

through Sector Risk Management Agency (SRMA) processes for maritime transportation. The objectives of stakeholder engagement were three-fold:

1. To understand how positioning, navigation, and timing services support maritime applications.
2. To determine how operators respond when PNT is denied, disrupted, or manipulated in a maritime environment.
3. To identify what options are available to reduce operational impact and increase PNT resiliency.

1.2.2 Complementary PNT Testing

The USDOT Pilot Program leveraged results from the Complementary PNT Demonstration Program conducted by the OST-R/Volpe Center in March 2020, along with feedback from the stakeholder engagement.[3] Positioning and navigation technologies that demonstrated promise or potential for utilization in a maritime environment were incorporated into the USDOT Pilot Program testing. Characterization of the RF operational environment as well as testing of the complementary PNT technologies were conducted under operational and other nominal open sky conditions as well as during scheduled GPS signal disruption coordinated tests. In order to assess existing and proposed PNT system configuration performance when GPS signals are intentionally disrupted, USDOT participated in the GPS Equipment Testing for Critical Infrastructure (GET-CI), a "live-sky" GPS jamming and spoofing event organized by the Department of Homeland Security during the month of June, 2021.[4] [5]

Complementary PNT testing of sensors, data collection equipment, and software involved either laboratory testing and/or performing dry runs of a subset of simplified jamming and spoofing scenarios in order to validate and debug the test approach. Under this approach, the parameters of the intentional attack were defined. The implementation methodology of the intentional attacks included spoofing emulated at the receiver radio frequency input, as well as live-sky testing.

Analysis tools were used to evaluate the stand-alone GPS receiver under nominal, environmental-normal scenarios as a baseline. Resiliency to GPS jamming and spoofing threat scenarios was then assessed by comparing performance under these scenarios relative to the nominal environmental baseline. The resilience of the stand-alone GPS receiver as well as that of the integrated PNT sensor suite were assessed. This performance assessment included quantitative metrics such as positioning accuracy and integrity, and velocity/range rate accuracy and integrity. The availability and integrity degradation was assessed under the threat scenarios to levels that can be practically measured or inferred from the collected threat scenario data.

---

[3] U.S. Department of Transportation, John A. Volpe National Transportation Systems Center, *Complementary PNT and GPS Backup Technologies Demonstration Report*, January 2021, https://rosap.ntl.bts.gov/view/dot/55765.
[4] U.S. Department of Homeland Security, DHS S&T Invites Critical Infrastructure Owners and Operators to GPS Spoofing Test Event, New Release, web, April 7, 2020, https://www.dhs.gov/science-and-technology/news/2020/04/07/news-release-st-invites-critical-infrastructure-gps-spoofing-test.
[5] "Live-sky" testing describes a scenario where the RF signals being sent to the GNSS/GPS receiver in the test system are from actual GNSS/GPS navigation satellites overhead at that time.

Because undesired spoofed signals are often stronger than desired GPS signals, an additional goal of the pilot testing was to identify and/or develop a meter or measuring device that can detect the stronger undesired signal of a spoofing attempt. When a spoofed signal is identified, the device would notify the vessel operator that other navigation methods should be used. This system could prevent a vessel from entering hazardous waters, running aground, or straying into foreign waters because of a spoofed GPS signal. Alarm information, and other data outputs available from the protective and complementary PNT technologies considered are discussed later in the report.

1.2.3 Report of Results from USDOT Pilot Program

This internal Federal Government report documents the results from the stakeholder engagement conducted and the results of pilot testing. These results provide insights to support the development of PNT profiles for maritime applications required by EO 13905, and will inform additional PNT research and development. The results and lessons learned from this pilot program will also be transferable to other modes of transportation (aviation, rail, vehicles, and pipeline) to improve their PNT resiliency.

2. NIST Foundational PNT Profile

In addition to development and implementation of a 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, applies the NIST Cybersecurity Framework (CSF) to the PNT ecosystem.[6] 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.[7] 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.

The PNT Profile is voluntary and entirely recommendatory in nature, intended to be a foundational set of guidelines. It does not represent any enforceable regulations, does not define mandatory practices, does not 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 its recommendations will not necessarily protect organizations from all PNT disruption or manipulation. Each organization is encouraged to make their risk management decisions 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 upon 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

[6] "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.

[7] The text in much of Section 2 highlights the rationale behind the adoption of NISTIR 8283, as described by 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 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.

It 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.[8] 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:

[8] "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 NIST.IR.8323 Foundational PNT Profile describes the five Framework Core functions as follows:

1. Identify – 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. Protect – 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. Detect – 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. Respond – 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. Recover – 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 2-1). When considered together, these functions provide a high-level, strategic view of the life cycle of an organization's management of PNT cybersecurity risk.

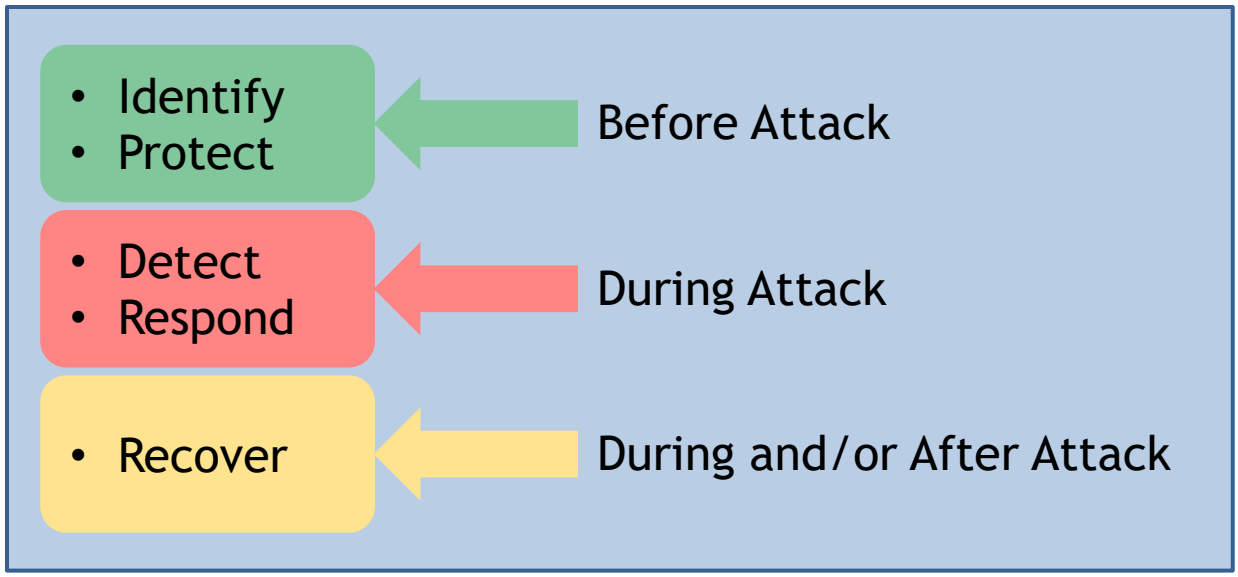


Figure 2-1. Five Functions within the NIST PNT Profile

3. USDOT Pilot Program

In this chapter, section 3.1 describes the activities carried out to identify the relevant PNT vulnerabilities and threats. These activities included operational impact assessment through stakeholder engagement, identifying and characterizing known on-board PNT sources and threat modalities, and characterization of the ship and operational RF environment as it affects the performance of PNT systems. Section 3.2 describes the concept of operations for the protective solution developed by the technical team. Section 3.3 provides details on the configuration of the proposed system, the testing process, and the preliminary analysis and evaluation of test results.

3.1 PNT Vulnerabilities and Threat Identification

Identify is the first function of the PNT Profile, in order to determine the potential threats to the system, whether natural or human-made. The identify function includes:

- Identification of the business or operational environment and organization's purpose;
- Identification of all assets, including applications dependent on PNT data;
- Identification of sources and infrastructure that provide PNT information; and
- Identification of the vulnerabilities, threats, and impacts should the threat be realized in order to assess the risk.

It is also important to understand the GPS signal conditions and RF environment typically encountered during operations—in this case, aboard a ship operating in port and underway at sea—to identify any significant signal reception issues or concerns. Together, this information will help determine the effectiveness of jamming and spoofing detection techniques, and the viability of new GPS or complementary PNT equipment/technologies.

3.1.1 Operational Impact Assessment through Stakeholder Engagement

The technical team worked the identify function along three facets of the maritime enterprise. The first was outreach to commercial vessel operators, regulators, and enforcement organizations, technology providers, PNT experts, and policy agencies. The second facet was through interviews and personal interactions with ship's crews, vessel management services, and equipment vendors from the MARAD fleet. The third facet was the collection of pertinent data, including from aboard an operational ship.

3.1.1.1 Outreach and Data Gathering of PNT Impacts on Maritime Operations

In December 2020, USDOT hosted a daylong workshop, "GPS Jamming and Spoofing in the Maritime Environment," which featured speakers from government, industry, and non-profit PNT organizations.[9] The workshop was open to the public and provided an opportunity to gather a wide range of

[9] "Virtual Workshop on GPS Jamming and Spoofing in the Maritime Environment, Agenda and Presentation," U.S. Department of Transportation, last updated December 9, 2020, https://www.transportation.gov/pnt/agenda-virtual-workshop-gps-jamming-and-spoofing-maritime-environment.

perspectives on the potential impacts of GPS disruptions. The technical team also evaluated several pertinent reports and internal U.S. Navy and Department of Defense directives.[10]

Specific operational impacts were presented, some in the form of first-hand experience from major shipping operator captains, interference report agencies such as the U.S. Coast Guard Navigation Center, GPS jamming and spoofing scenarios aimed at shipping operations described by Non-Governmental Organization (NGO) leaders, and the fundamentals of PNT vulnerabilities by technical experts from Government and academia. Highlights from the workshop minutes are included as Appendix A to this report and provide a detailed description of the presentations given by the speakers and respective question and answer sessions. One clear message surface from the workshop: GPS jamming and spoofing are very real and unless mitigations are developed, the economic and safety impacts will only escalate. Further discussion in Section 3.1.3.1 is given on equipage and real-world experiences of spoofing events while under operation as well as scenarios under which future impacts are possible and even probable.

3.1.1.2 Crew, Ship Management Services, and Operating Administration Interviews

In parallel with stakeholder outreach and commercial vessel operator engagement, the technical team conducted a series of ship tours and surveys, interview sessions with the RRF ship management services and equipment vendors, and review sessions with MARAD personnel. This information gathering and discovery process aided the "identify" function by connecting the operational experiences shared in the public workshop to specific shipboard roles, responsibilities, procedures, and equipage. Scenarios were discussed and visual inspection of the bridge management procedures, equipage, crew actions, and in-port services such as maintenance, data services, and equipage plans.

3.1.1.3 Shipboard Technical Data Collection and Technology Vulnerability Impacts

Following the information gathering process, the Project Team coordinated three technical data collection efforts to address detailed identification of vulnerabilities, assess threats, and consider complementary and backup services for GPS that could serve as mitigations to operational impacts. Subsequent sections of the report expand on the technical aspects of the three areas.

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. Extension of Complementary PNT Demonstration evaluations to low Earth orbit (LEO) PNT services.

3.1.1.4 Review of GPS Interference User Reporting Data

The National Security Council created the interagency Purposeful Interference Response Team (PIRT) in 2008 with four mission domains to collect, analyze and respond to incidents of interference affecting

[10] See section 5, References.

space system and services.[11] GNSS suspected purposeful interference is one of the four mission domains, with code name CRUCIBLE that focuses on GPS anomalies and interference that users report of any kind affecting U.S. Government civil space systems and leased commercial space supported services, capabilities, or interests. USDOT records, analyzes, and coordinates investigation efforts if warranted—as in the case of purposeful interference—that are forwarded on to the PIRT member enforcement organizations. The CRUCIBLE unclassified reports include information that is useful for characterizing operational impacts to help assess potential consequence to maritime operations. Specifically, the reports contain:

1. Reporting entity.
2. Location, time, and duration of the interference event.
3. Equipment description, e.g., platform, receiver type, additional PNT units, etc.
4. Operating environment, e.g., stationary/moving, urban/rural, maritime/surface/rail/aeronautical, etc.
5. User initial impact assessments of their Space-Based GNSS operations.

DOT processed unclassified reports collected from interagency CRUCIBLE members in different critical infrastructure global sectors and derives its own data subset for focused transportation related events. An initial review of recent entries in the USDOT CRUCIBLE unclassified data subset provided confirmation that significant and useful information is available for the maritime environment. Entries pertinent to maritime operations provided a cross-section of locations, GPS equipage, vessel descriptions, and in some cases operation types.

3.1.2 On-board PNT Systems

GPS equipment installed on the RRF vessels was inventoried by the technical team with assistance from MARAD personnel. Equipment from this list was selected as being representative of devices in common use in maritime applications, and later used to support jamming and spoofing susceptibility testing. This testing assisted in creating recommendations for possible technology solutions that provide mitigation against and/or alerts of GPS threats. In addition, the equipment inventory sought to identify other

[11] The Purposeful Interference Response Team (PIRT) was charted by the National Security Council (NSC) in 2008. The U.S. Strategic Command (USSTRATCOM) chaired the PIRT until 2018, as the U.S. Government lead for space operations and the operators of the primary U.S. Government 24-hour operations center for space situational awareness. The organization has since transitioned to U. S. Space Command (USSPACECOM) leadership. The PIRT is an interagency coordination group with core and conditional members (Department of Defense, Department of State, Department of Commerce, Department of Homeland Security, Department of Transportation, the Director of National Intelligence, and the Federal Communications Commission as core and several conditional member organizations) designed to bring together experts from across the U.S. Government to evaluate reports of suspected purposeful interference that impacts U.S. Government space systems, commercial and foreign systems providing services to the U.S. Government, and other U.S. commercial and allied space systems and services of interest to the U.S. Government. PIRT serves as an investigative and coordinating body to ensure all relevant U.S. Government agencies have access to the same information and key analytical documents to develop resolution and response options, and formalizes and facilitates existing processes and relationships. The PIRT maintains the classified CRUCIBLE data archive.

shipboard equipment and systems, especially those that radiate RF energy. That information will help characterize the general RF environment and support system integration.

Table 2 lists the eight combinations of GPS receivers found installed on the MARAD RRF fleet of 38 vessels. The two GPS receivers of interest in this table are the Furuno GP150 and Furuno GP170, which together represent 97 percent of all GPS receivers installed across the RRF fleet.[12] [13] The GP170 was identified as a widely used GPS receiver for maritime applications and selected as the test device.

Table 2. List of MARAD RRF Common GPS Equipment

Equipment Combination	Number of RRF Ships with Given Equipment Combination	Number of Furuno GP170 GPS Units Installed	Number of Furuno GP150 GPS Units Installed	Number of Other GPS Units Installed	Total Number of GPS Units for each Given Combination
A	5	0	2	0	10
B	1	1	0	0	1
C	3	1	1	0	6
D	2	1	2	0	6
E	16	2	0	3	35
F	6	2	1	0	18
G	1	2	2	0	4
H	4	3	0	0	12
Fleet Total	**38**	**64**	**25**	**3**	**92**

(Source: MARAD)

MARAD arranged for the technical team to tour and survey an *Algol*-class Fast Sealift Ship, the SS *Denebola*, while the ship was in Boston, MA for maintenance. Originally built in the early 1970s as high-speed commercial container ships, the eight *Algol*-class ships were acquired by the U.S. Navy by 1982, and converted to transport military vehicles and other materiel. A second *Algol*-class vessel, the SS *Antares*, homeported in Baltimore, MD, was selected for data collection, since the ship would be underway at-sea for a Turbo Activation (TA) event on August 28, 2021–September 2, 2021. A TA exercise is an annual series of no-notice activations of vessel in the U.S. Transportation Command (USTRANSCOM) Organic Surge Fleet, which is comprised of ships from the Military Sealift Command (MSC) Surge Fleet and the MARAD RRF. The TA allowed the study team to measure RF signals aboard an active vessel engaged in underway operations.

[12] Three ships were equipped with two Furuno GP170 units, and had either a JLR-7700 MK II or Simrad MX512 also installed; these three units represent the remaining 3 percent of all GPS receivers installed.

[13] The technical team did not test devices that are no longer commercially available as part of the Pilot Project. It was found that neither the Furuno GP150 (the predecessor model to the Furuno GP170) nor the Simrad MX512 is commercially available. The JLR-7700 MK II that uses the discontinued differential GPS (DGPS) service.

SS *Denebola* Pier side Inspection

On March 24, 2021, study team visited the SS *Denebola.* This allowed the study team to inspect the GPS equipment, its installation and configuration on the bridge, the location of antennas, and the identification of other RF devices installed aboard the vessel. It also allowed the study team to confer with the vessel operators.

SS *Antares* Underway Exercise and Data Gathering

From August 28 to September 2, 2021, the SS *Antares* participated in a Turbo Activation, which included an emissions control (EMCON) exercise to identify RF signals detectable on the flying bridge. One member of the Pilot Project technical team accompanied the vessel on the six-day voyage to collect baseline data and conduct scenario testing.

3.1.2.1 Current PNT System Configuration

The data-gathering effort determined that MARAD RRF ships typically have two or three GPS units installed—commonly the Furuno GP170 or Furuno GP150—with a few exceptions. The GPS unit supplies PNT information to the vessel's electronic chart display and information system (ECDIS), which also relies on other GPS units as redundant PNT sources. This system design represents a vulnerability to the RRF vessels by being reliant on GPS alone for PNT data.

3.1.2.2 Downstream System Dependencies on PNT Information

The safe and efficient vessel operation in a maritime environment depends on accurate high-integrity PNT information. PNT information derived from a GPS receiver or other sources are utilized by several downstream situational awareness and safety-critical systems. MARAD RRF critical systems with PNT dependencies include automatic identification systems (AIS), electronic chart display and information systems, emergency positioning indicating radio beacons (EPIRBs), and Global Maritime Distress and Safety Systems (GMDSS).[14] Since the vessel's position is broadcasted and shared with other nearby vessels and shoreside networks, a disruption of the PNT source will not only affect the vessel's own systems but also can present safety and operational risks to other vessels operating in the same geographical region. Such risk motivates the need to explore approaches to enhance the PNT source resiliency so that PNT information passed down to on-board systems and/or broadcast to other vessels and shoreside networks is trustworthy, even when GPS signal disturbances are present (for the case of GPS PNT sources).

3.1.3 Threat Modalities

Threats to PNT systems come from both natural and human-made causes. Not all human-made threats are intentional, as sometimes there are unintended consequences of other legitimate operations. No matter the origin of the threat, PNT systems need to be protected to ensure accurate PNT information.

[14] John A. Volpe National Transportation System Center, "GPS Dependencies in Transportation: An Inventory of Global Positioning System Dependencies in the Transportation Sector, Best Practices for Improved Robustness of GPS Devices, and Potential Alternative Solutions for Positioning, Navigation and Timing," Washington, DC, August 31, 2016, https://rosap.ntl.bts.gov/view/dot/12386

3.1.3.1 Intentional Threats: GPS Anomalies

Accurate and reliable PNT capabilities are essential for the safety for all modes of transportation and will become increasingly important for autonomous vessels in maritime transportation. The primary and most recognizable PNT service supporting critical infrastructure is GPS. However, because GPS relies on signals broadcast from a satellite constellation in medium Earth orbit, its signals are low power at the receiver and thus vulnerable to unintentional disruption and intentional interference such as jamming and spoofing. In 2001, the Volpe Center conducted a vulnerability assessment of transportation infrastructure relying on GPS, and found that as GPS further penetrates into the civil critical infrastructure, it could become a tempting target for exploit by individuals, groups, or countries hostile to the United States.[15]

Jamming has long been a recognized threat to GPS due to the low-level signal at the GPS receiver. North Atlantic Treaty Organization (NATO) military drills in the Baltic Sea in 2019, with 40,000 troops and 29 Nations participating, experienced GPS jamming.[16] Spoofing was considered an unrealistic threat for many years because it was complicated to perform. However, new low-cost software defined radio (SDR) devices and high-profile demonstrations at the University of Texas that spoofed a drone (in 2012) and a sophisticated yacht (in 2013) brought spoofing into the public eye.[17] DHS defines spoofing as:[18]

> *Spoofing is caused by 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 GPS 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 digital data to the target receiver for its use in 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 or delayed and it is possible for effects to continue even after the spoofing has ended.*

[15] John A. Volpe National Transportation Systems Center, "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," Washington, DC, April 29, 2001, https://rosap.ntl.bts.gov/view/dot/8435

[16] "Norway proves Russian interference," GPS World, March 20, 2019, https://www.gpsworld.com/norway-proves-russian-interference/.

[17] Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys, "Drone Hack," *GPS World*, August 2012, pp. 30–33, https://radionavlab.ae.utexas.edu/images/stories/files/papers/drone_hack_shepard.pdf. Also, Jahshan Bhatti and Todd E. Humphreys, "Hostile Control of Ships via False GPS Signals: Demonstration and Detection," *NAVIGATION*, 64:1, pp. 51–66, https://doi.org/10.1002/navi.183.

[18] Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure, p. 4.

Another likely GPS spoofing attack occurred in the Black Sea in 2017, where over 20 ships reported their GPS position at an inland airport.[19] The number of separate vessels that reported the same false position and the characteristic jumping between the false and true position of the ships is strong evidence of a large-scale spoofing attack. More recently, incidents of GPS spoofing have been occurring around the world, particularly in maritime environments.[20]

The USDOT Workshop on GPS Jamming and Spoofing in the Maritime Environment brought first-hand testimony from major shipping operators, including APL Maritime Ltd. (Rockville, MD) and Maersk Line Limited (Norfolk, VA). Captain William Westrem, master of APL Maritime's *President Eisenhower*, recounted three experiences around the globe, supported with bridge-control video of the ECDIS and supporting navigation equipment, which showed the GPS signal being manipulated (e.g., a docked vessel where the ECDIS and supporting navigation equipment reported non-zero velocity and movement on the chart). Under nominal visibility conditions, this threat or impact is easily identified and mitigated. However, if underway or in low- or zero- visibility conditions, such an impact represents both an operational and a safety threat.

Additional comments were given at the workshop by Captain Richard G. Hoey, master of the *Maersk Montana*, who recounted a specific experience in the Suez Canal where the vessel was in the southbound (travelling) lane, but the navigation equipment reported and guided the vessel toward the center of the channel, into the buoy/divide lane separating southbound traffic from northbound traffic. Had human intervention (based on visual observations) not been taken, the conditions for a collision were imminent. Mr. Dana Goward, President of the Resilient PNT Foundation, further outlined scenarios based on GNSS jamming and spoofing principles combined with malicious intent on shipping operations that can easily lead to economic and safety impacts of significant scale.

Reports from civilian users experiencing GPS anomalies such as service degradations, disruptions, jamming, spoofing, or other incidents are reported to either of the following civil agency operations centers:

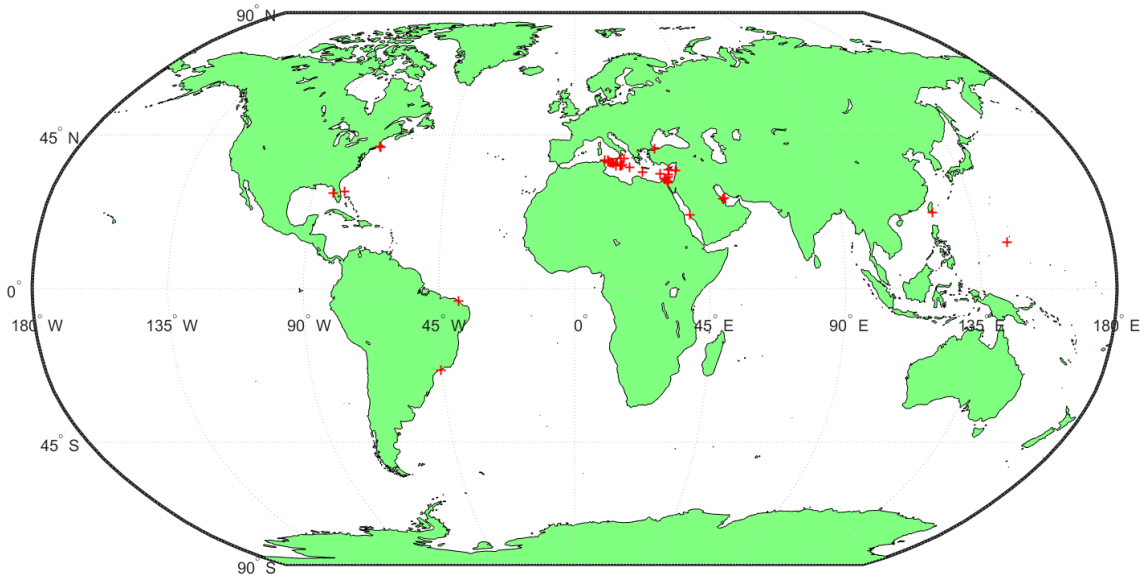
- **Aviation Users:** Federal Aviation Administration (FAA) Wide Area Augmentation System (WAAS) (https://www.faa.gov/air_traffic/nas/gps_reports/)
- **Non-Aviation Users**: United States Coast Guard (USCG) Navigation Center (NAVCEN) (https://www.navcen.uscg.gov/?pageName=gpsUserInput)

During the period of January 1, 2021 through December 31, 2021, 56 maritime GPS anomalies were recorded in the USDOT CRUCIBLE data subset. A compilation of pertinent data and known characteristics of the anomalies, including approximate location (latitude, longitude) is provided in Appendix B:

[19] "GPS Spoofing Patterns Discovered," Resilient Navigation and Timing Foundation, September 15, 2017, https://rntfnd.org/wp-content/uploads/GPS-Spoofing-Patterns-Press-Release.1-26-Sep-17-RNT-Foundation.pdf.
[20] "MSCI Advisory 2022-005, Various-GPS Interference and AIS Spoofing," MARAD Maritime Security Communications with Industry portal, March 14, 2022, https://www.maritime.dot.gov/msci/2022-005-various-gps-interference-ais-spoofing.

Maritime GPS Anomalies Collected by the U.S. Department of Transportation Spectrum Monitoring Operations Center in 2021. (Note: latitude and longitude are approximate estimations and, in some cases, updated based on the narrative from the user of where the incident was initially experienced.)

Since GPS anomalies are reported by users who typically do not have the resources to identify the cause of the anomaly, it is not possible to determine how many of the events listed were attributed to intentional jamming or spoofing attacks. Regardless, these GPS disruptions are happening across the globe (see Figure 3-1), and the actual number of disruptions is likely much higher. In 50 percent of the user reports filed, the reporting source indicated many other vessels experienced the same issues; however, discrete submission by those other impacted vessels were not formally received or filed. This indicates a possible 50 percent of user reports not filed during active incidents. Therefore, automated methods for detecting jamming or spoofing events during maritime operations are critical so that other modes of navigation such as complementary PNT (CPNT) technologies can be enabled to ensure PNT resiliency.



(Source: Volpe Center)

Figure 3-1. World Map of Reported GPS Anomalies (January 1, 2021 through December 31, 2021)

3.1.3.2 Environmental and RF Interference

Unintentional environmental factors can also affect the performance of on-board PNT sources as well as complementary technologies under consideration. In particular, GPS and other RF-based PNT systems can suffer from signal degradation due to interference from other devices aboard ship and from other RF transmissions in the vessel's operational environment, especially if such transmissions generate integer harmonics in the passband of the L1 reception band. GPS-based PNT solutions can also be significantly degraded due to satellite signal blockages, or multipath effects caused by objects and structures aboard or around the ship. In order to understand and quantify the impact on current PNT systems and assess the effectiveness of protective and complementary technologies, a detailed

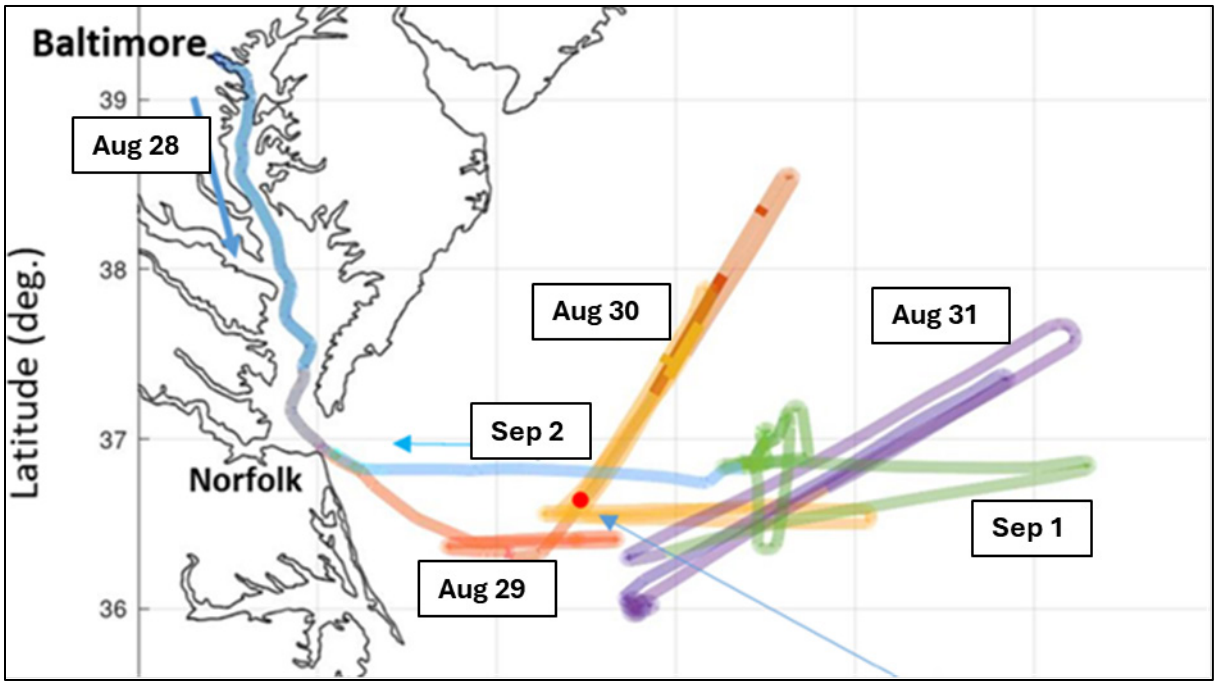
assessment of the RF environment was performed while the vessel was engaged in underway operations.

3.1.4 Operational Environment Characterization

To identify the threats to the PNT systems, the RF environment aboard an operating RRF vessel was analyzed to characterize the existing frequency ecosystem. During the period August 28–September 2, 2021, a member of the study team embarked aboard the SS *Antares* during a TA event that involved 18 ships (17 MARAD RRF ships and 1 MSC vessel). The *Antares* crew conducted a number of required demonstration activities in port, followed by several specific maneuvers at sea including:

- A sustained speed run,
- A fuel economy run,
- A simulated underwater mine avoidance run,
- Cruising in formation, and
- An RF emissions control (EMCON) exercise.

A plot of the ship's course during the six-day exercise is shown in Figure 3-2. The colors identify the calendar dates based on UTC time (offset by four hours from local time). The ship was out of range of shore-based cell towers from some time on August 29 until approaching Norfolk on September 2. The red dot indicates the location on Monday, August 30, where the RF EMCON test was performed.



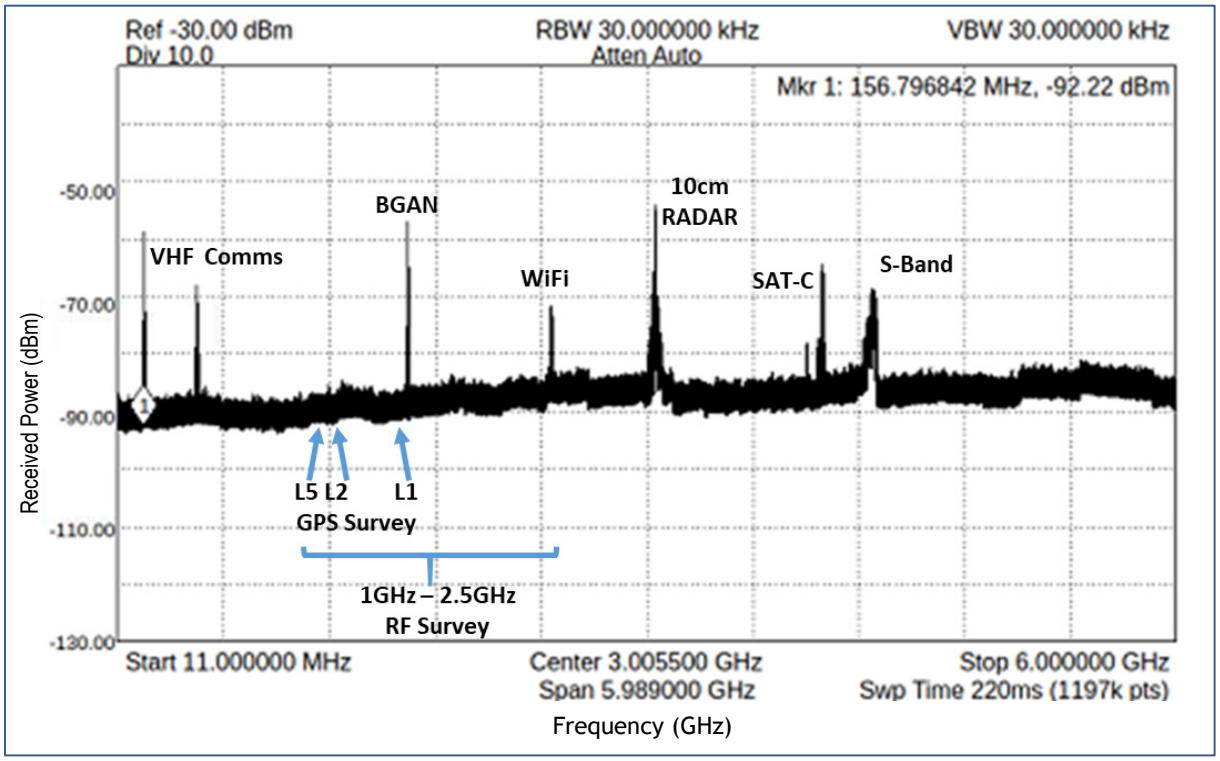
(Source: Volpe Center/Zeta Associates)

Figure 3-2. SS *Antares* Track during Turbo Activation Exercise

The RF EMCON test was originally intended to be a non-instrumented exercise to familiarize the crew with U.S. Navy EMCON concerns and protocols. The presence of an on-board RF collection system

(detailed in the next section) provided a more informed experience for the crew, and an opportunity to monitor the RF spectrum while individual transmitters on the ship were turned on and off. Figure 3-3 is a summary of the EMCON test, showing a single spectral display with frequency/system associations while all transmitters were turned on. The arrows indicating L5, L2, and L1 identify the location of GPS signal frequency bands. Notice also the high-power Broad Global Area Network (BGAN) transmission, which operates in a frequency band close to the L1 signal.[21] This could be is of significant concern, since GPS signals are extremely low in power, making them highly vulnerable to being overpowered by interference from stronger RF signals, particularly those operating in nearby frequency bands.

In a marine setting, awareness of the RF environment when onboard systems transmit is particularly important due to the high corrosion exposure of metal joints found in a ship's structure. Dissimilar metal joints can create a diode that generates unwanted signals when excited with high-energy RF transmissions. This is known as the "rusty-bolt" effect or "passive intermodulation." If the wavelength of the created diode is that of the L1 frequency, an unwanted signal will generate every time the high power shipboard transmission occurs.



(Source: Volpe Center/Zeta Associates)

Figure 3-3. RF EMCON Spectral Capture with all Systems Turned ON

[21] BGAN operates in the L-Band (1.0–2.0 GHz). Equipment uses receiving (Rx) frequencies of 1525.0–1559.0 MHz and transmitting (Tx) frequencies of 1626.5–1660.5 MHz. The GPS L1 frequency 1575.42 MHz. (For further information see, Dimov Stojce Ilcev, "Introduction to Inmarsat broadband global area network for mobile backbone networks," Bulletin of Electrical Engineering and Informatics, 9:2, April 2020, pp. 843–852, https://doi.org/10.11591/eei.v9i2.2136.)

3.1.4.1 Objective

GNSS measurement and positioning performance were evaluated from data collected on the *Antares* during the six-day TA exercise. The technical team performed a radio frequency (RF) and GPS measurement survey to characterize emissions and GPS performance in a typical maritime operational environment. The purpose of this evaluation was to provide insight on typical GPS performance in the maritime environment, to support recommendations being developed to improve maritime PNT resiliency.

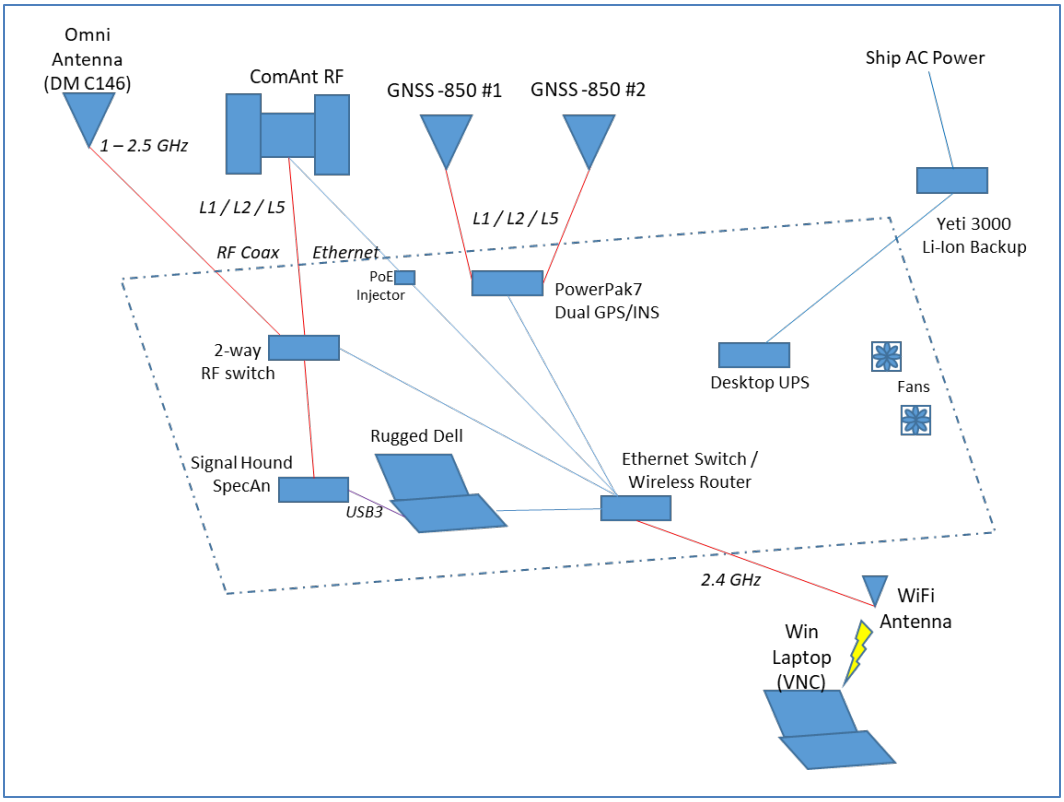
A survey system was installed on the *Antares* to capture RF spectrum transmissions in and near the GPS bands (L1, L2, and L5) and to collect GPS measurement data. The GPS spectral data was inspected to determine emitters close to the GPS band, while the wider-band spectral data revealed potential RF spectrum conflicts with PNT technologies and other existing systems. The GPS collection enabled characterization of the ship's multipath conditions and provided data useful for investigating shipboard GPS interference.

3.1.4.2 Test Setup and Data Collection

The survey system was comprised of equipment to capture RF spectrum in and near the GPS bands (L1, L2, and L5) and to collect GPS measurement data. The main items for the survey system were:

- RF and digital electronics for sweeping GPS frequency bands,
- RF switches routing signals from many antennas,
- A dual GPS receiver (multi-frequency, multi-constellation GNSS receiver) with an internal inertial measurement unit (IMU), and
- Laptop computers for control and data collection under software control.

The components of the survey system are depicted in Figure 3-4. All equipment was located on the ship's flying bridge (uppermost deck, above the wheelhouse) with the exception of the monitor laptop, which was located in an office behind the bridge. The dashed line indicates devices that were enclosed together in a single water-resistant equipment chest on the flying bridge.



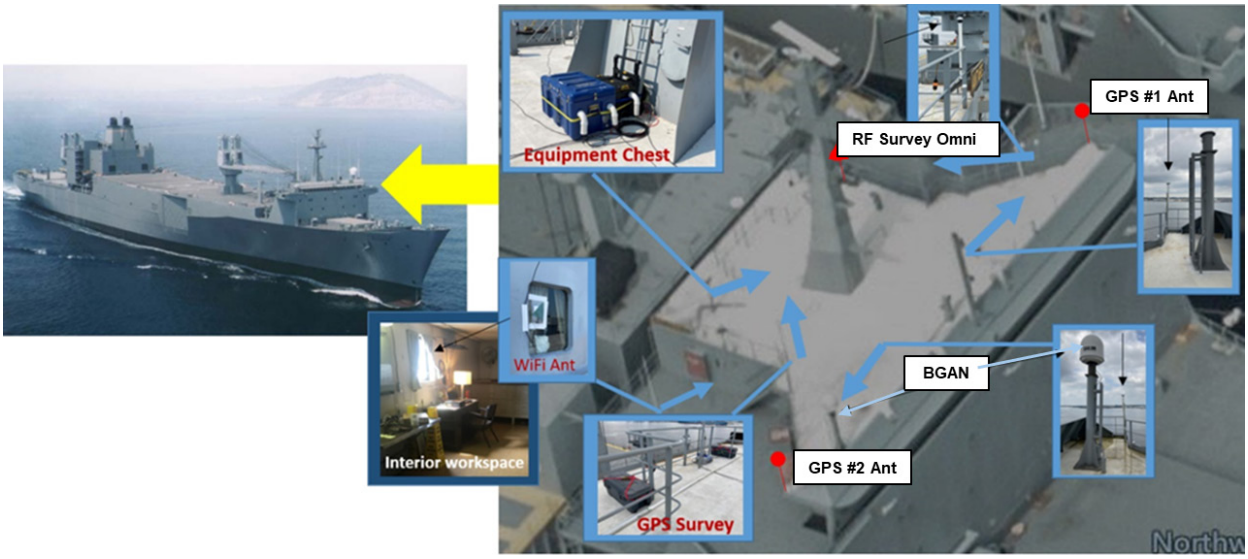
(Source: Volpe Center/Zeta Associates)

Figure 3-4. Survey System Schematic

A Signal Hound Spectrum Analyzer was nominally configured to process RF frequencies spanning from 1.0–2.5 GHz from a single omnidirectional antenna, and RF within the GPS L1, L2, and L5 frequency bands from six directional antennas and a second omnidirectional antenna. The RF for the wider span collection (the "Wide-Span Survey") used a simple passive antenna, while the RF collection for GPS L1, L2, and L5 (the "GPS-Band Survey") was filtered to the bands of interest and amplified. The spectrum analyzer sourced RF from these antennas sequentially via RF switches.

The GNSS data collection was conducted with a dual-antenna NovAtel PwrPak7D-E2 (PwrPak7). The PwrPak7 was integrated with an Epson G370N inertial measurement unit (IMU) and used two NovAtel GNSS-850 antennas mounted at the very ends of the flying bridge (Antenna 1 on the port side and Antenna 2 on the starboard side). The PwrPak7 is configured to receive and process signals from multiple GNSS constellations (including GPS, Galileo, GLONASS, BeiDou, and SBAS signals), and utilizes a TerraStar-C PRO Precise Point Positioning (PPP) service subscription. The PwrPak7 receiver and the two antennas are survey-grade devices that are relatively wideband, which benefits multipath mitigation and positioning accuracy, but makes the system more susceptible to RF interference. The receiver was configured to provide pseudorange measurements that are minimally smoothed by carrier range since this provides more insight into code tracking errors.

The *Antares* is a large cargo ship measuring 946 feet in length, with a beam of 105 feet. Figure 3-5 depicts the locations of the survey system components installed on the *Antares* flying bridge. The two GPS antennas (red dots) were located at the port and starboard extremes of the flying bridge to maximize their baseline separation. The omnidirectional antenna for the wide-span survey passive RF collection was attached to the rear railing and is shown by the red triangle.



(Source: Volpe Center/Zeta Associates)

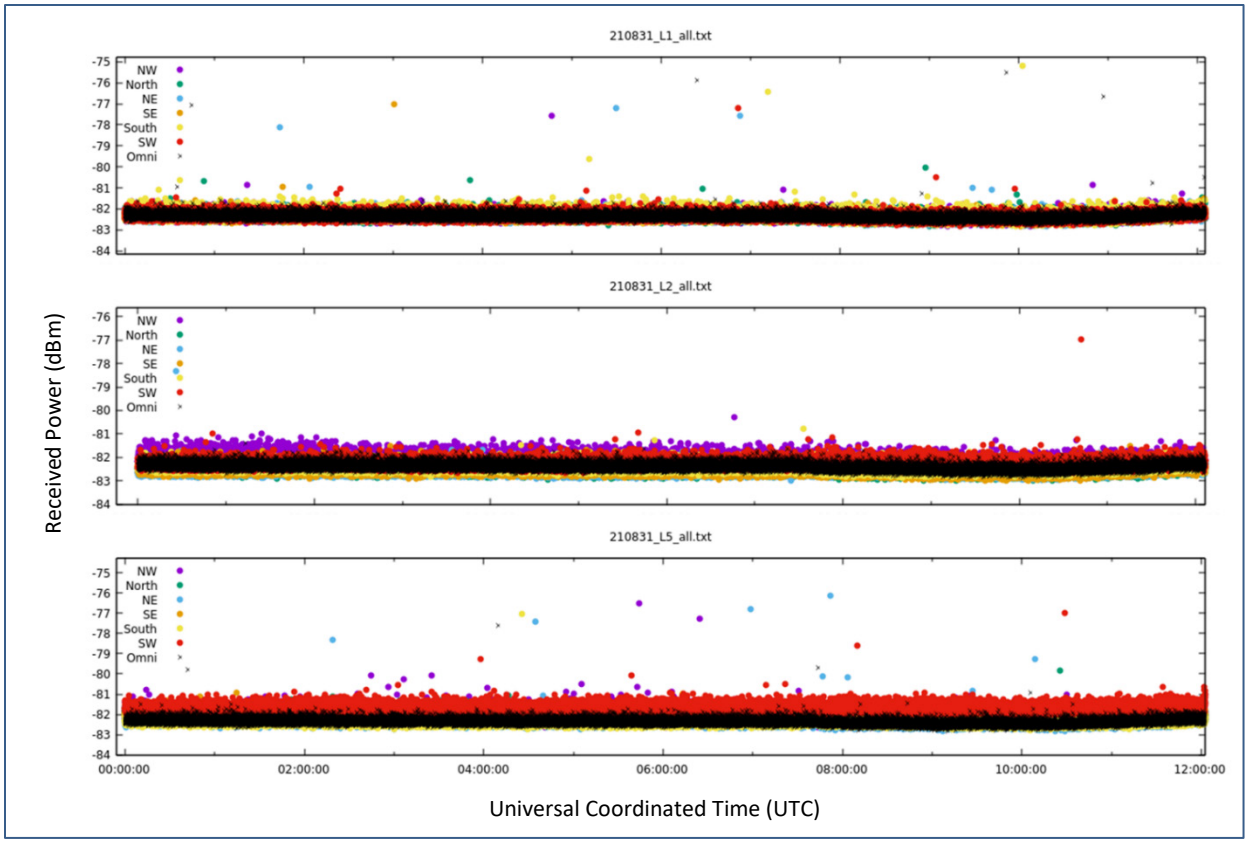
Figure 3-5. Equipment Setup on the SS *Antares*

Three boxes for the omni- and directional antennas were secured along the rear railing. These boxes are shown in an inset in the lower left; the two larger boxes contain three directional antennas to provide six-sector antenna coverage of the L1, L2, and L5 GPS bands. The smaller box has one omnidirectional antenna mounted on top, and the high-speed RF switch and the L1, L2, and L5 filter/amplifier mounted inside. There is a high-powered BGAN transmitter for use by the ship, located near GPS Antenna #2. The passive omnidirectional antenna was located so the main radar mast blocks most of the signal received from the BGAN transmitter, to mitigate the potential of it overdriving the spectrum analyzer.

3.1.5 Analysis and Results

3.1.5.1 GPS-Band Survey

The GPS-Band Survey collected measurements of signal strength drawn from 22 MHz spectrum-analyzer sweeps of each GPS band, with sweeps repeated as the RF source was switched through a sequence of antennas oriented for directional information. The peak sample from each sweep is taken as the measure of instantaneous signal strength for the particular combination of GPS band and antenna direction. Representative examples of directional data for the GPS L1, L2, and L5 frequencies, measured when the *Antares* was sailing in the open ocean, are provided in Figure 3-6.



(Source: Volpe Center/Zeta Associates)

Figure 3-6. GPS L1, L2, and L5 Directional Data from August 31, 2021

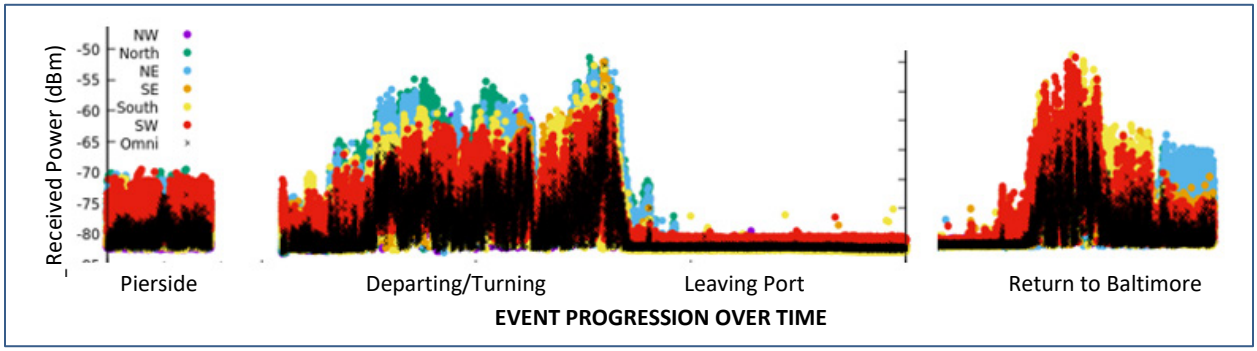
The three plots in Figure 3-6 are examples when no or negligible interference was present over a 12-hour period, at sea and far from shore. The legend on the upper left equates each colored dot (data point) with antenna direction. Each measurement interval records data from six directional antennas (covering 360 degrees in azimuth), as well as from a GPS omnidirectional antenna pointed toward the sky (with data points indicated by a black '+'). The vertical axis is signal strength taken from the peak value in the spectral sweep, so a data point above the noise floor indicates that RF power was received from a given direction and at a given power level. There is a set of seven data points, taken approximately every 1.7 seconds, for each of the L1, L2, and L5 bands. Single outlier data points represent either a very brief received burst of energy or a random burst of noise energy.

It should be noted that the RF supporting these plots was filtered for L1, L2, and L5 using 34 MHz passbands. This filtering would be considered very robust for mitigating any unwanted emissions adjacent to GPS frequencies. The conditioned RF from this filtering is also amplified with nearly 50 dB of gain. Because of this high gain, the brief noise bursts that appear in these plots may not be seen in the Wide-Span Survey waterfall plots, since those were collected by a passive (non-amplified) antenna.

The GPS L1 band-sweeps throughout the entire six days on the *Antares* were similar to the L1 plot shown in Figure 3-6. This indicates that there was no significant GPS L1 band interference detected. The

GPS L2 band was similarly quiet; however, during the first few days of collection there was a persistent low-level interference source present. This turned out to be self-interference from a device in the equipment chest that was subsequently mitigated by moving the chest a few inches away from the GPS-Band Survey antennas.

In contrast, the GPS L5 band was not as quiet as L1 and L2. While L5 coexists with ground-based aircraft transmitters used for civilian distance measuring equipment (DME) and military Tactical Air Navigation (TACAN) systems, interference from unknown sources was detected both from shore transmitters and while the *Antares* was far offshore. During departure and return near Baltimore, L5 interference was observed as shown in Figure 3-7.



(Source: Volpe Center/Zeta Associates)

Figure 3-7. L5 Directional Data and Baltimore Harbor

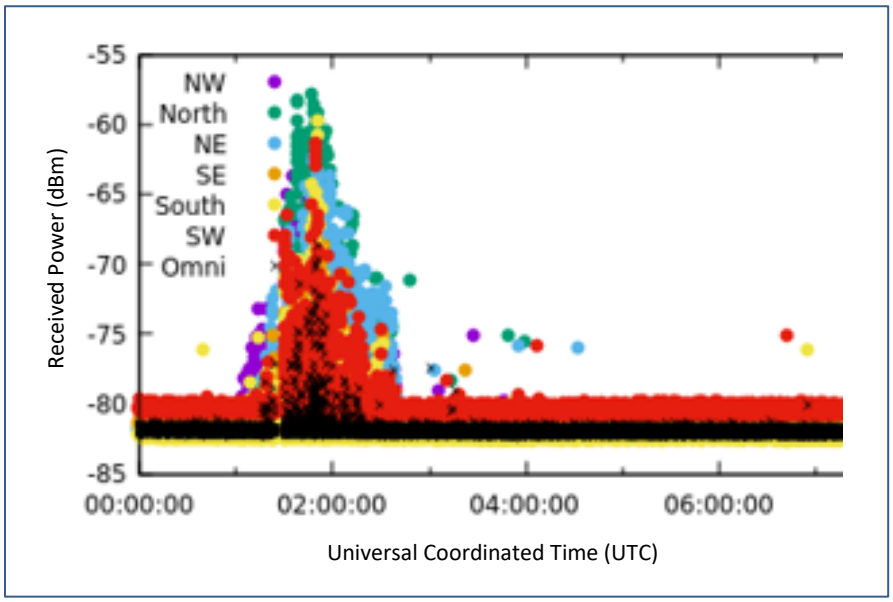
A large cluster of dots—especially dots of the same color—indicates persistent interference present coming from the same direction. The color of the strongest peaks indicates the relative direction of the interfering signal. The GPS-Band Survey antennas were oriented such that green (north) was pointed directly toward the ship's starboard side and yellow (south) was toward the port side.

The left plot of Figure 3-7 shows readings taken while the vessel was alongside Pier 8. The middle plot was taken while departing Baltimore and shows data collection while the ship was alongside the pier, pulling away from the dock, turning to perform a lifeboat exercise, and then departing to the east-southeast. The peak colors can be seen to change between blue and green as the ship turned, leaving the pier. The interference signal was on the starboard side of the *Antares* and may have been blocked from view as the ship moved, causing the peak amplitude to drop down and rise again, twice. Once the *Antares* left Baltimore, the signal faded out entirely.

The plot on the right reflects the L5 directional data when the *Antares* returned to Baltimore. This shows data collection while the ship passed Pier 8 on its left and then backed in for docking. The signals were first coming from the port side (red and yellow) and then shifted to the starboard side (blue). Reviewing the path of the *Antares* versus time and comparing the signal direction provided an estimate of the interference source location to be somewhere between Pier 8 and Fort McHenry. The system causing this L5 interference in Baltimore Harbor was not determined, but the high density of collection points

indicates the interference signal was persistent and perhaps continuously radiating, although with varying amplitude over time.

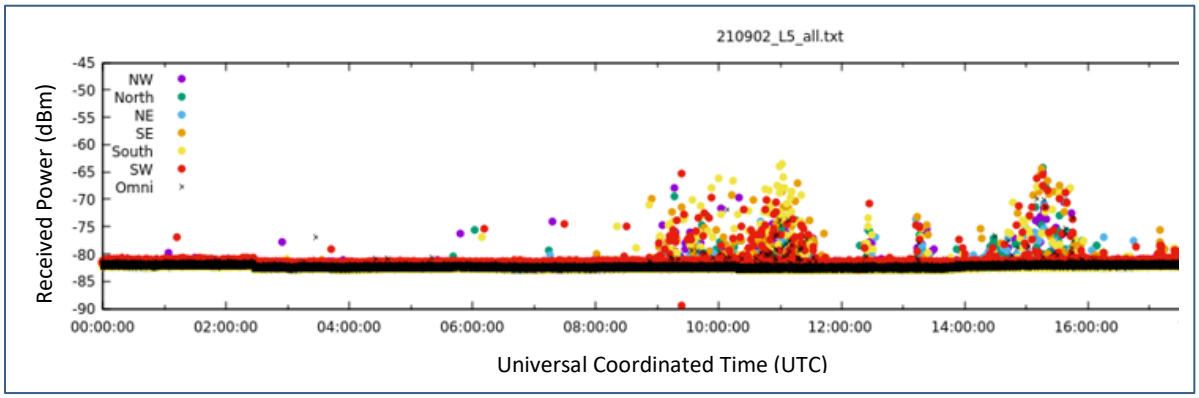
L5 interference was also observed near Norfolk, VA for both departure and return and while the *Antares* was at sea. Figure 3-8 shows L5 directional data as the ship passed Norfolk, at the mouth of Chesapeake Bay and headed to sea, where the interference tracked along the starboard side of the *Antares*, in the direction of Norfolk at approximately 10:00 p.m. local time.



(Source: Volpe Center/Zeta Associates)

Figure 3-8. L5 Directional Data on Departure from Norfolk, VA

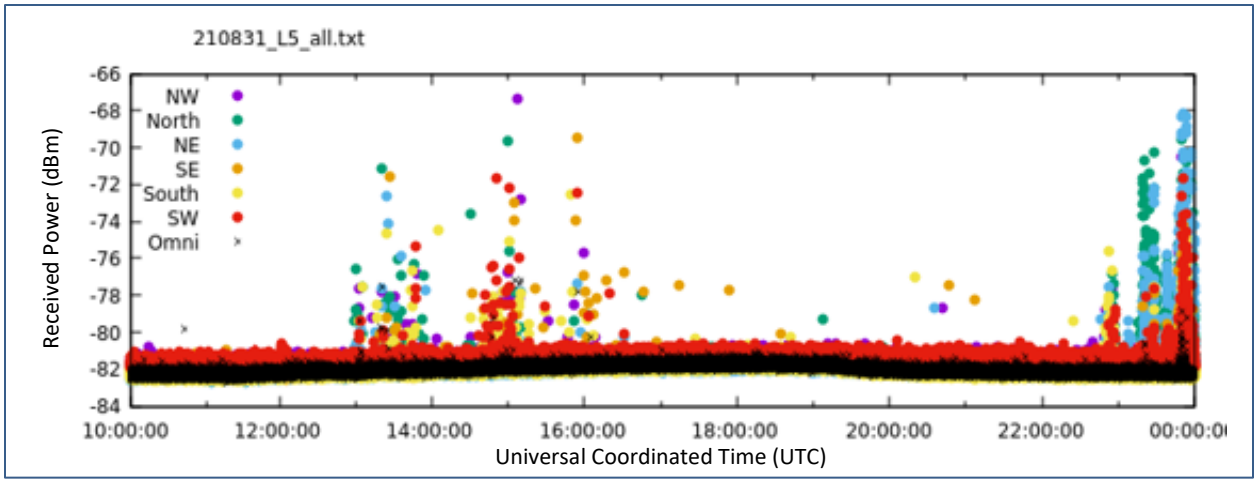
L5 interference observed on the return passing also seemed to be emanating from Norfolk but seemed less persistent than on departure (see Figure 3-9).



(Source: Volpe Center/Zeta Associates)

Figure 3-9. L5 Directional Data on Return to Norfolk, VA

The L5 interference observed at sea also seemed less persistent than at either Baltimore or on departure when passing Norfolk (see Figure 3-10).



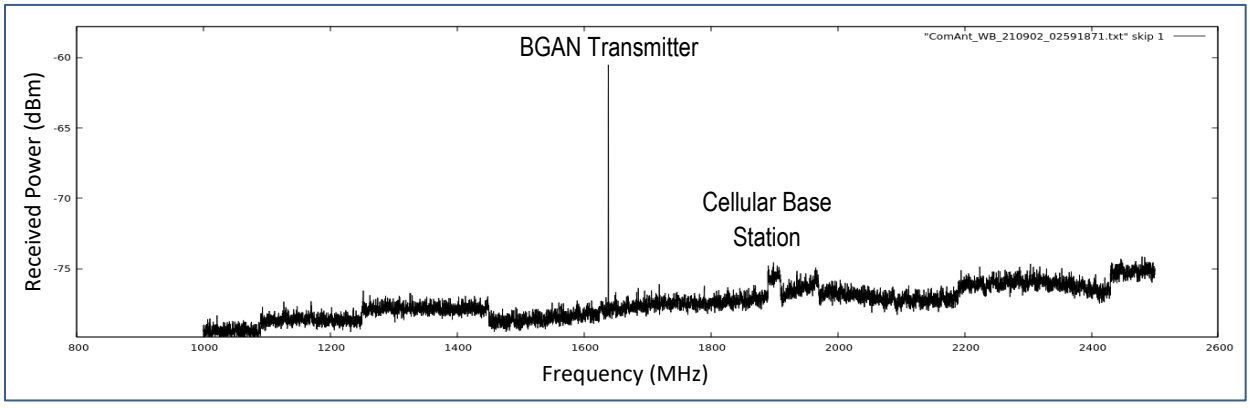
(Source: Volpe Center/Zeta Associates)

Figure 3-10. L5 Directional Data while at sea on August 31, 2021

Ultimately, the source(s) and location(s) of the L5 interference could not be conclusively determined and may have been from shore, on the *Antares*, or from another vessel. The L5 interference observed in Baltimore Harbor and near Norfolk could be further investigated, to gain an understanding of its location and source. This could be accomplished from shore using the Volpe Center's instrumented van.

3.1.5.2 Wide-Span Survey Results

The Wide-Span Survey collected traditional spectrum analyzer sweeps over the 1.0 GHz–2.5 GHz band using the passive omnidirectional antenna. A sample of one such sweep is shown in Figure 3-11. The strong peak at about 1650 MHz is a BGAN transmission. A cellular base station signal can also be seen rising above the noise floor at around 1900 MHz. (The varying noise floor across frequency is an artifact of the analyzer used.)

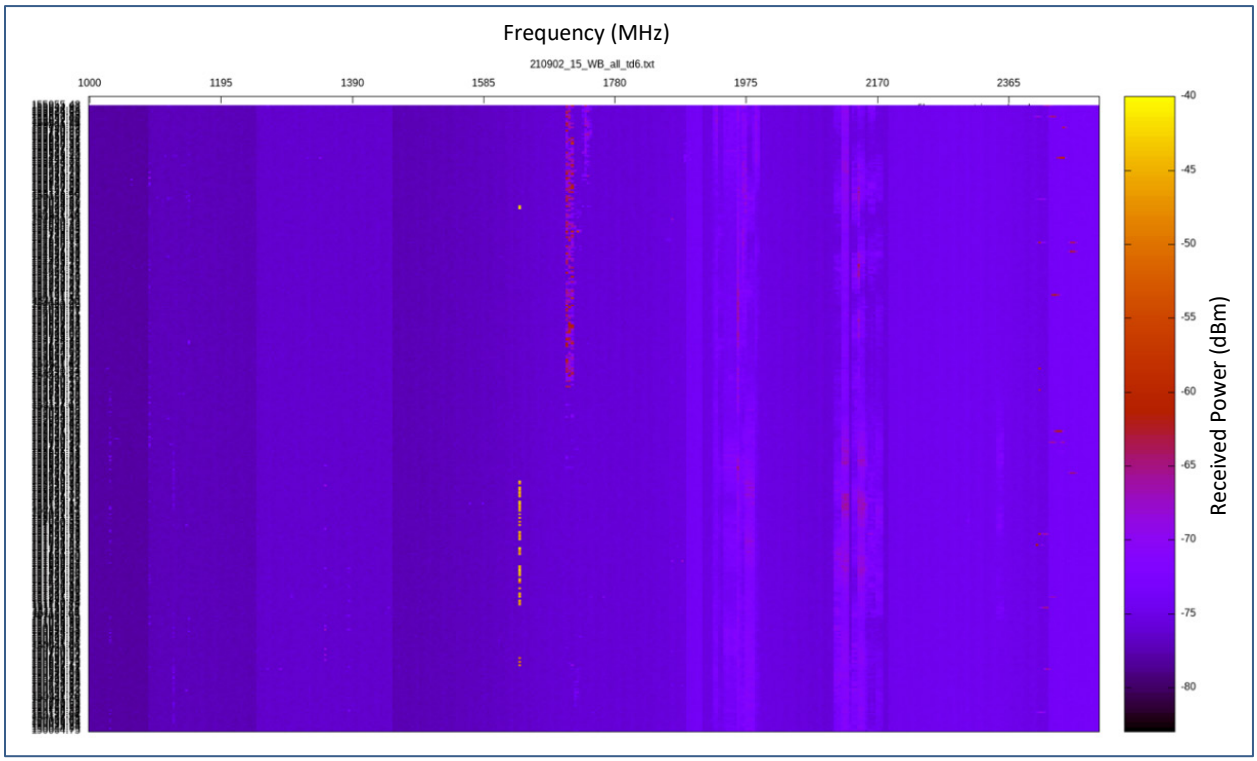


(Source: Volpe Center/Zeta Associates)

Figure 3-11. Single Spectral Sweep from 1.0 GHz to 2.5 GHz

Successive spectrum analyzer sweeps were collected with "peak hold" enabled for 0.7 seconds. These many Wide-Span Survey sweeps can be summarized over time with a waterfall plot as shown in Figure

3-12. This plot shows one (1) hour of individual sweeps (i.e., those represented in Figure 3-11), and reflects approximately 2,100 sweeps. The horizontal axis represents frequency (1.0 GHz to 2.5 GHz), the vertical axis time, and the specific colors indicate signal amplitude (per the scale on the right). The line of yellow points in this plot towards the middle represent roughly twelve (12) minutes of sporadic BGAN transmission. The three reddish bands to the right of BGAN appear in cellular base station frequency bands.



(Source: Volpe Center/Zeta Associates)

Figure 3-12. Waterfall Plot of Spectral Data Amplitude

3.1.5.3 Additional Signal Observations

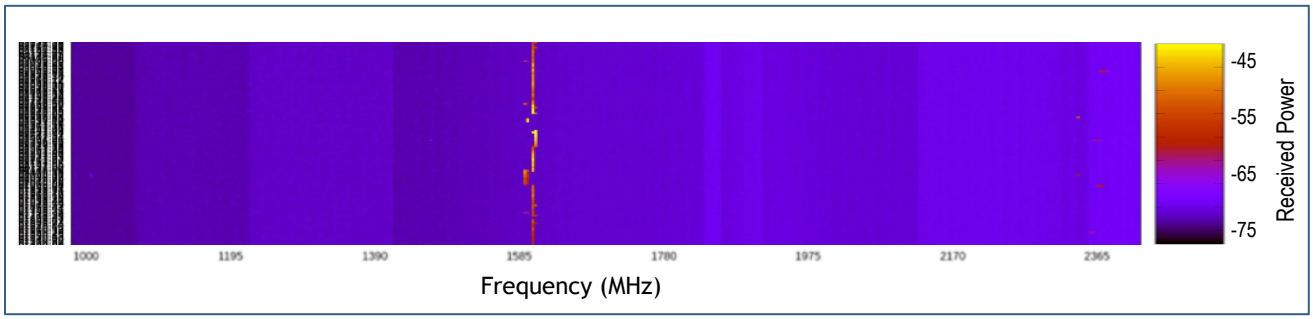
3.1.5.3.1 Broad Global Area Network (BGAN) Transmissions

One of the strongest signals in the 1.0–2.5 GHz band is from the BGAN transmit signal. BGAN is an INMARSAT satellite system, and the *Antares* has a BGAN Sailor terminal on the flying bridge. Figure 3-13 shows a picture of the BGAN directional antenna with its radome (protective cover) removed. This antenna is steerable to track INMARSAT geosynchronous satellites.

(Source: https://sync.cobham.com/)

Figure 3-13. BGAN System

A BGAN transmission example as measured with the Wide-Span Survey equipment is shown in the excerpt waterfall plot of Figure 3-14 (using the same color scale as Figure 3-12). The data displayed is for a reduced frequency span to highlight the BGAN transmission and illustrate how the apparent transmit power and transmit frequency can vary.

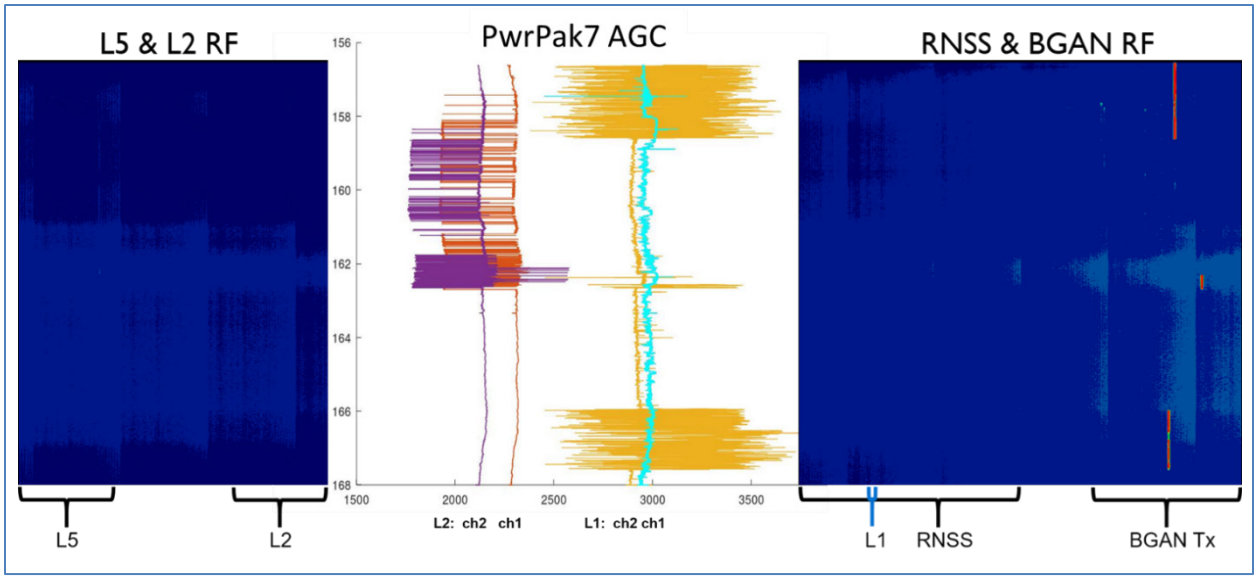


(Source: Volpe Center/Zeta Associates)

Figure 3-14. BGAN Transmission Example

While the BGAN antenna is mounted fairly high on the *Antares* flying bridge, above most other antennas, the transmit beam can reflect off metal structures, such as the mast superstructure and a large crane located aft of the bridge. These reflections can be quite strong, and can direct RF energy directly toward the GPS antenna and other antennas.

Figure 3-15 shows the PwrPak7 dual GPS receiver automatic gain control (AGC) levels for L2 and L1 from each of two GPS antennas on the flying bridge. The AGC voltage is an indicator of the received power level from the antennas. The light blue trace is for the receiver connected to the antenna (refer to Antenna 1 in Figure 3-5) mounted across the flying bridge from the BGAN antenna, while the gold trace is for the receiver connected to the antenna (refer to Antenna 2 in Figure 3-5) mounted much closer to the BGAN system.



(Source: Volpe Center/Zeta Associates)

Figure 3-15. Dual Receiver AGC Response Aligned with GPS and BGAN Spectral Data

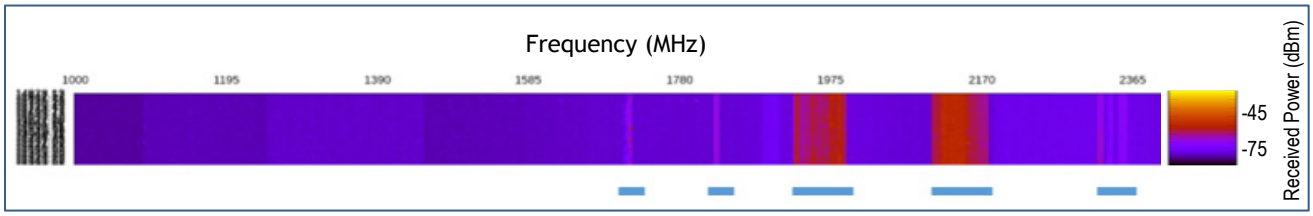
The bright red lines of the BGAN high-transmit power (in the waterfall plot on the right) correlate with the receiver AGC connected to the GPS antenna closest to the BGAN transmitter (Antenna 2). This AGC response indicates the BGAN transmit power is likely overdriving some component in the RF chain of this GPS equipment despite the frequency offset between BGAN (about 1.65 GHz) and GPS L1 (1.575 GHz). The greater antenna separation of GPS Antenna 1 appears to have mitigated this issue, since its AGC is relatively stable.

It should be noted that the GPS-Band Survey measurements in the L1 and L2 bands were not affected by BGAN signals. This is a reasonable outcome, because the RF filtering was much more robust than with the PwrPak7 dual-GPS receiver. While the dual-GPS receiver and antennas employ more typical commercial L1 filtering, the GPS-Band Survey signal path used a high-performance L1, L2, and L5 filter, which was able to reject the high-power BGAN transmit signal.

The PwrPak7 dual GPS receiver L2 AGC responses (the center, purple and brown traces in Figure 3-15) also exhibited some fluctuations. These are suspected to be due to internal device attenuators switching in and out as the L2 power fluctuated around some internal receiver threshold. The AGC levels appear to be jumping between distinct levels and this is most likely associated with having L2 input power from the antennas to the receivers very close to that internal threshold. There were no apparent causal signals evident in the Wide-Span Survey sweep around the L2 frequency. Nor did the GPS-Band Survey results indicate any significant interference. Lastly, no GPS L5 AGC data is shown because this PwrPak7 receiver was not equipped for L5 signal processing.

3.1.5.3.2 Cellular Telephone and Unknown Signals

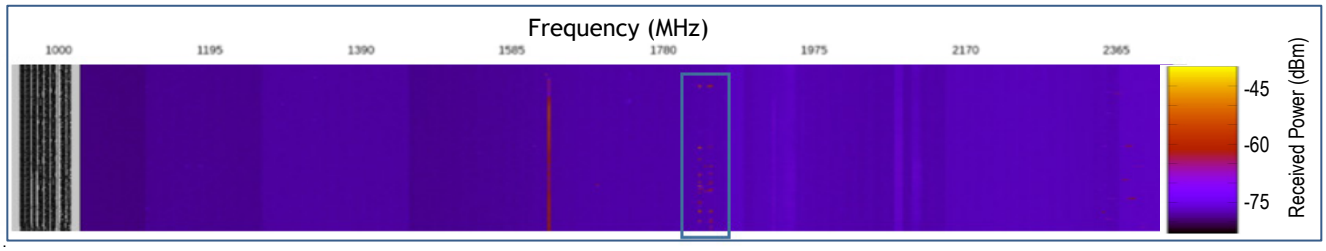
There are several bands of transmission that appear to coincide with cellular handset frequency allocations. These are highlighted with blue bars under the spectrogram in Figure 3-16.



(Source: Volpe Center/Zeta Associates)

Figure 3-16. Cellular Telephone Transmissions

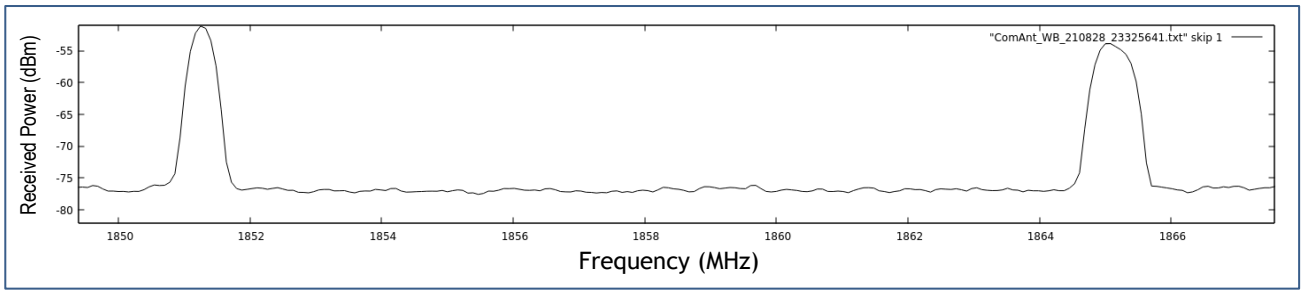
There were several detections of unknown bursts of RF energy. One set is shown within the highlighted blue box in Figure 3-17. These were detected in the evening of August 28, while the *Antares* was traveling southward down Chesapeake Bay.



(Source: Volpe Center/Zeta Associates)

Figure 3-17. Example of Unknown Signals #1

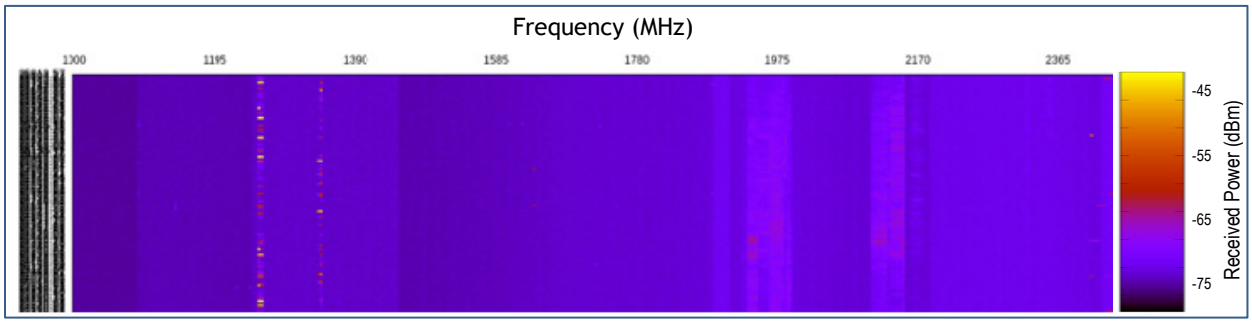
The first pair of transmissions is broken out and explained with the original spectrum analyzer sweep in Figure 3-18. The transmit frequencies were 1851.25 MHz and 1865.00 MHz. These are peak values measured over a duration of 0.7 seconds, so modulation details may be smoothed over.



(Source: Volpe Center/Zeta Associates)

Figure 3-18. Expanded View of Unknown Signal #1

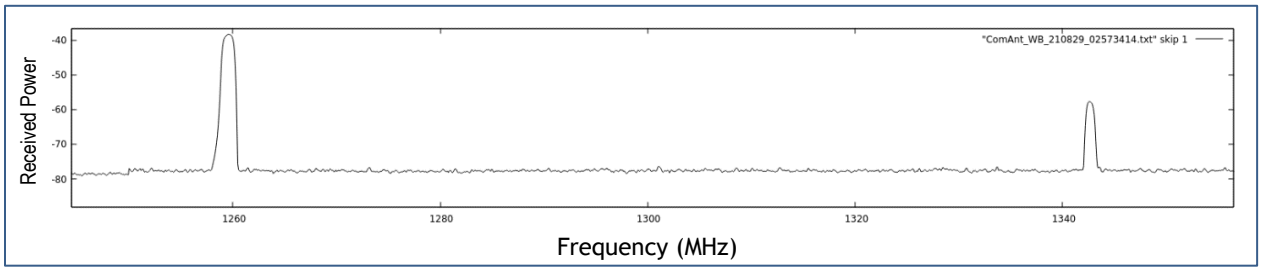
Another unknown transmission pair began to appear a few hours later and is shown in Figure 3-19 on the left. These were more powerful or closer than the previous example, and were detected at a different pair of frequencies, 1259.5 MHz and 1342.5 MHz.



(Source: Volpe Center/Zeta Associates)

Figure 3-19. Example of Unknown Signal #2

An expanded view of this signal is shown in Figure 3-20. As with the previous pair, this signal could be from two or more sites or ships transmitting, perhaps communicating with each other, one closer to the *Antares* and one further away and therefore weaker. Very similar bursts appeared on the return trip up Chesapeake Bay, while returning to Baltimore.



(Source: Volpe Center/Zeta Associates)

Figure 3-20. Expanded View of Unknown Signal #2

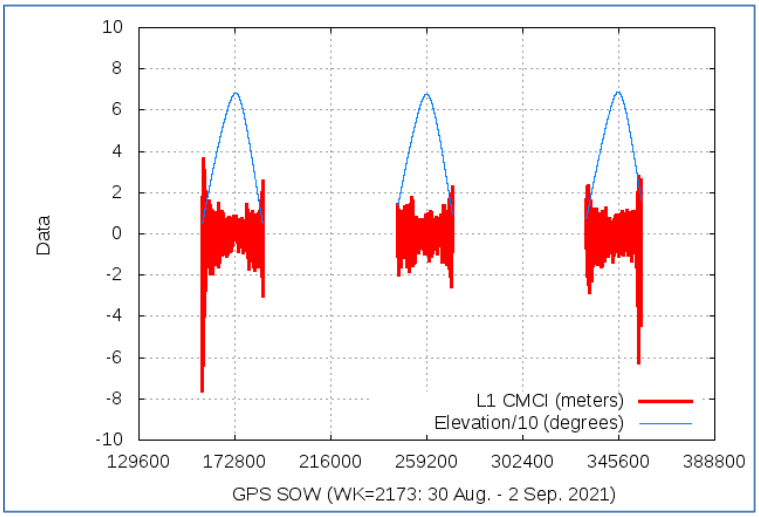
3.1.6 GNSS Processing

3.1.6.1 Multipath Analysis

One of the concerns with GNSS performance in the shipboard environment is the effect of large structures that could cause signal blockage, the propensity of metal surfaces causing multipath, and the potential for RF interference from ship communication and other navigation systems. Therefore, the focus of the analysis was characterizing signal tracking continuity and code multipath.

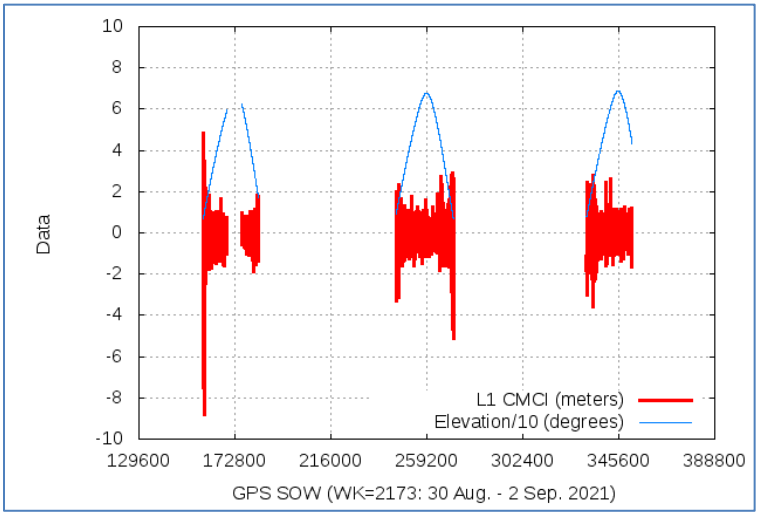
The typical approach to analyzing multipath is to compute code (pseudorange) minus carrier range corrected for ionosphere (CMCI) using dual-frequency carrier range. The GPS L1 C/A code multipath from a survey grade receiver such as the PwrPak7 can be as large as ten meters, while carrier multipath is only a few centimeters. The differencing technique of code-minus-carrier removes common signal dynamics, and clock and troposphere components, but doubles the ionospheric delay. The dual frequency carrier estimate of ionosphere removes this ionospheric component, allowing observation of

code noise and multipath. Examples of this processing from the two GPS antennas utilized by the PwerPak7 receiver are shown in Figure 3-21 and Figure 3-22 for pseudorandom-noise (PRN) code 32.[22]



(Source: Volpe Center/Zeta Associates)

Figure 3-21. L1 CMCI for PRN 32 from Antenna 1



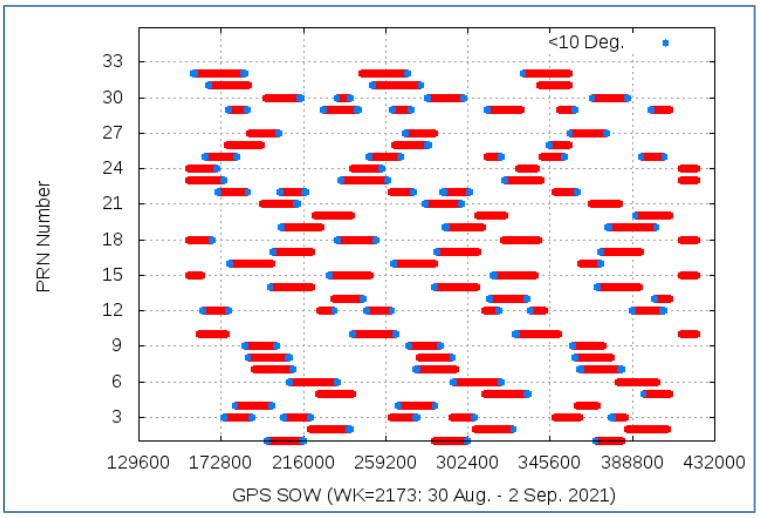
(Source: Volpe Center/Zeta Associates)

Figure 3-22. L1 CMCI for PRN 32 from Antenna 2

These plots show CMCI from three satellite passes over a three-day collection period and a scaled version of line-of-sight elevation angle to the satellite. The satellite pass data is for continuous receiver tracking of two hours or longer, with no carrier cycle-slips or loss-of-lock. (A two-hour limit is needed to estimate accurately any carrier ambiguities from CMCI with the assumption that code multipath over this duration is approximately zero-mean.) As expected in these figures, CMCI errors are larger at low

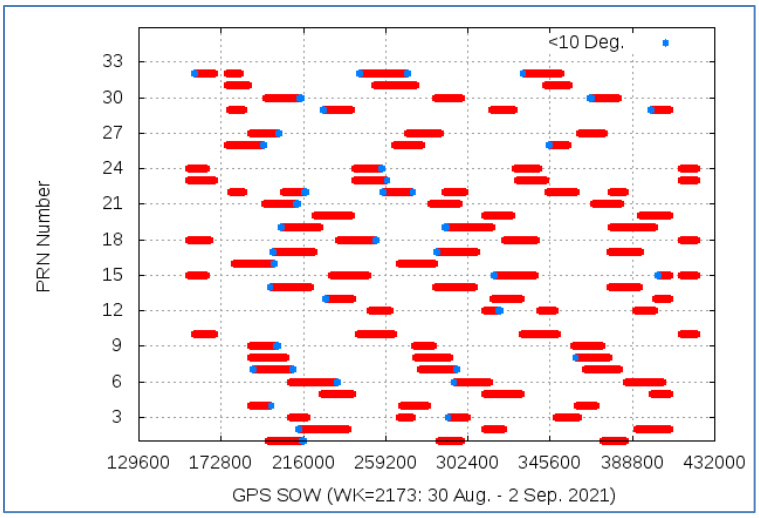
[22] Every satellite within the GPS constellation transmits its unique pseudorandom-noise (PRN) code part of the C/A navigation message. The PRN code allows the GPS receiver to identify exactly which satellite it is receiving. "PRN 32" identifies that the signal was received from a GPS satellite tracked as "Satellite 32."

satellite elevations and become smaller at zenith. Another interesting observation is that the first satellite pass from Antenna 2 is not continuous, which indicates loss-of-lock or cycle slips detected in the processing. To further explore the tracking continuity on each antenna, Figure 3-23 and Figure 3-24 show all the GPS satellite passes for this collection and highlight tracking below 10 degrees elevation (in blue).



(Source: Volpe Center/Zeta Associates)

Figure 3-23. Satellite Passes from L1 C/A CMCI Processing from Antenna 1



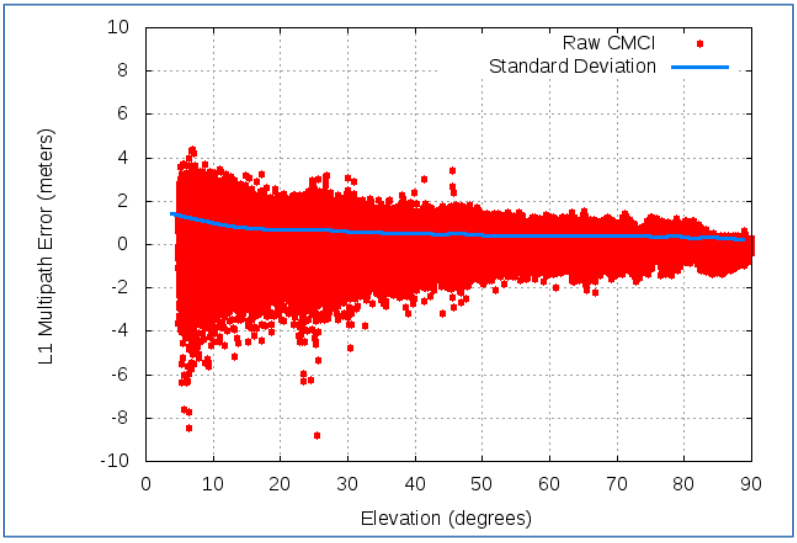
(Source: Volpe Center/Zeta Associates)

Figure 3-24. Satellite Passes from L1 C/A CMCI Processing for Antenna 2

Antenna 1 generally acquires satellites below 10 degrees and tracks down to this same elevation as the satellites set. This tracking at 10 degrees or lower suggests code multipath, signal blockage, and RF interference are not impacting signal tracking significantly, such that long continuous satellite tracks should be expected. For Antenna 2 (Figure 3-24) however, tracking is not nearly as robust. As will be

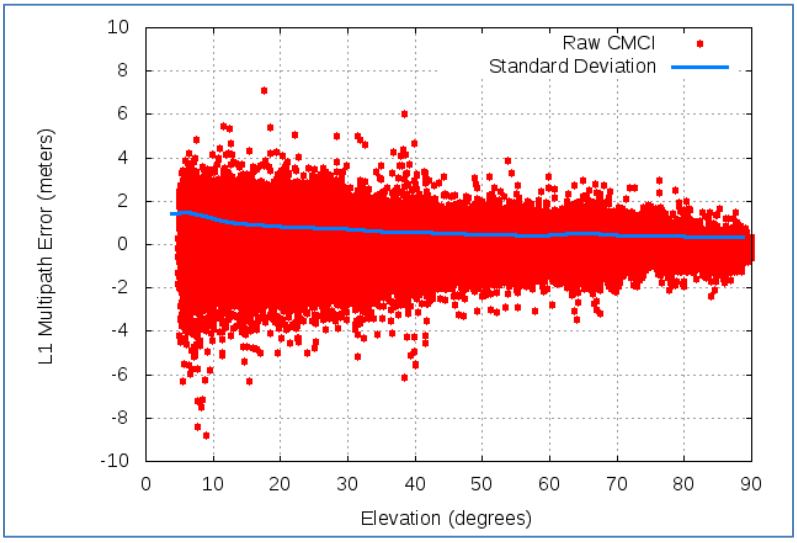
shown later, this is largely caused by this antenna's location near to the BGAN antenna, resulting in RF interference that degrades L1 C/A tracking.

Figure 3-25 and Figure 3-26 show raw L1 C/A CMCI and its standard deviation for all satellites versus satellite elevation angle, for each antenna. These multipath errors are consistent with expectations for a survey grade receiver/antenna in this environment (with standard deviation of under 2 meters at an elevation of 5 degrees). It is important to note that multipath error could be much larger—up to 100 meters—for a typical non-survey-grade GPS receiver, and the measurement performance shown in this analysis should not be assumed for MARAD's currently installed non-survey-grade GPS equipment.



(Source: Volpe Center/Zeta Associates)

Figure 3-25. L1 C/A CMCI vs. Elevation Angle for Antenna 1

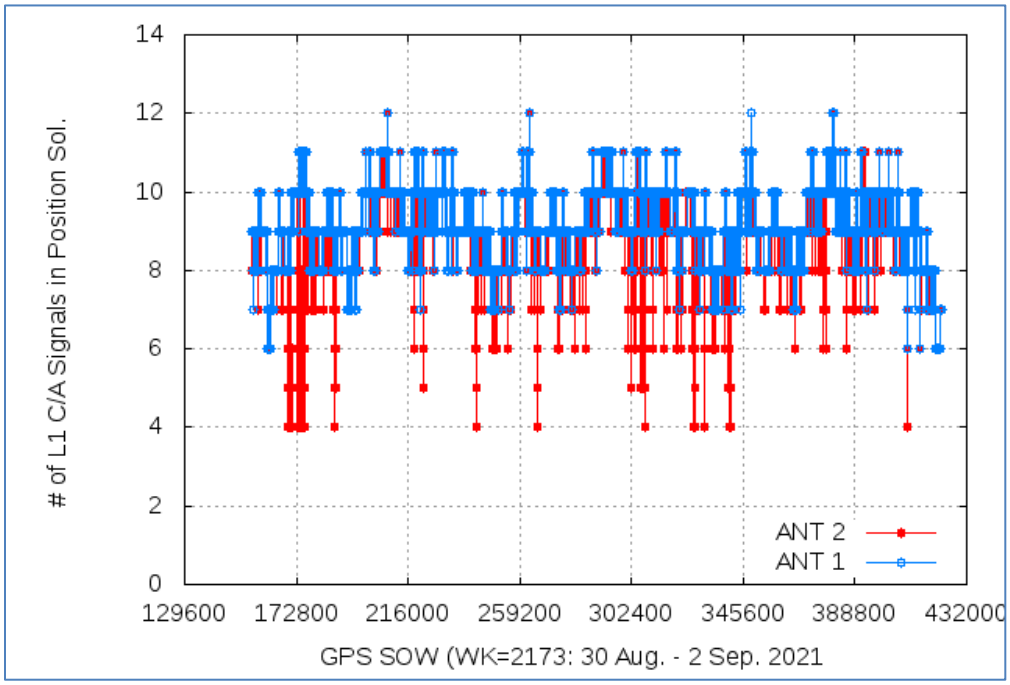


(Source: Volpe Center/Zeta Associates)

Figure 3-26. L1 C/A CMCI vs. Elevation Angle for Antenna 2

3.1.6.2 Position Performance

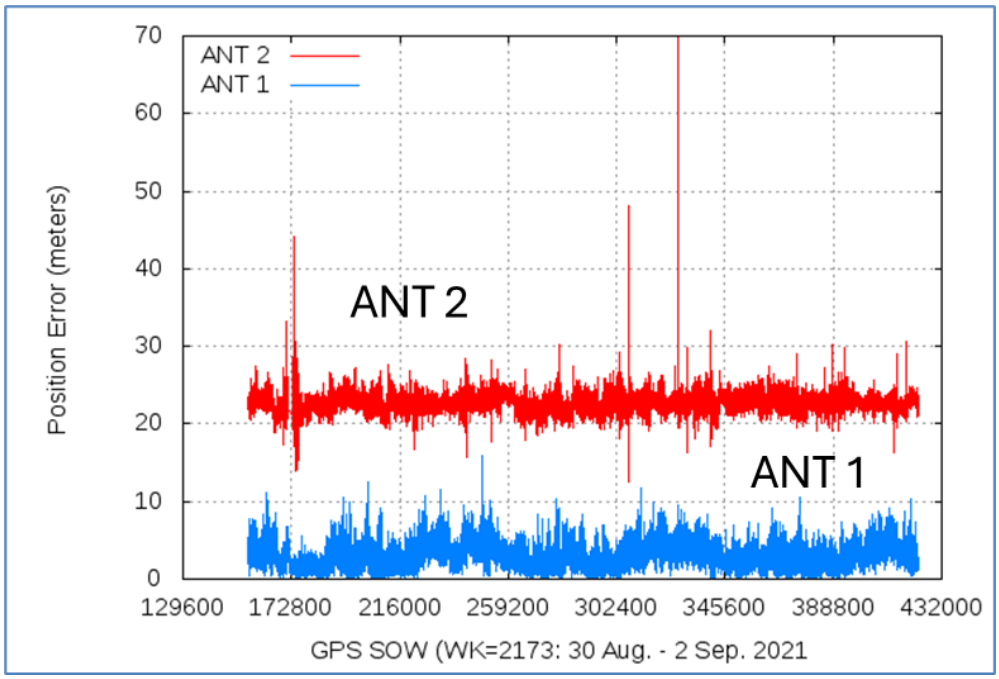
The positioning performance was evaluated for both antennas over the same time span used for the multipath analysis. Point position solutions were computed using L1 C/A signals only, to be comparable with performance from current signal frequency equipment installed on MARAD's fleet. These estimates were compared with the receiver's "best position" estimates using all available GNSS measurements and the IMU. Specifically, this "all-view, best-position" solution was used as "truth" in this processing. It made use of multiple frequencies to remove ionospheric error as well as ranging from multiple constellations, and typically had anywhere from 20 to 35 range sources used in its solution. Figure 3-27 shows the number of L1 C/A ranging sources used for Antenna 1 and Antenna 2 position solutions.



(Source: Volpe Center/Zeta Associates)

Figure 3-27. L1 C/A Signals used in Antenna 1 and Antenna 2 Position Solutions

Antenna 2 signal tracking was not as robust as Antenna 1 because of its proximity to the BGAN terminal. This is evident with Antenna 2 typically having fewer signals in its position solution. Figure 3-28 shows the difference in position estimates for Antenna 1 and 2 from the truth estimate.



(Source: Volpe Center/Zeta Associates)

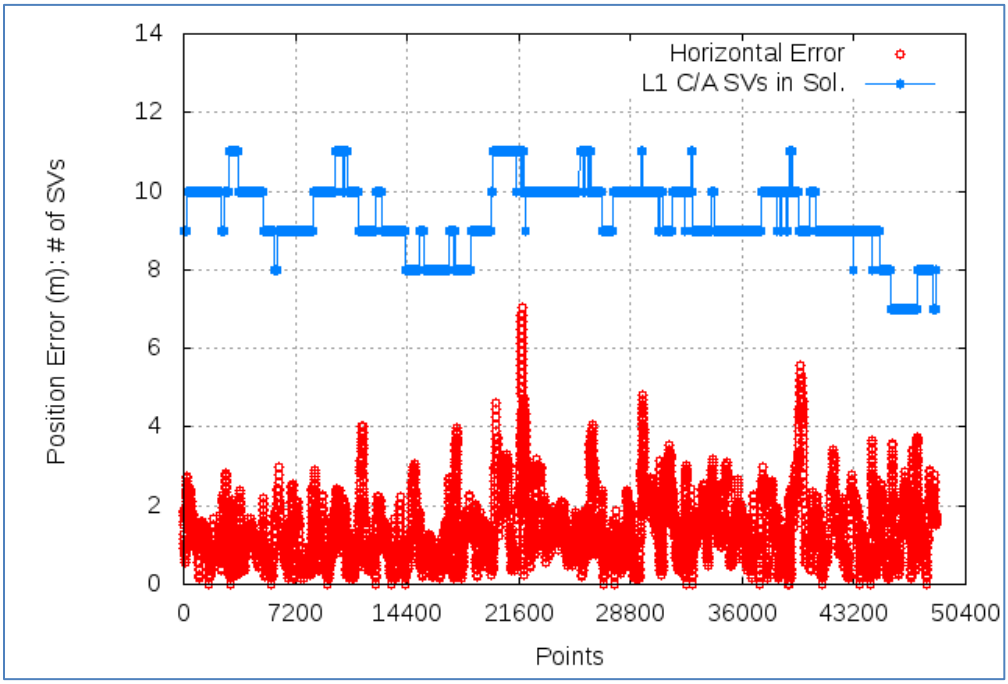
Figure 3-28. L1 C/A Position Errors for Antennas 1 and 2

The best position (truth) estimate is for Antenna 1, so the difference with Antenna 1 and L1 C/A reflects the accuracy of single frequency positioning error while Antenna 2's difference reflects this same positioning error and the 22-meter offset between these antennas. Recall these antennas were located on the starboard and port sides of the flying bridge. The positioning error based on these differences from truth typically ranges from a few meters to around 10 meters for Antenna 1 and similarly for Antenna 2 but with some much larger excursions. These larger excursions are most likely related to fewer ranging sources caused by RF interference and signal blockage.

Another observation from Figure 3-28 is the position difference of the 22 meters between the antennas is easily seen, even with this L1 C/A only point positioning. Therefore, differencing these position estimates over this baseline should be an effective detection mechanism for measurement spoofing, since this offset would be constant unless the receivers are captured by a spoofer. It would be possible with some modest signal processing to reduce the noise in these L1 C/A position estimate (through filtering and outlier screening) such that even better resolution of this 22 meter position offset between the two antennas could be obtained. This would improve false alert concerns but most likely at some expense to timely alerts, which could be a reasonable trade-off for a maritime application.

Lastly, to determine if the L1 C/A only position performance from the PwrPak7 receiver could be used as a proxy for single frequency equipment typical of MARAD's fleet, a Furuno GP170 receiver, connected to a Furuno GPA17S antenna were installed on a clear, unobstructed roof in Fairfax, VA for a 15-hour static data collection. Signal blockage on the roof was not as challenging as onboard the *Antares*, but multipath is comparable. Figure 3-29 shows the position error and L1 C/A ranging sources used in the

solution from this collection. The number of signals and position errors are similar to the PwrPak7 results from the *Antares*. This result is promising to support the use of the currently installed GPS equipment, such as the Furuno GP170, for spoof detection as described above, but this performance should be more rigorously characterized in the ship environment before using for this purpose.



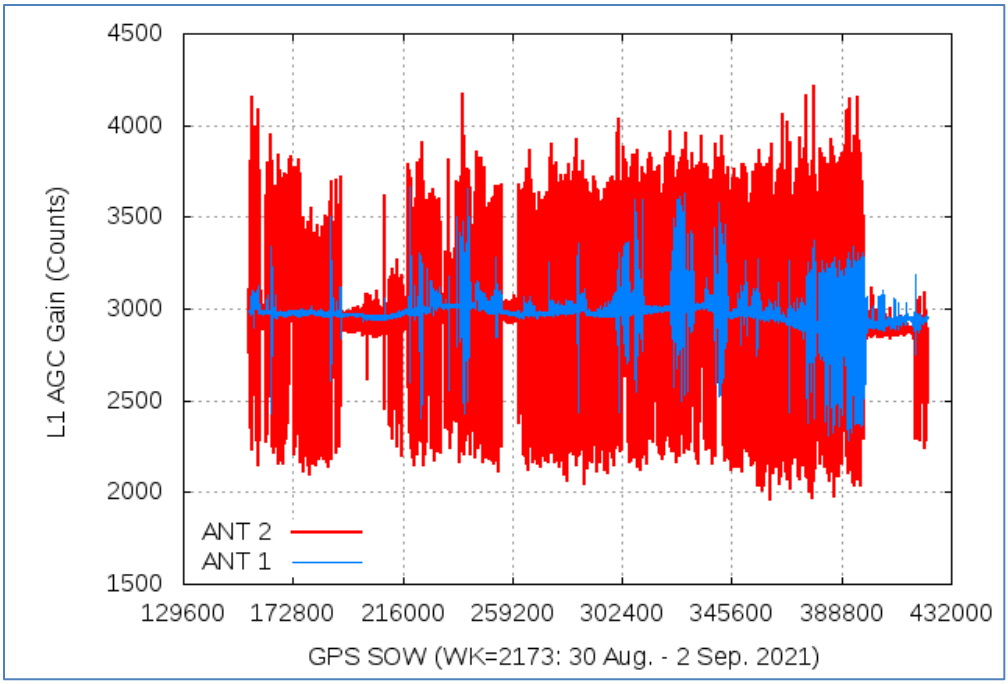
(Source: Volpe Center/Zeta Associates)

Figure 3-29. Furuno GP-170/GPA017S Performance at Zeta

3.1.6.3 Radio Frequency (RF) Interference

GPS Antenna 2 was located next to the BGAN antenna, and separated from GPS Antenna 1 by approximately 22 meters. The PwrPak7 and GNSS-850 antenna are designed to receive signals from multiple satellite constellations, including GPS and GLONASS. Processing GLONASS signals requires an antenna that provides no signal attenuation up to at least 1610 MHz. The BGAN transmissions (approximately 1650 MHz) are relatively close in frequency to that of the GPS L1 signal, and at a much higher power than the GPS signal.

Figure 3-30 shows the automatic gain control (AGC) response for receivers connected to Antennas 1 and 2, to demonstrate the difference in L1 interference between each of these antennas. The purpose of the AGC is to adjust the incoming signal level to optimize signal digitization for GNSS signal processing; under normal conditions, it would be at nearly a fixed value. As the figure shows, the AGC for the receiver connected to Antenna 2 (in red) is being constantly adjusted based on additional signal power detected from the BGAN terminal. The AGC with Antenna 1 (in blue) is also being adjusted but to a much lesser extent and the majority of the time is near a fixed value.

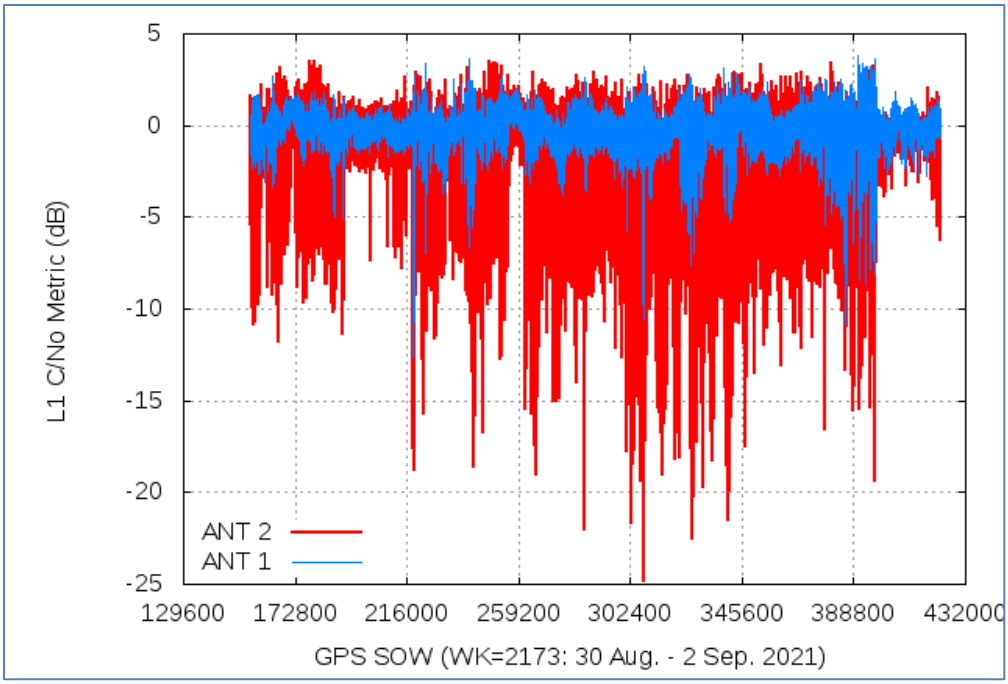


(Source: Volpe Center/Zeta Associates)

Figure 3-30. L1 AGC from Receiver/Antenna 1 and Antenna 2

The impact of the BGAN interference was further demonstrated by computing an L1 C/N_0 metric for both antennas. This metric is formed every second by first correcting each satellite-measured C/N_0 by subtracting an expected estimate drawn from a 2nd order function developed for this equipment that represents nominal measured C/N_0 versus satellite elevation. These corrected values are then averaged over all satellites to form this metric. Only satellites above 20 degrees of elevation were included in the metric to minimize the influence of multipath signals. If no interference is present, this metric would indicate a value of near zero decibels, as all measured C/N_0 values would be close to nominal. When interference is present, this metric would indicate a negative value as RF interference tends to decrease C/N_0 values.

Values of the C/N_0 metric for Antennas 1 and 2 are shown in Figure 3-31, where the impact for Antenna 2 (in red) is very clear with many instances of C/N_0 being degraded more than 10 dB. Values greater than 15 dB will typically cause loss-of-lock on some satellites. The impact on the equipment was exacerbated by the close proximity of Antenna 2 to the BGAN antenna and the GNSS receiver being open to GLONASS signals. Both the AGC and this C/N_0 metric are useful indicators for both interference and spoofing detection.



(Source: Volpe Center/Zeta Associates)

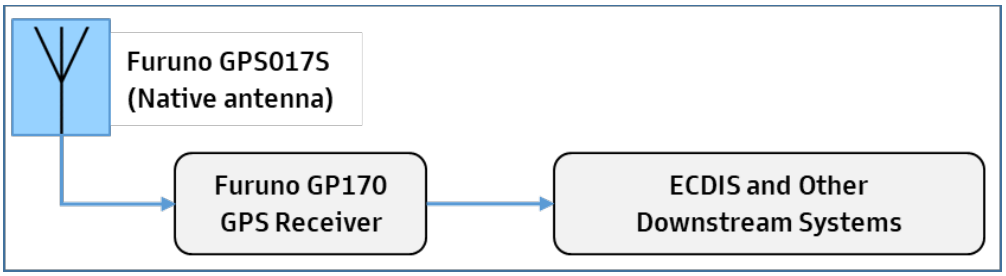
Figure 3-31. L1 C/N_0 Metric from Receiver/Antennas 1 and 2

3.2 Protective Solution

This section describes the protective solution evaluated during the Pilot Project, including its configuration and concept of operation. Also described is a concept for an overall solution, test results on key elements of the solution, and potential future enhancements. The testing included establishing the nominal baseline RF environment, followed by tests in the presence of sophisticated, but realistic GPS threat vectors. Analysis of these two conditions would demonstrate and quantify the potential added resiliency of each protective measure relative to the currently installed PNT systems.

3.2.1 Description and Concept of Operation

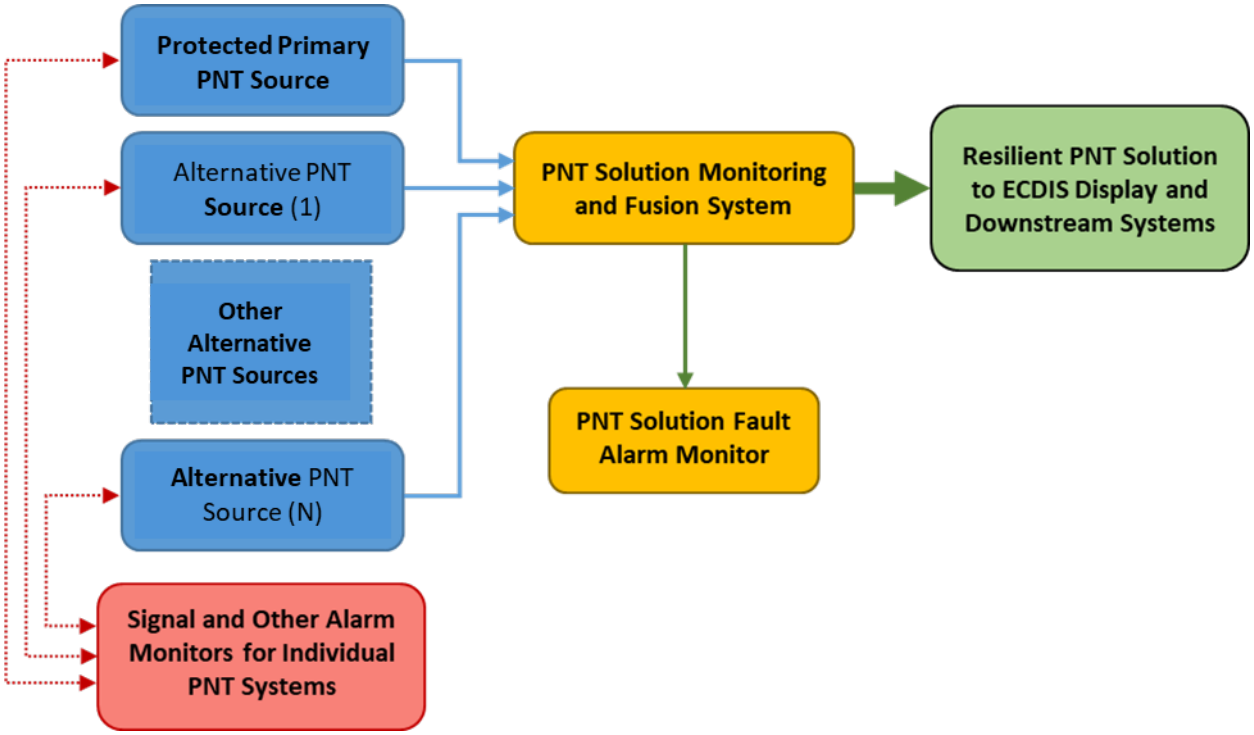
Current PNT source configuration is a passive omnidirectional antenna and an L1 GPS receiver (see Figure 3-32). Across the 38 vessels in the MARAD RRF fleet surveyed, the Furuno GPA017S GPS antenna is predominant. For their PNT receiver, 33 ships have at least one Furuno GP170, and 17 ships have at least one Furuno GP150. In addition to the information displayed directly by the GPS receivers themselves, PNT data is distributed as outputs to shipboard ECDIS units and other downstream systems. This configuration leaves the existing PNT source susceptible to intentional and unintentional signal disruptions and manipulations, and provides no indication of the quality of the PNT solution to the user.



(Source: Volpe Center)

Figure 3-32. Schematic of Current GPS Installations aboard MARAD RRF Vessels

Figure 3-33 illustrates an example of a comprehensive resilient PNT system. This system includes a protected GPS receiver capable of detecting and mitigating many GPS signal disturbances (including jamming, signal and data spoofing), complementary PNT source(s) to provide cross-checking and fusion capabilities, and monitoring and alarm capabilities. The monitoring and detection function includes a switching or fusion algorithm that detects solution degradation, mitigates GPS signal disturbances, and uses additional PNT sources to provide the user with reliable, precise, and true PNT data.

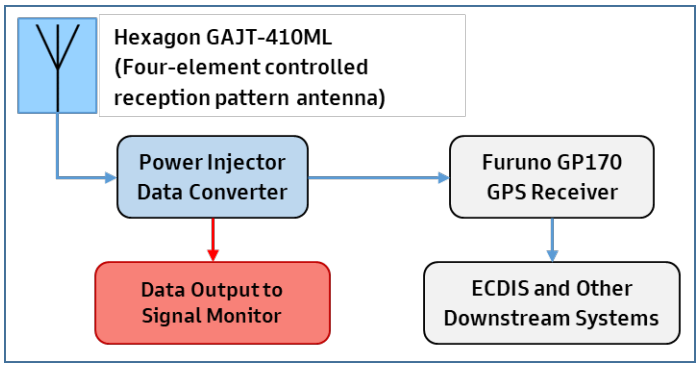


(Source: Volpe Center)

Figure 3-33. Conceptual Schematic of Comprehensive Resilient PNT System

This project explores two key components of the overall resilient solution. The first component is a protected primary GPS receiver and the second is an alternate PNT source. The primary PNT receiver is protected by enhancing the existing system with a capability to monitor and mitigate GPS signal disruptions. This was achieved by replacing the native GPS antenna with a multi-element nulling antenna capable of suppressing GPS interference, jamming, and spoofing signals in the direction of the

source(s) independent of the modality of the attack. In particular, the suppression of the unauthentic signal is agnostic to whether the attack is a data or measurement spoofing attack. The diagram of this system is shown in Figure 3-34.

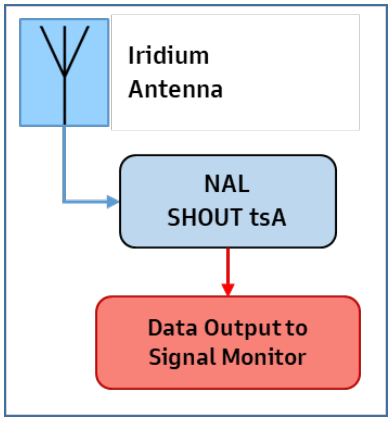


(Source: Volpe Center)

Figure 3-34. Schematic of Protective Solution as Tested aboard the SS *Antares*

The second solution explored was use of a complementary PNT source. The device evaluated was a NAL Research Corporation SHOUT tsA receiver using a Satelles Satellite Time and Location (STL) subscription service. The complementary space-based PNT Solution considered and tested in this Pilot Project is shown in Figure 3-35. This solution was selected as an initial test candidate for the following reasons:

1. It is a space-based solution that can provide global availability, making it especially well-suited for the oceanic maritime environment; and
2. STL exhibited acceptable performance and potential during an earlier demonstration of complementary space-based PNT technologies.[23]



(Source: Volpe Center)

Figure 3-35. Schematic of Complementary Space-Based PNT Solution as Tested during Pilot Program

[23] *Complementary PNT and GPS Backup Technologies Demonstration Report*, January 2021.

3.2.2 Component 1: GNSS Receiver Resiliency Enhancement

3.2.2.1 Equipment Selection and Suitability

The technical team sought to identify techniques and products that provide alerting capabilities (e.g., a detection meter) when GPS jamming or spoofing conditions are present. Some simple and relativity effective techniques for interference detection are well known, for example by using the GPS receiver's AGC and C/N_0 estimates. Other more sophisticated techniques such as nulling antennas that provide both alerting and mitigation of stronger signals are just now coming to market.

An evaluation of COTS products was undertaken to identify devices that provide both a) an improved GPS operation for interference and spoofed environments and b) an alerting capability. The evaluation included advertised functionality and performance, mitigation capabilities, ease of installation, potential for future integration with ECDIS, availability, cost, and the detection meter capability. (Future field or laboratory testing will be conducted for suitable products that can be reasonably purchased or loaned by the equipment manufacturer.)

(Source: https://novatel.com/)

Figure 3-36. Hexagon GAJT-410ML Antenna

The technical team selected the NovAtel Hexagon GAJT-410ML (hereafter referred to as "GAJT") for the demonstration of the protective solution.[24] The Hexagon antenna is an L1 and L2, four-element controlled reception pattern antenna (CRPA) that replaces a receiver's native antenna (i.e., the antenna typically supplied by the GNSS device manufacturer) (see Figure 3-36).

Based on the technical information provided in GAJT specification documentation, the GAJT it is a multi-element antenna array with nulling capability. The nulling algorithm belongs to a class of adaptive beamforming techniques where the complex array weighting vector is found as a solution to a constrained optimization problem. The algorithm solves for the constrained weighting vector by minimizing the error between the constrained solution and quiescent solution subject to a minimum power constraint. In the presence of a jammer or a strong spoofer, the constrained weighting vector solution effectively results in a good approximation of the quiescent pattern with a null placed in the

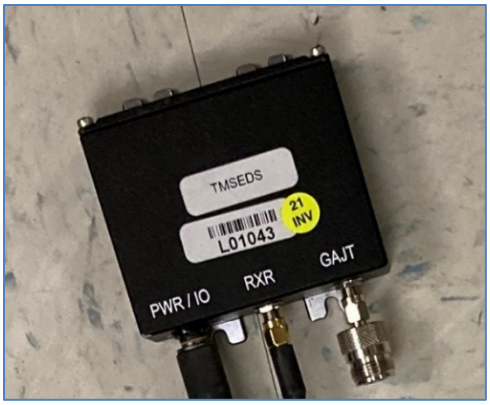
[24] This GAJT model is functionally equivalent to the GAJT-410MS antenna, which is marketed for marine use.

direction of the jammer or spoofer. This is considered an adaptive beamforming technique because a priori knowledge of the direction of the jammer or spoofer is not needed, and its beamforming pattern adapts in real-time to a dynamic jamming or spoofing environment.

When a null is successfully placed in the direction of the spoofer, the carrier and code tracking loops can no longer lock on the spoofing signal. The receiver will be unable to demodulate the spoofing data therefore protecting the receiver from both signal and data spoofing attacks. This nulling technique fails if the transmitted power of the spoofer is below the receiver and antenna noise floor. However, most successful spoofing attacks require at least a period of high-power transmission that is greater than the noise floor or a period of knockoff jamming to break receiver tracking of authentic signals.

Additionally, in order of the spoofer to cover a large area, there is a region around the spoofer where the power will continuously exceed the noise floor. Therefore, adaptive nulling antennas are expected to successfully defeat, or limit the effect of, the vast majority of spoofing attacks as long as the number of spoofers is smaller than the maximum number of spoofers supported by the antenna array (usually N-1 where N is the number of elements in the array). An example of more sophisticated data and signal spoofing that defeat the nulling algorithm is a satellite-based spoofing attack (or unintentional bad uploads to a satellite) where it is possible to deliver a uniform power below the noise floor from a high elevation angle on a large swath on the earth surface. Since the power received will consistently be below the noise floor it will go undetected by the nulling antenna and will require additional mitigation techniques including data validity checking.

The Hexagon antenna is paired with a power injector data converter (PIDC) that provides power to the antenna, a protected signal to the receiver, and data outputs (via a user interface) on received power and direction of unwanted signals (see Figure 3-37). This antenna-and-converter combination could provide MARAD's RRF vessels with protection from spoofed or jammed signals while providing some information about the harmful signal(s). It would allow the RRF vessel to **Detect** in real-time jamming or spoofing (data and measurement) attacks and **Respond** by blocking it at the antenna. The GAJT antenna's spoofing mitigation and detection happens on the device's physical layer; it does not perform any data range or other validity checking beyond what is inherently performed by the GPS receiver in its current configuration.



(Source: Volpe Center)

Figure 3-37. Power Injector Data Converter (PIDC)

3.2.2.2 Principle of Operation and Implementation

The GAJT-410ML PIDC output of interference power and relative interference bearing from both antennas would be monitored continuously. The output power would be treated in a similar fashion to an AGC detector where exceedance of a threshold level would trigger an alert from the "detection meter." The relative bearing reported from the GAJT could then be used with ship heading to provide additional situational awareness on interference direction. This GAJT monitoring would be utilized in concert with continuous monitoring of GPS antenna positions computed by each Furuno receiver. The difference in these reported positions would be compared with an offset threshold. If this threshold was exceeded or if no position estimates are computed, this would indicate GPS navigation outputs should no longer be utilized and the complementary PNT source should be selected. Reversion to use of GPS for navigation would be dictated when reported interference power and position offset returned to nominal values.

The GAJT-based mitigation and detection happens on the physical layer and the device does not perform any data range or other validity checking beyond what is inherently performed by the GPS receiver in its current configuration. When paired with the nulling capability of the GAJT antenna, the GPS receiver would be unable to demodulate the spoofing data therefore protecting the receiver from the vast majority of both signal and data spoofing attacks. (Some hysteresis should be included in this alerting concept to mitigate toggling back and forth between GPS and complementary PNT sources.)

3.2.3 Component 2: Use of Complementary PNT Technology

This analysis also investigated the use of a non-GNSS solution to provide a form of complementary PNT technology to assist with jamming and spoofing detection. A NAL Research Corporation SHOUT tsA prototype unit, on loan from the U.S. Department of Homeland Security, was used, and integrated with a Satelles STL subscription service. The SHOUT/Satelles solution offers the potential of a complementary space-based PNT solution.

3.2.3.1 Principle of Operation and Implementation

The SHOUT tsA would be operated in STL mode continuously to support immediate availability of the PNT solution. In addition, SHOUT output metrics could be monitored for comparison with selected thresholds as a check on PNT operation and quality. Metric comparisons could include ensuring a sufficient number of observed satellites, adequate burst reception rates, and an average of reported burst C/N_0 above a nominal value. Position age and accuracy, which appear on the SHOUT tsA home screen, could also be monitored if these data items are determined to be available within SHOUT tsA output messages. Additional diagnostic data items may be determined through further device investigation and testing.

3.2.4 Alternative Solutions Identified but not Evaluated during Pilot Project

One approach that requires further research is the dual antenna concept discussed in section 3.1.6.2. Under this framework, the baseline distance between two GPS/GNSS antennas on the ship would be

measured and constantly monitored in some manner. When the known separation distance between the two antennas deviates from the baseline, the system would detect a potential issue with the received GPS/GNSS signal and alert the user to switch to a complementary PNT source. The concept has been proven but would require additional planning and testing to mature the concept.

3.3 Detect, Respond, and Recover Capabilities of Protective Solution

The ability of the proposed GPS receiver setup and hardware configuration to detect, respond to, and recover from targeted attacks was tested during a live-sky jamming and spoofing test event. This section describes that testing event, equipment configuration, data collection, and analysis, followed by an evaluation of the receiver resiliency enhancement of the protective solution.

3.3.1 GPS Equipment Testing for Critical Infrastructures (GET-CI)

The Furuno GP170 receiver was included in a DHS "GPS Equipment Testing for Critical Infrastructure" (GET-CI) event held at the Mountain Home Range Complex, ID on June 21–26, 2021. The event was open to manufacturers, owners, and operators, and allowed evaluations of GPS equipment used within critical infrastructure with the intent of understanding equipment vulnerabilities. The test was conducted in a live-sky environment, with RF jamming and spoofing signals directed at GPS L1 C/A processing.

3.3.1.1 Test Description and Setup

The equipment selected for testing consisted of a Furuno GP170 receiver and Furuno GPA017S antenna (see Figure 3-38), which represent the equipment installed aboard many of MARAD's RRF vessels. The Hexagon GAJT-410ML antenna was used with the Furuno GP170 receiver on alternating days to demonstrate its potential for mitigating jamming and spoofing and for alerting users to these conditions. This configuration of the GP170 with the GAJT-410ML (and its PIDC) are as previously shown in Figure 3-35 for the proposed protective solution.

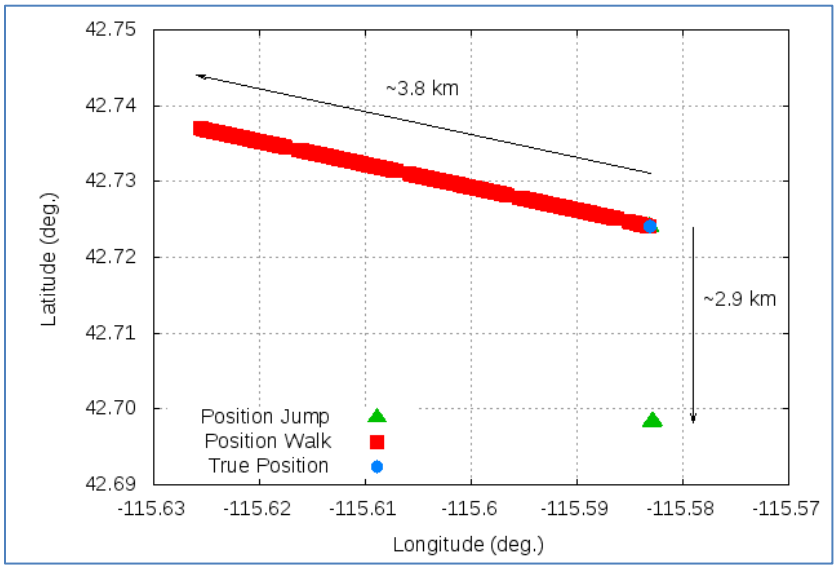
(Source: www.furunousa.com)

Figure 3-38. Furuno GPA017S Antenna

A total of 22 fixed-infrastructure test scenarios were executed over four days. The tests were designed to elicit different equipment responses and included conditions to cause GPS receiver time-and-position to jump or ramp/walk. Tests were also included to stress receiver processing robustness by transmitting erroneous GPS L1 C/A navigation data. For each test, receivers were allowed a clean RF environment to reach steady state prior to the transmission of any spoofing or jamming signals. The spoofed signals were then transmitted with or without the benefit of knock-off jamming.[25]

3.3.1.2 Data Analysis and Results

While there was a large quantity of data collected from each day, performance of the Furuno GP170 receiver over the course of the entire event can be summarized by three figures (Figure 3-39, Figure 3-40, and Figure 3-41). Figure 3-39 shows the position reported by the Furuno GP170 when using its native Furuno GPA017S antenna for tests with a position jump and a position walk from testing. When the spoofed signal was transmitted, the Furuno GP170 receiver dropped the valid L1 C/A signals and was captured by the false signals. This caused the receiver position to walk or jump over several kilometers, consistent with scenario intentions. The receiver provided little or no indication it had been captured by these spoofed signals.



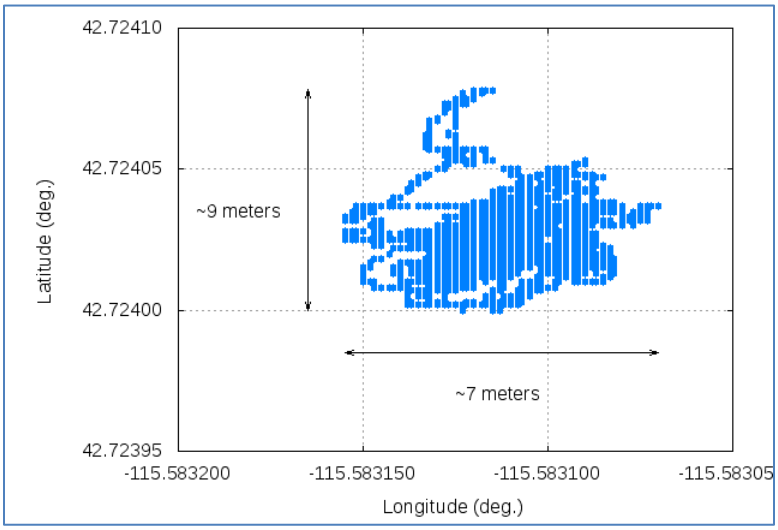
(Source: Volpe Center/Zeta Associates)

Figure 3-39. Furuno Capture Examples with Position Walk and Position Jump

In contrast, Figure 3-40 shows the Furuno GP170 position estimates for an entire day of testing when using the Hexagon GAJT-410ML antenna. The same types of jamming and spoofing tests were executed, but while using the Hexagon antenna, the Furuno GP170 receiver reported position estimates consistent

[25] Knock-off jamming refers to a pre-spoofing event, when a jamming signal is first transmitted for a short duration (usually few seconds), forcing the victim GNSS receiver to lose code and carrier lock on authentic GNSS signals. After losing lock, the receiver transitions back to a signal acquisition state. The knock-off jamming event increases the likelihood that the receiver will subsequently acquire the transmitted spoofing signals, which usually have higher power than authentic GNSS signals.

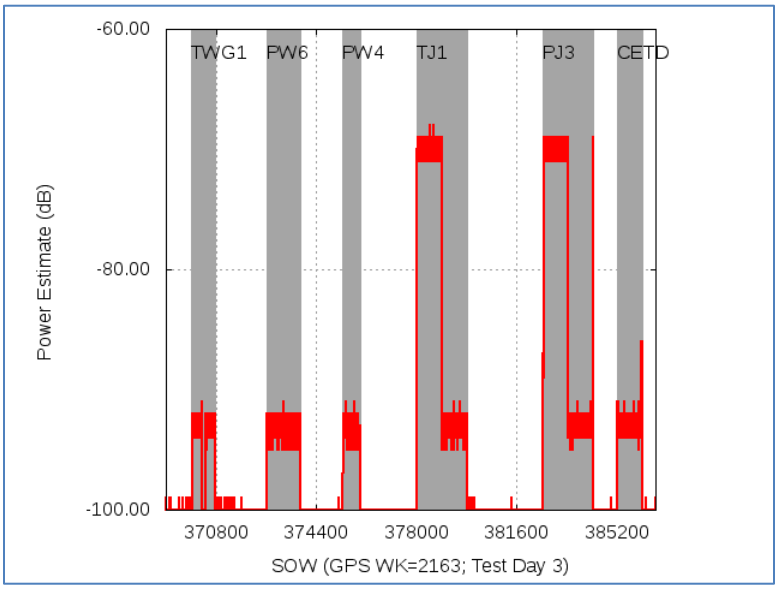
with normal performance. These results are indicative of Furuno GP170 performance for the entire week; with its native antenna, the receiver was negatively impacted by the test scenarios and when using the protective GAJT antenna, it was not impacted.



(Source: Volpe Center/Zeta Associates)

Figure 3-40. Furuno Position Performance

Figure 3-41 shows the reported power and direction for unwanted signals. This data is demonstrated by showing reported power estimates for jamming and spoofing events during a day of testing. The grey rectangles show when the jamming and spoofing signals were turned ON and the red line shows the power level reported by the protective GAJT antenna. The large power estimates for TJ1 (Time Jump) and PJ3 (Position Jump) are indicative of tests where the spoofing signals were preceded with knock-off jamming.



(Source: Volpe Center/Zeta Associates)

Figure 3-41. GAJT Power Reporting

3.3.2 Characterization of Complementary PNT Performance and Data Collection

Satellite time and location (STL) is a proprietary time-of-arrival (TOA) multilateration system designed by Satelles, Inc. (Reston, VA) offering three-dimensional (3D) positioning and timing using dedicated satellite signals of the Iridium satellite communication system (i.e., STL is not a signal-of-opportunity system).[26] The STL signals are broadcast by all 66 satellites of the Iridium constellation for continuous global coverage. Iridium is a low Earth orbit (LEO) constellation, at about 780 km altitude and transmitting in the frequency band 1621.35–1626.5 MHz.

Due to the proximity of LEO satellites (25 times closer to the Earth than GNSS satellites) and its use of a high-power signal, the STL broadcast signal is about 1,000 times (30 dB) stronger than that of GPS. In addition, STL uses the complex and overlapping beam patterns of the Iridium satellite signals, as well as cryptographic techniques in order to mitigate spoofing. Presently, the STL signals are proprietary and accessible only by STL subscribers using proprietary equipment from manufacturers licensed by Satelles.

3.3.2.1 Objective

The SHOUT tsA satellite tracker from NAL Research was tested to evaluate some aspects of its suitability as a complementary space-based source of PNT for integration into MARAD's RRF fleet. The SHOUT tsA is a dual system receiver capable of providing PNT information derived from GNSS signals or from the STL signal generated by Iridium satellites. Testing efforts focused on the device's STL PNT capability. The two objectives of testing were positioning performance and independence of systems; robustness to interference was not evaluated. The focus of the analysis was from an on-road data collection for characterization of positioning and timing performance of the SHOUT tsA capability.

3.3.2.2 Test Description and Setup

Two NAL Research SHOUT tsA units were used in the testing efforts, with one unit integrated into a USDOT van used as a mobile collection platform. The SHOUT tsA is a hand held device weighting about a pound with rough dimensions of 5" x 3" x 1.25", plus a short, cylindrical Iridium antenna protruding from the top (see Figure 3-42). The antenna can be removed to support input from alternate sources. The device can be configured through a touch screen or application and uses a USB port for charging. The output is a 1PPS signal output through a built-in HD-BNC port.

[26] For additional information about the Satelles STL system, see https://satelles.com/.

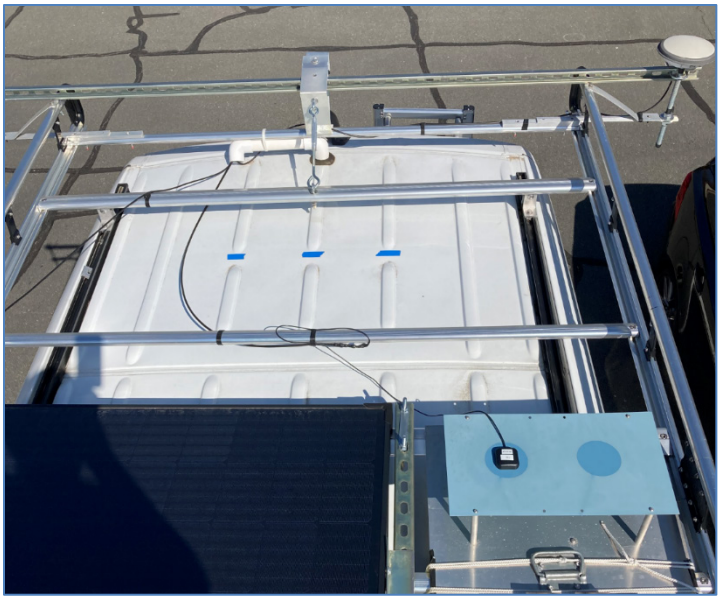
(Source: Volpe Center/Zeta Associates)

Figure 3-42. SHOUT tsA Satellite Tracker

The SHOUT tsA unit was mounted in the test van interior (see Figure 3-43) and the native antenna replaced with a TAOGLAS IAA.01 magnetic-mount Iridium patch antenna affixed to a metal panel on the roof of the test van, elevated with standoffs above a mounting fixture secured to the roof rack (see Figure 3-44). The serial connection for data collection from the SHOUT unit was via a USB cable to a laptop. The 1PPS output was connected to a circuit used for timing measurements, as diagramed in Figure 3-45, which was mounted in a rack in the van. This configuration allowed data and timing collection for STL operations suitable for characterization of its dynamic positioning capability.

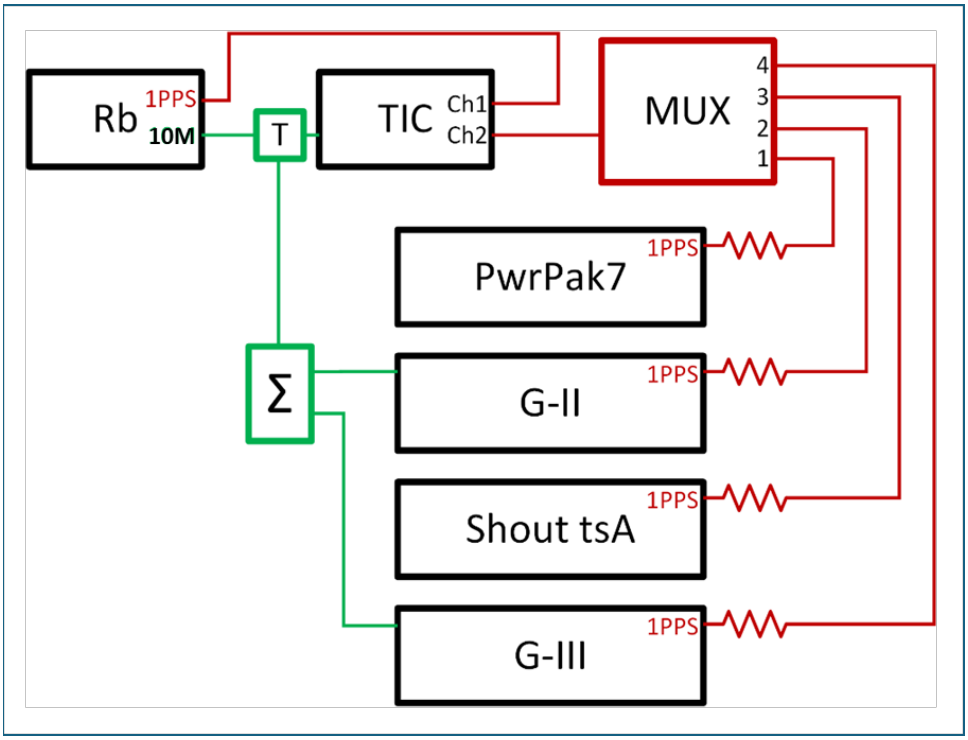
(Source: Volpe Center/Zeta Associates)

Figure 3-43. SHOUT tsA Mounted inside the Test Van



(Source: Volpe Center/Zeta Associates)

Figure 3-44. Iridium Antenna on Elevated Plate and Cable Routing



(Source: Volpe Center/Zeta Associates)

Figure 3-45. Circuit for Timing Offset Measurements from Four Receivers

The GNSS positions used for "truth" in this analysis were provided by a dual-antenna NovAtel PwrPak7D-E2 receiver (PwrPak7) (the same GNSS device installed aboard the *Antares*) integrated into the test van.

The PwrPak7 employed a TerraStar-C Pro PPP service, which offers multi-constellation GNSS corrections to support highly accurate positioning measurements. In addition to its GNSS capabilities, the PwrPak7 includes an IMU. Integration of this receiver included measurement of GNSS antenna offsets from the IMU center with respect to the vehicle coordinate reference frame as well as steps for rotational calibration of this reference frame with the IMU orientation. This integration provided for real-time fusion of GNSS and IMU measurements during mobile collection. Further, the receiver allows the positioning solution to be translated to a user antenna at another location on the vehicle.

Using measurements from the center of the IMU to the Iridium antenna, this configuration provided for highly accurate position outputs from the PwrPak7 suitable for truth and referenced to the SHOUT antenna location for direct comparison with SHOUT position outputs. The accuracy of the physical measurements to the Iridium antenna were confirmed by taking a separate GNSS collection from an antenna temporarily set in place of the Iridium antenna and by comparing these GNSS positions from this location with the PwrPak7 positions translated to this location.

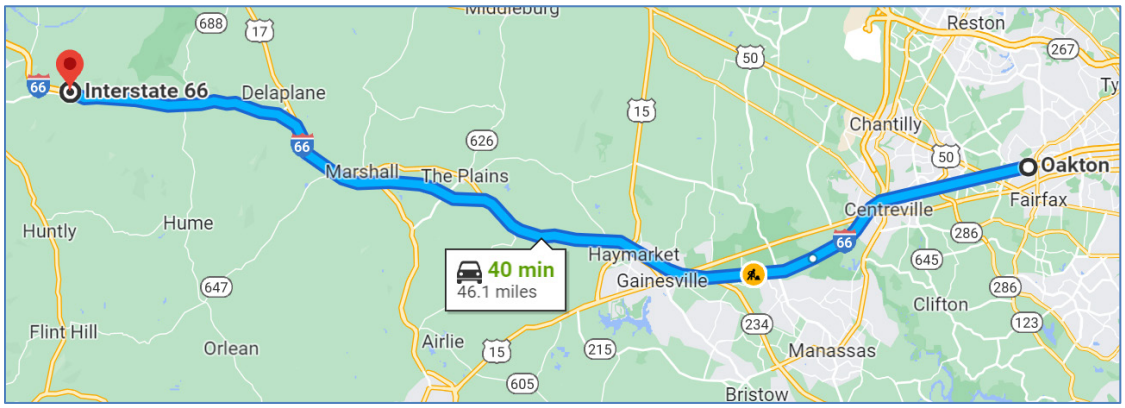
3.3.2.3 Device Operation

The SHOUT tsA unit is a dual-system receiver with respect to PNT (i.e., GNSS and STL), but the two PNT systems operate independently and cannot be operated simultaneously. Instead, the device's PNT mode must be selected to be either GNSS or STL, and all screen and serial outputs only provide content related to the selected mode. A user must select a system, monitor its performance, and manually change the mode should the selected system be deemed degraded. At every change of mode to STL, the system goes through a cold start, with time reported as zero over multiple epochs until timing information is obtained via received bursts. Similarly, no position is reported initially, and even when position is first reported, it takes time until the reported accuracy of the position converges to an acceptable range. (Characterization of the wait times for acquisition and convergence was not part of the Pilot Program, and no testing was done on the SHOUT tsA GNSS positioning performance.)

An operational consideration for the SHOUT tsA relates to mode switching and the time required for acquisition and convergence. With no capability for simultaneous operation of the two PNT systems, and the cold start period encountered when switching to STL mode, any decision to change mode to STL due to degraded GNSS would require waiting through acquisition and convergence time to get PNT data. Rather than establishing an inherent waiting period at the moment when reliable PNT is most required, the preferred approach would be to operate the SHOUT tsA in STL mode continuously, while monitoring some other source of GNSS PNT data, so that the STL position would be immediately available. In STL mode, the SHOUT tsA has three options for geolocation mode: Static, Dynamic, and Auto. The device includes a motion sensor and when in Auto geolocation mode reports a basic status for this sensor indicating whether the device is in motion. The data analyzed in this document was collected with the SHOUT tsA operating in Auto geolocation mode.

3.3.2.4 *Data Analysis and Results*

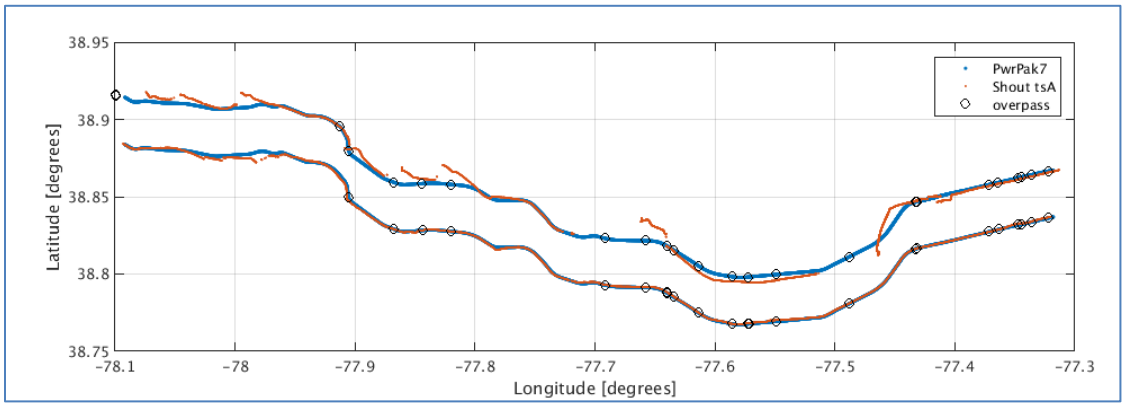
The data collection scenario selected for analysis was a highway drive that offered open sky conditions with few obstructions. This collection was initiated in the late evening of December 11, 2021. The route started and ended in a parking lot at Zeta Associates in Fairfax, VA. The route consisted of an out-and-back drive on an interstate highway, starting westbound on I-66 from Exit 60 to Exit 13 and back; approximately 46.1 miles each way (see Figure 3-46). The route was chosen to represent, as best as possible, the sky view and dynamics of an ocean voyage, with some recognized differences: a higher speed of travel, more frequent turns, and potential satellite signal obstructions (e.g., overpasses).



(Source: Volpe Center/Google Maps)

Figure 3-46. Map of Complementary PNT Interstate Test Drive

Position data from the collection are shown in Figure 3-47 on a rectangular grid for latitude and longitude. The blue track represents the position from the PwrPak7, indicating the true ground track of the van along the test route. The upper track in the figure is the first (westbound) half of the route, while the lower track is the second (eastbound) half of the route, shifted southward by 0.03 degrees (for display purposes only). On-ramp, off-ramp and turn-around segments are omitted in the figure. In comparison with the blue track, positions reported by the SHOUT tsA unit (shown in red) include some large diversions, especially on the westbound (upper) track and at the beginning of the eastbound (lower) track.

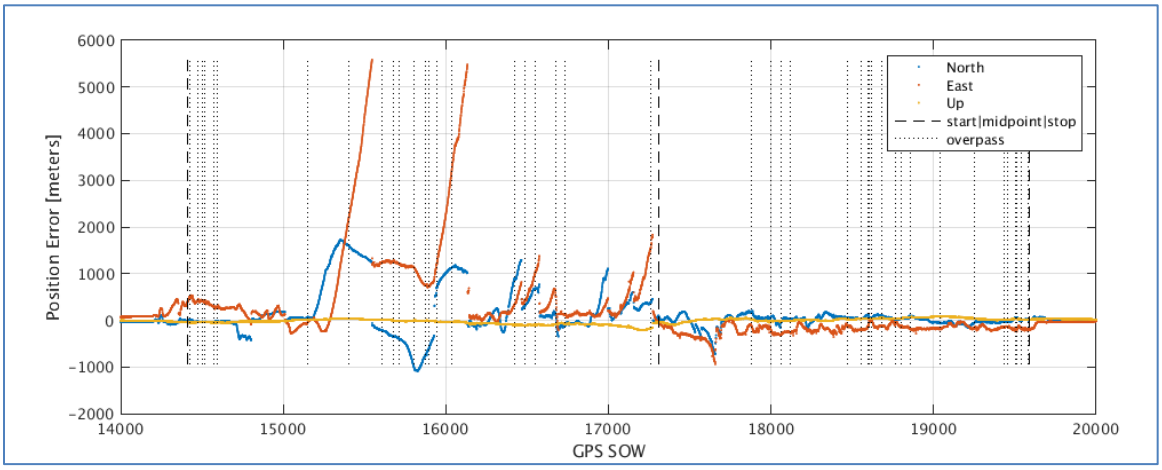


(Source: Volpe Center/Zeta Associates)

Figure 3-47. SHOUT Positions with True Ground Track along Interstate Route Showing Overpasses

The locations of overpasses are indicated in Figure 3-47 with black circles, and were encountered on both the outbound and inbound track. The excursions appear to have no relationship to the overpasses, with only one apparent coincidence of a diversion start and crossing under an overpass. This is as expected for burst data, where the momentary obstruction of an overpass for travel at highway speeds is not expected to impede the reception of many, if any, data bursts. Further study of the route may reveal additional obstructions along the highway, such as tall buildings obscuring some lower-angle views of the sky, which could help to explain the diversions.

The data from the SHOUT tsA units were directly compared with GNSS/IMU truth positions from the PwrPak7, referenced to the Iridium antenna location. The error in the SHOUT position estimates over the duration of the interstate drive are shown in Figure 3-48 in units of meters in the north, east, and up directions. The outbound and inbound segments of the drive are delimited with heavy black vertical dashed lines, and the overpasses are represented with dotted vertical black lines.



(Source: Volpe Center/Zeta Associates)

Figure 3-48. Position Errors along Interstate Route Delimited for Outbound and Inbound Segments

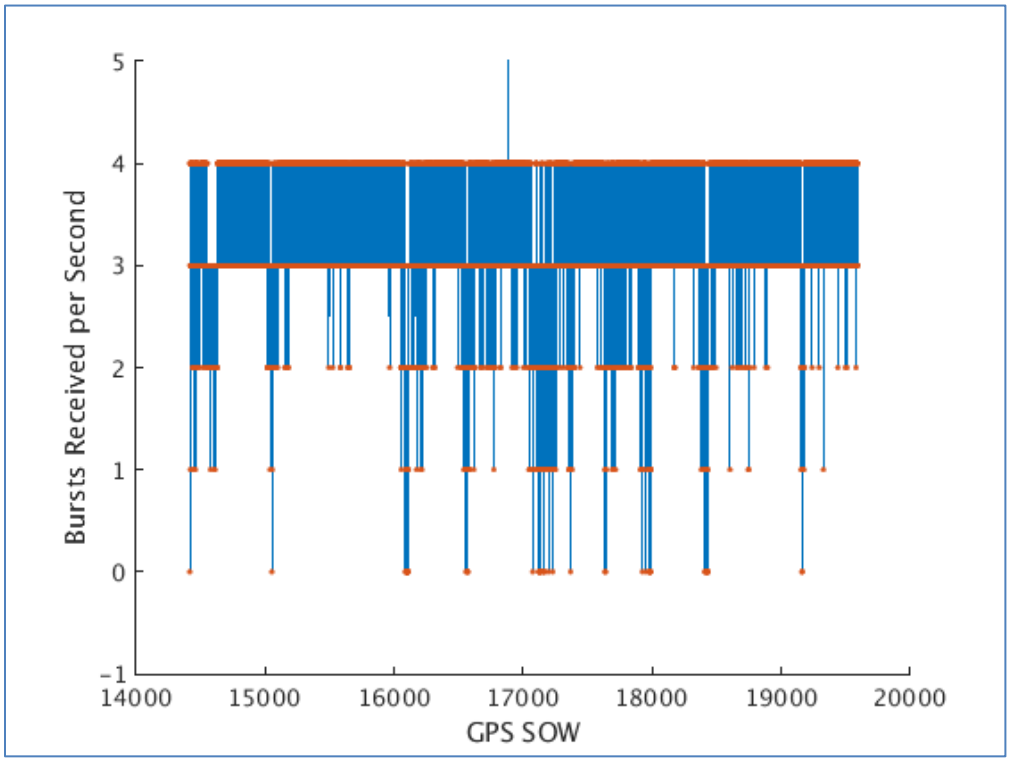
The figure draws attention to the contrast between performance for the inbound and outbound segments, with errors primarily on the outbound segment showing large excursions in SHOUT position relative to truth position. Two excursions in longitude (east) exceed five kilometers, with additional excursions along both longitude and latitude (north) of up to two kilometers. Considering the primary direction of travel for this route was from east-to-west and back, the larger excursions for longitude may be sensible if SHOUT positioning error tends to exhibit itself as lagging position updates.

Ignoring the large excursions, the pattern of position errors may imply a delay in SHOUT position estimates with much of the longitude error being positive (eastward) for the west-traveling outbound segment and negative (westward) for the east-traveling return segment. The analysis was completed without access to documentation about the SHOUT data outputs. As such, the label/purpose for only a subset of data fields in the serial output message are understood, as verified through matching value

changes in the message fields with labelled output values shown within status messages on the touchscreen.

3.3.2.4.1 Total Bursts, Maximum C/N_0, and Number of Satellites

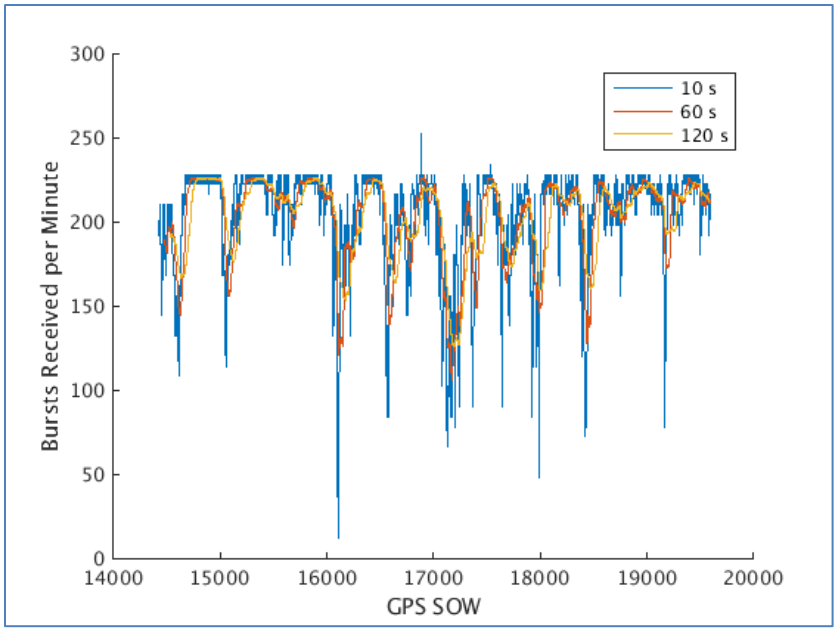
SHOUT output data includes the total number of data bursts received. When collecting in STL mode, this field increments at successive 1-second epochs as additional bursts are received. Figure 3-49 shows the first difference of this data element over the period of the interstate test drive to give a sense of burst rate. The figure shows three or four bursts received per second for most epochs. The burst rate never exceeds four bursts in any one-second interval. (The single value shown above four is an artifact corresponding to a two-second difference due to exactly one missed epoch during this period.



(Source: Volpe Center/Zeta Associates)

Figure 3-49. First Difference of Total Bursts for Raw Burst Rate per 1-Second Epoch

Figure 3-50 shows the burst rate re-computed by differencing the number of bursts received over larger intervals of 10, 60, and 120 seconds, and scaled appropriately to represent the burst rate per minute. This figure appears to reveal a maximum burst rate. In some periods the burst rate decreases significantly, while in other periods the burst rate rises to plateau at a maximum value of ~225 bursts per minute for an extended time, but it never moves beyond this value. This rate corresponds to a rate of 3.75 bursts per second, consistent with Figure 3-49.



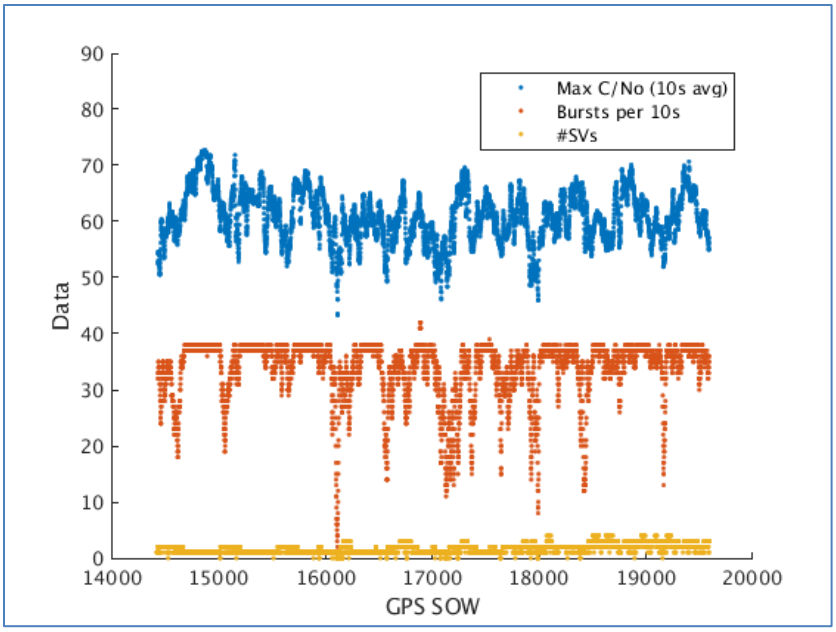
(Source: Volpe Center/Zeta Associates)

Figure 3-50. Burst Rates Computed from Total Bursts Using Various Time Intervals

Two additional SHOUT output data fields give "Max CNO" and "Num of Sats." These are assumed to represent the maximum value of carrier to noise density ratio (C/N_0) measured over all bursts received since the last epoch, and the total number of satellite vehicles (SVs) from which any burst was received since the last epoch, respectively. The C/N_0 field usually reports with values between 40 and 80, but occasionally takes on a value of zero, presumably indicating that no C/N_0 value was measured during the interval. Parallel with this, the field for the number of satellites usually reports a value of 1 to 4, but also occasionally takes on a value of zero. There appears to be a perfect correspondence between the zero values of these two fields, i.e. whenever one field is zero, the other is also zero.

In contrast to the C/N_0-SV correspondence, the number of bursts received can at times be observed to increase at epochs where the C/N_0 reports a zero value, and can also at times be observed to remain constant at epochs when the C/N_0 reports a non-zero value. While not fully understood, these inconsistencies may imply a difference in definition between a burst received and a valid C/N_0 measurement of a burst, or a minor offset in the period of support for the reported values. Regardless of the mismatch at the low level, burst rates and C/N_0 do appear to be highly correlated, as can be seen when the data is plotted.

In Figure 3-51, the burst rate is computed over intervals of 10 seconds and the C/N_0 is averaged over a period of 10 seconds, with zero values excluded. The number of satellites is also plotted, using the raw value. In this figure, burst rates appear to fall from the theorized maximum value during periods when the average of the maximum C/N_0 is lower than a value of ~60. In principle, C/N_0 levels below some threshold for reception would be expected to cause degraded burst reception resulting in fewer received bursts.



(Source: Volpe Center/Zeta Associates)

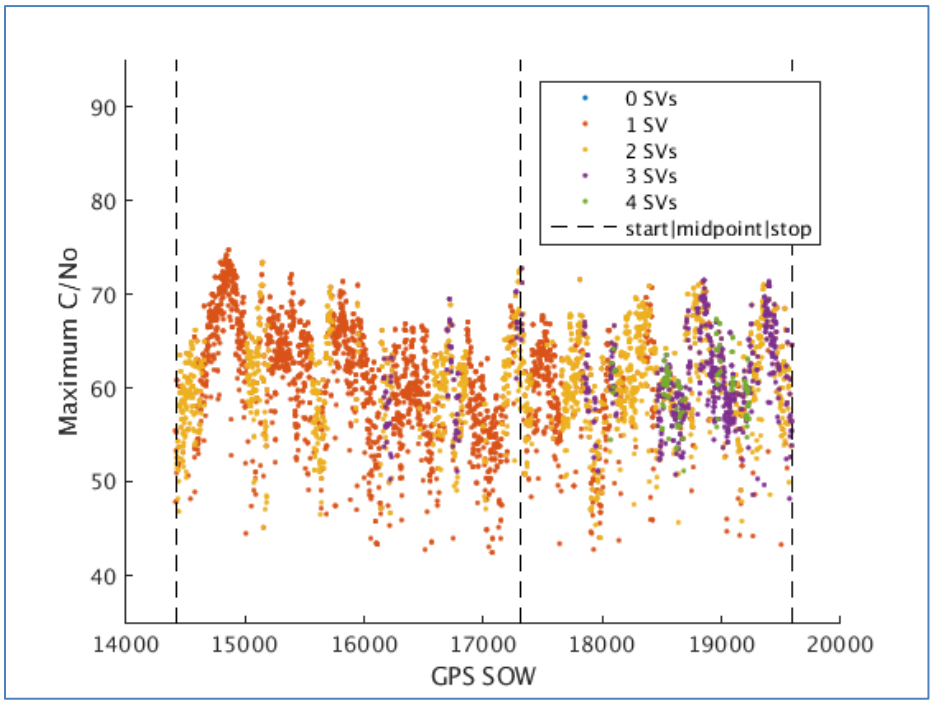
Figure 3-51. Averaged Maximum C/N_0, 10-Second Burst Rate, and Number of Satellites

The number of satellites in Figure 3-51 generally varies from one to four with a few periods indicating zero satellites. For a maximum metric such as C/N_0, an output value is expected to either remain the same or increase when additional observations are available; however, for the left third of the plot whenever the number of satellites increases from one to two, the C/N_0 appears to degrade (as does the burst rate). If the first satellite was the same throughout, this would imply its C/N_0 is degrading when bursts are received from the second satellite, which does not seem sensible. A better explanation is that the periods with two satellites correspond to one satellite setting while another is rising. During these periods, both satellites—being at lower elevation—have degraded C/N_0, thus causing the net degradation in the maximum metric. During the same period, the burst rate suffers along with the C/N_0 for an unintuitive result that fewer bursts are received when the number of satellites increases; however, consistent with the explanation for C/N_0, reduced burst rates may be expected when bursts from both satellites are being received at C/N_0 values pushing down against a reception threshold.

Burst rate was observed to plateau without exceeding a rate of ~225 bursts per minute. The interest in establishing whether the system or device operates with a maximum or nominal burst rate is in understanding whether dips in the burst rate should be interpreted as degradations to burst reception. With consideration for the number of satellites in Figure 3-51, it can be observed that the maximum observed burst rate is achieved for a single satellite operating at a high C/N_0, and that this rate is not exceeded even when bursts are being received by as many as three or four satellites as shown on the right side of the figure. This supports the notion of a maximum rate.

This theory is still inconclusive, given the evidence of reduced burst rates from surmised low-elevation satellites, coupled with insufficient insight into the state of the constellation from device outputs,

especially when multiple satellites are in view. Figure 3-52 shows a plot of raw maximum C/N_0 over the interstate test drive with colored data points indicating the number of observed satellites. Some periods with as many as three or four satellites still suffer with a degraded maximum C/N_0 relative to other periods with fewer satellites, implying several satellites are in view but reception from each is at low C/N_0 over those periods. A more conclusive indication that a maximum burst rate exists would be a period of time with both a large number of satellites and a consistently high value for maximum C/N_0.

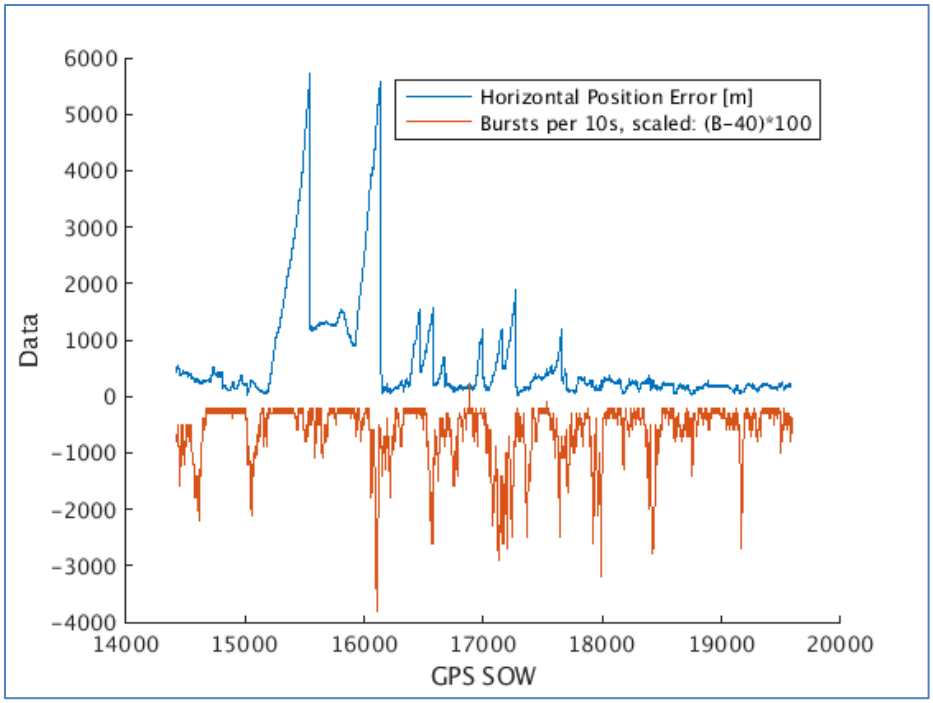


(Source: Volpe Center/Zeta Associates)

Figure 3-52. Maximum C/N_0 Values and Corresponding Number of Satellites

3.3.2.4.2 Uncertain Cause of Excursions

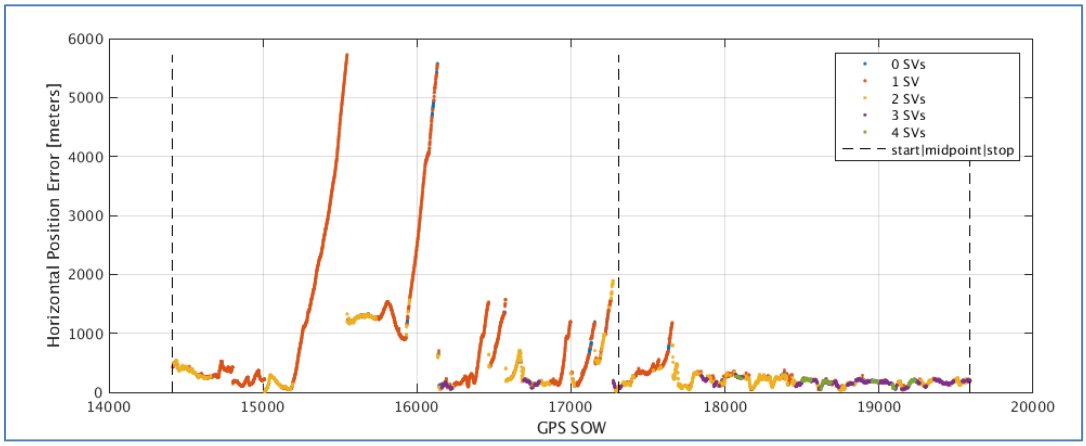
Figure 3-53 shows the horizontal error (computed from the east and north errors of Figure 3-48) aligned in time with the burst rate computed with a 10-second interval. (The burst rate is scaled and shifted vertically in the plot to appear below the horizontal error for ease of comparison.) The two largest position excursions appear to be unrelated to the periods of degraded burst rate. The second large excursion begins before a period of heavily degraded rate, yet re-converges during the degraded period. Of the other excursions, only one, in the middle of the plot, appears to align well with a degraded burst rate. The comparison for C/N_0 is similar given the correlation observed earlier (Figure 3-51) between C/N_0 and burst rate. It appears the burst rate and C/No values encountered during the interstate drive had little to do with the periods of poor positioning performance.



(Source: Volpe Center/Zeta Associates)

Figure 3-53. Horizontal Position Error versus Scaled 10-Second Burst Rate

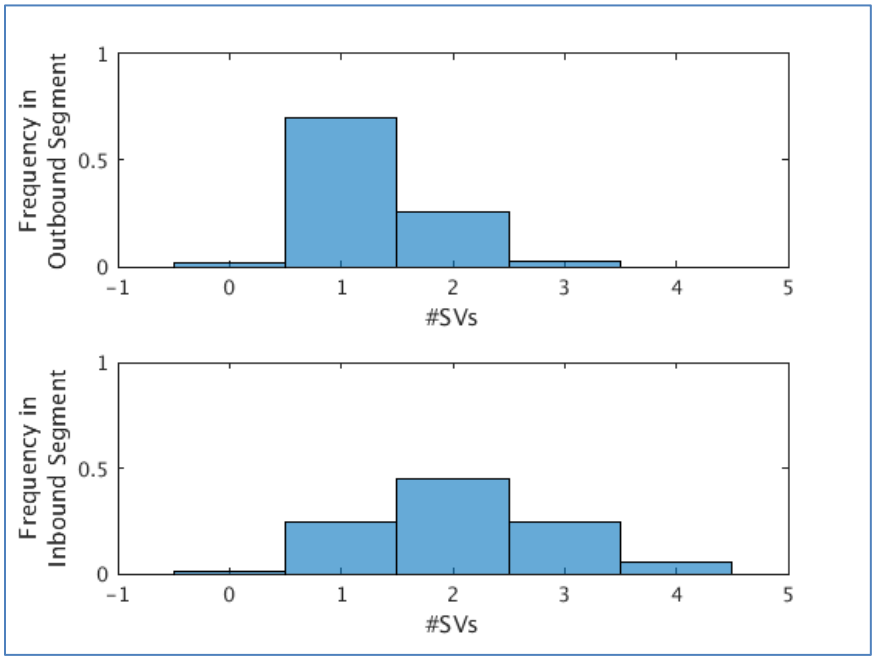
In contrast, the position excursions do appear to correlate well with the number of observed satellites. In Figure 3-54, the horizontal error is displayed using colored markers for each epoch to indicate the number of observed satellites, with the outbound and return segments delimited as in earlier plots. This shows that the number of observed satellites is generally smaller for the outbound segment, with one or two satellites observed for most epochs, while two to four satellites are observed for most of the return segment. Further, most of the excursions correspond to periods of just one satellite, and no excursions occur for periods of three or more satellites.



(Source: Volpe Center/Zeta Associates)

Figure 3-54. Horizontal Position Error versus Number of Observed Satellites

In the return segment, after a single excursion during a period with only one observed satellite, the remainder of the segment suffers no additional excursions while generally tracking two or more satellites. Position performance seems more likely to degrade when the number of satellites hovers between one or two or fewer, and less likely when two or more satellites are sustained. With the interstate test drive collection divided between outbound and return segments, the frequency of the number of satellites observed is shown in Figure 3-55. If the first 400 seconds of the return segment (to include the single excursion) were lumped in with the outbound segment, the contrast in observed satellites would be even more pronounced than in Figure 3-55.



(Source: Volpe Center/Zeta Associates)

Figure 3-55. Distributions of Number of Satellites in Outbound and Inbound Segments

The examination of known obstructions, burst reception rates, and burst C/N_0 have not shown any strong evidence of causality for position excursions, while having a reduced number of observed satellites does appear to provide the conditions for large position excursions to occur. The difference between segments for the number of observed satellites may be a simple matter of reduced satellite coverage, but this is uncertain without a known source for Iridium ephemeris information.

With the out and back format of the interstate test drive, the two segments do have some additional comparative value toward answering this question. Outside of the data observations, the segments were comparable in the sense that they traversed the same basic route, targeted a similar maximum speed, and were subject, with minor exceptions, to the same known overpass obstructions. The segments also had some differences including time period of travel, lanes of travel, van/antenna orientation, and traffic dynamics, not all of which expected to have much significance for positioning performance.

The period of travel differs in the sense that the inbound segment took place directly after the outbound segment. The primary significance is this allows for a difference in the state of the Iridium constellation in terms of numbers and positions of satellites in the sky for the distinct durations of the two segments. The lanes of travel differ in that the outbound segment traversed the lanes of I-66 West, while the inbound segment traversed the lanes of I-66 East. The separation distance between the east- and west-bound lanes is generally not large and is not expected to have any bearing on performance except as it may relate to proximity to obstructions along the route that may reduce the number of satellites in view. The orientation of the van and the consequent orientation of the Iridium antenna differ by roughly 180 degrees between the segments. For the antenna, this is not expected to have any bearing on performance, as the antenna is indicated to have reasonably good radial symmetry.

The traffic dynamics did differ somewhat between the two segments, as implied by the longer duration represented for the outbound segment (several minutes of slower traffic, but never stopped). In general terms, vehicle dynamics may be expected to have some effects on positioning performance. An assessment of any relationship between the vehicle dynamics and the position excursions may be worthwhile, but has not been investigated in this effort.

The data supports differences in the constellation as the primary reasons for reduced satellites on the outbound segment and related position excursions, but leaves some space for additional factors including differences in obstructions and vehicle dynamics along the segment. An additional collection that eliminates factors of obstruction and dynamics would be helpful for better determination of causes for reduced satellites and position excursions. The proposed collection would be from a static location with an open view of the sky over a long duration, with the SHOUT tsA operating in Dynamic geolocation mode to ensure algorithm behavior comparable to dynamic collections.

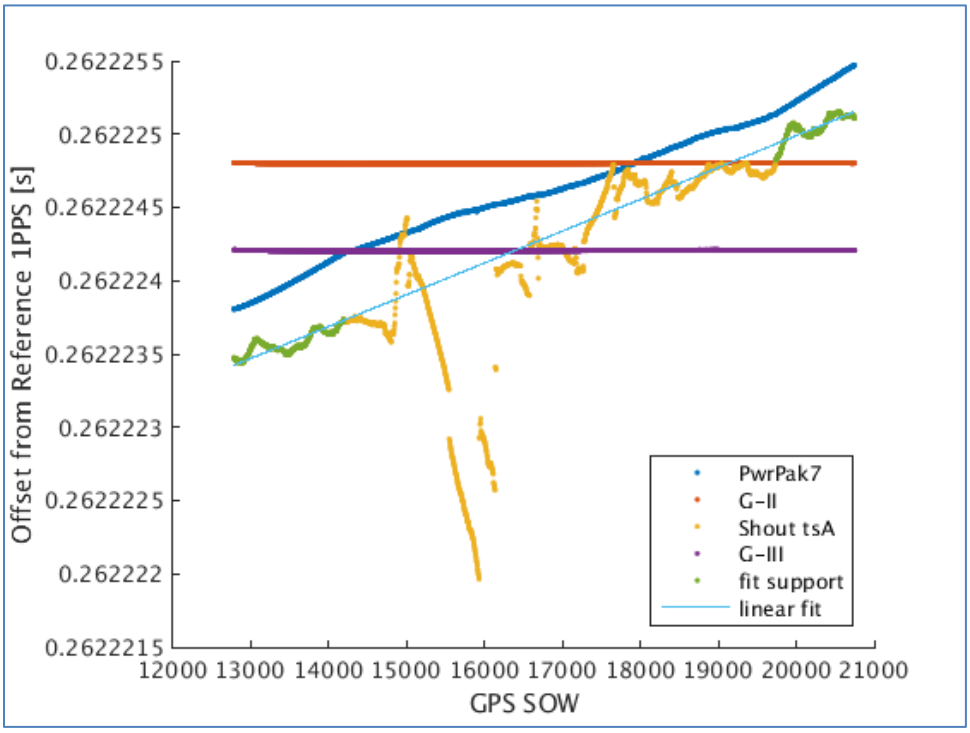
3.3.2.4.3 Timing Measurement and Non-Excursion Statistics

Timing measurements were also collected from the SHOUT tsA unit during the interstate test drive. In particular, the 1PPS output of the SHOUT tsA was measured relative to the 1PPS pulse of a free running Rubidium frequency standard (Rubidium) using a timing interval counter (TIC). Similar measurements were also taken for the PwrPak7 and for two other reference receivers installed in the van. This was done in an automated fashion by using a programmable RF switch as a multiplexer to step through the four receiver 1PPS sources for sequential presentation for measurement at the TIC input (refer to previous Figure 3-45).

The time interval between the Rubidium pulse and the receiver pulse was reported at each successive second, along with a receiver designator and a clock time from the control computer before stepping to the next receiver. This yielded a time-tagged, timing offset measurement for each receiver for every four seconds. Rubidium pulsing was initialized with a healthy offset from receiver pulses, to avoid any race conditions and ensure adequate setup time between successive measurements. Aside from these

purposes, the magnitude of this offset was arbitrary. Instead, the key observation from these measurements is the change in receiver timing offset over time, for any given receiver.

Figure 3-56 shows the raw measurements for the four receivers over the full duration of the collection to include the stationary periods before and after the drive. The two reference receivers, show in red and purple, hold a near steady offset with the Rubidium, while offsets for the PwrPak7 in blue and the SHOUT tsA in yellow/green trend upward over the collect. This contrast relates to a distinction in the way time is estimated for receivers.



(Source: Volpe Center/Zeta Associates)

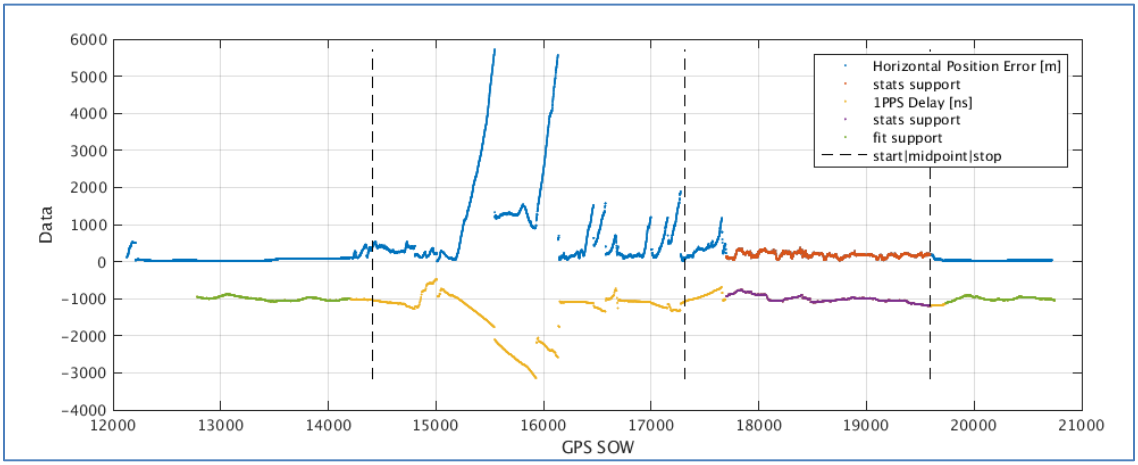
Figure 3-56. Raw Data from 1PPS Timing Collection for Four Receivers

The reference receivers accept a 10 MHz reference, in this case from the Rubidium, and generate their 1PPS output signals based on this input timing reference after an initial estimate from a GPS (and thereafter separately estimating GPS timing relative to the 1PPS). In contract, the 1PPS outputs for the PwrPak7 and the SHOUT tsA continuously represent estimates of time from their respective constellations. The difference in slope is expected and reflects a minor frequency error in the Rubidium, of ~0.2 parts per billion.

For the timing offset measurements to be useful, the Rubidium frequency error must be removed. This was done for the SHOUT tsA by first computing a least-squares regression line using only the segments of SHOUT data from before and after the drive when the van was stationary, then evaluating the line at the times of all SHOUT data points, and finally subtracting these line values from the corresponding SHOUT data appoints to remove the slope of the line, which slope represents the Rubidium error. The

computed regression line is shown in cyan in Figure 3-56, with the SHOUT data supporting the computation shown in green.

The adjusted SHOUT data after removing the estimated Rubidium error is shown in yellow/green/purple in Figure 3-57 (with a 1,000 ns offset for display purposes). In this figure, the data supporting the line fit, again shown in green, now straddles a horizontal gridline thus confirming the slope has been removed. With the slope removed, the gridline itself is now the least-squares fit of the adjusted SHOUT timing data from periods when the van was stationary. Taking this gridline as truth for time (i.e. zero delay from true time), the largest time excursion, an advance, has a magnitude of more than 2,000 ns.



(Source: Volpe Center/Zeta Associates)

Figure 3-57. Horizontal Error and De-trended Timing Offset for Interstate Collection

Figure 3-57 also includes the horizontal position error from earlier, revealing an unmistakable correlation between position and timing excursions. Further, the performance distinction observed earlier for position error between outbound and inbound segments is also clear in the timing data. As with position, most timing excursions appear in the outbound segment, with a single additional excursion in the early part of the inbound segment. After this, the inbound segment continues to its end with no additional timing excursions. The substantial period with no position or timing excursions is evidence that the SHOUT tsA can operate for periods with reasonably good position and timing performance. Figure 3-57 highlights this sub-period of the inbound segment in red for the position data and in purple for the timing data.

To quantify performance for the superior non-excursion period, statistics for the positioning and timing error for this period are presented in Table 3 and Table 4, respectively. The notion here is to characterize the best-sustained performance of the device, since it is evident this performance can be achieved under some conditions, with the understanding that the conditions causing the poorer performance—with large position and timing excursions—are not fully understood. If the conditions causing poor performance are shown with some frequency in the expected operating environment, this may lead to a conclusion that the device is not suitable.

Alternatively, if the conditions can be avoided in the expected operating environment, then the statistics presented in the tables are a useful representation of device performance. The mean longitude error in Table 3 indicates reported van positions were on average more than 160 meters to the west of truth during the eastbound sub segment, yet the longitude error varied with a standard deviation of only ~70 meters. The westward bias for eastward travel implies a delay in SHOUT tsA position estimates of more than five seconds, considering highway speeds along a trajectory not fully eastward. The smaller and positive latitude error also supports the observation of delay in that a smaller portion of the van motion was north/south with some motion in both directions, yet net motion was southward to produce delayed position on average to the north of truth for a smaller positive error, consistent with the table. As further evidence of a delay, a comparison of Figure 3-47 and Figure 3-48 for this segment show primarily positive latitude errors when the van trajectory is southward and negative errors when the van trajectory is northward.

Table 3 . Position Error Statistics for Non-Excursion Period (in Meters)

Parameter	Latitude	Longitude	Horizontal	Vertical
Mean error	24.1	-163.8	180.7	27.5
Standard deviation error	67.9	69.9	65.2	27.7
Root mean square error	72.1	178.0	192.1	39.0
Mean absolute error	60.2	164.3	180.7	31.7

(Source: Volpe Center/Zeta Associates)

Timing statistics shown in Table 4 do not include a mean error or other statistics that depend on mean error, because in using a free-running Rubidium—to allow observation of receiver timing changes without impairment due to any disciplining imposed on the reference—no absolute time reference was used. The standard deviation and span of time offset observations provides a sense of timing performance, with de-trended timing offset varying for a standard deviation of ~94 ns and walking over a span of ~435 ns from maximum to minimum offset during the non-excursion period.

Table 4. Timing Statistics for Non-Excursion Period

Parameter	Time Offset
Standard deviation	94.3 ns
Span of time offset	435.4 ns

(Source: Volpe Center/Zeta Associates)

4. Conclusions and Recommendations

The USDOT's PNT Profile Pilot Program has produced significant achievements in all four components that EO 13905 specifies for improving operational resilience through responsible use of PNT. As identified in EO 13905, the PNT profiles are intended to:

- Enable the public and private sectors to identify systems, networks, and assets dependent on PNT services;
- Identify appropriate PNT services;
- Detect the disruption and manipulation of PNT services; and,
- Manage the associated risks to the systems, networks, and assets dependent on PNT services.

The Pilot Program was focused on operations in the maritime environment and provided findings and recommendations along each of the four components by:

1. Identifying specific shipboard systems aboard MARAD RRF vessels that use or form PNT data—through stakeholder outreach, fleet inventories, and individual ship surveys.
2. Identifying both existing and complementary PNT data sources that are suitable for the maritime operating environment—through operational testing and data collection aboard both stationary and active ships.
3. Detecting the disruption and manipulation of PNT services in a marine environment—through successful testing of shipboard PNT equipment in both laboratory and real-world operational settings, under normal and disrupted/manipulated conditions. The primary evaluation in the study leveraged the GET-CI event as the environment for testing the baseline shipboard GPS equipage with and without added protective capability.
4. Providing MARAD with a framework to manage the associated risks to the shipboard systems, networks, and assets dependent on PNT services—by identifying 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. Both protection and augmentation solutions were evaluated as part of the Pilot Program with commercial products and services, specifically the Novatel Hexagon/GAJT-410ML for protection (as well as a potential detection device) and the SHOUT/Satelles STL tsA product for augmentation.

The basis for the Pilot Program was the NIST Foundational PNT Profile specified in NISTIR 8323. As a Pilot Program, the team sought to develop actionable areas for increasing shipboard PNT resilience. The central findings from the Program team were developed through the five NISTIR 8323 Framework Core

functions. Addressing those five functions led to three actionable fronts for managing operational risk from PNT disruption and/or manipulation:

1. Know your risks (Section 3.1, PNT Vulnerabilities and Threat Identification)
2. Protect your systems (Section 3.2, Protective Solution)
3. Incorporate diversified sources of PNT signals (Section 3.3, Detect, Respond, and Recover Capabilities of Protective Solution)

In alignment with the actionable objective of the Pilot Program, the findings above 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 results provided in Section 3 demonstrate that these solutions should be further evaluated with respect to the full set of operational requirements for a platform such as vessels of the Ready Reserve Force. However, from the PNT Profile perspective, the USDOT Pilot Program findings lead to two 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 paired with the GAJT nulling antenna, the GPS receiver will be unable to demodulate the spoofing data therefore protecting the receiver from the vast majority of both signal and data spoofing attacks. This solution, if desired, does have the capability to serve also in a detect-and-characterize function (power and direction of arrival) on interfering signals. Further, a dual antenna/receiver pair can be used to detect a spoofing attack through self-differential means.
2. Augment shipboard equipage in the RRF with LEO-based timing and, potentially, positioning technology. Solutions such as the SHOUT/Satelles STL service can be added with minimal integration (human in the loop procedures) to provide both a check of GPS-based PNT outputs and a complementary space-based PNT source for ship management equipage.

While these recommendations 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 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.

5. References

Bhatti, Jahshan and Todd Humphreys. "Hostile Control of Ships via False GPS Signals: Demonstration and Detection." *NAVIGATION*, 64:1, pp. 51–66. https://doi.org/10.1002/navi.183.

Government Accountability Office. "Defense Transportation: DOD Can Better Leverage Existing Contested Mobility Studies and Improve Training" GAO-21-125. Washington: Government Accountability Office. https://www.gao.gov/products/gao-21-125.

GPS World Staff. "Norway proves Russian interference." *GPS World*, March 20, 2019. https://www.gpsworld.com/norway-proves-russian-interference/.

Ilcev, Dimov Stojce. "Introduction to Inmarsat broadband global area network for mobile backbone networks." *Bulletin of Electrical Engineering and Informatics*, 9:2, April 2020, pp. 843–852. https://doi.org/10.11591/eei.v9i2.2136.

John A. Volpe National Transportation System Center. 2016. GPS Dependencies in Transportation. Washington: U.S. Department of Transportation. August 31, 2016. https://rosap.ntl.bts.gov/view/dot/12386.

John A. Volpe National Transportation Systems Center, "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," Washington: U.S. Department of Transportation, April 29, 2001. https://rosap.ntl.bts.gov/view/dot/8435.

John A. Volpe National Transportation Systems Center. Complementary PNT and GPS Backup Technologies Demonstration Report, January 2021. Washington: U.S. Department of Transportation. https://rosap.ntl.bts.gov/view/dot/55765.

Maritime Administration. "MSCI Advisory 2020-016, Various GPS Interference." MARAD Maritime Security Communications with Industry web portal, September 22, 2020. https://www.maritime.dot.gov/msci/2020-016-various-gps-interference.

Metrick, Andrew and Kathleen H. Hicks. 2018. Contested Seas: Maritime Domain Awareness in Northern Europe. Washington: Center for Strategic and International Studies. March 2018. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180328_metrickhicks_contestedseas_web.pdf?aasgbcystp_dve22m_uodvujvvs0_mkm.

National Institute of Standards and Technology. "Cybersecurity Framework." Gaithersburg: National Institute of Standards and Technology, web, no date. https://www.nist.gov/cyberframework.

National Institute of Standards and Technology. "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.

Resilient Navigation and Timing Foundation. "GPS Spoofing Patterns Discovered" (press release). Alexandria: Resilient Navigation and Timing Foundation, September 15, 2017. https://rntfnd.org/wp-content/uploads/GPS-Spoofing-Patterns-Press-Release.1-26-Sep-17-RNT-Foundation.pdf.

Shepard, Daniel, Jahshan Bhatti, and Todd Humphreys. "Drone Hack." *GPS World*, August 2012, pp. 30–33. https://radionavlab.ae.utexas.edu/images/stories/files/papers/drone_hack_shepard.pdf.

U.S. Department of Transportation. "Virtual Workshop on GPS Jamming and Spoofing in the Maritime Environment, Agenda and Presentation." Washington: U.S. Department of Transportation, last updated December 9, 2020. https://www.transportation.gov/pnt/agenda-virtual-workshop-gps-jamming-and-spoofing-maritime-environment.

U.S. Navy, Chief of Naval Operations. OPNAV Instruction 3501.199C, "Required Operational Capabilities (ROC) and Projected Operational Environment (POE) for Strategic Sealift Ships to Include the T-AKR Fast Sealift Ships (FSS), Large Medium Speed Ro/Ro (LMSR), Aviation Support Ships (T-AVB), Auxiliary Crane Ships (T-ACS), and Ready Reserve Force (RRF) Dry Cargo Ships." December 17, 2007.

U.S. Navy, Commander, Military Sealift Command. Memorandum, "Military Sealift Command (MSC) Updated Electronic Chart and Display Information System (ECDIS) Operational Requirements and Policy." August 9, 2011.

U.S. President. Executive Order. "Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services, Executive Order 13905." *Federal Register* 85, no. 32 (February 18, 2020), pp. 9359–9361. https://www.govinfo.gov/content/pkg/FR-2020-02-18/pdf/2020-03337.pdf.

Appendix A: Highlights from the U.S. Department of Transportation Workshop on GPS Jamming and Spoofing in the Maritime Environment

SUMMARY REPORT

U.S. Department of Transportation Workshop on GPS Jamming and Spoofing in the Maritime Environment December 3, 2020

As part of the PNT Profile Pilot Program, the U.S. Department of Transportation held an on-line public workshop on December 3, 2020, to discuss GPS Jamming and Spoofing in the Maritime Environment. Over 200 participants attended the session, which was co-hosted by the Office of the Assistant Secretary for Research and Technology (OST-R) and MARAD. The following highlights are provided for informational purposes only. (For further information, see the Federal Register notice 85 FR 75404 at https://www.federalregister.gov/documents/2020/11/25/2020-26120/workshop-on-gps-jamming-and-spoofing-in-the-maritime-environment.)

WORKSHOP AGENDA

1:00 PM	Introductions and Welcoming Remarks	Diana Furchtgott-Roth, Deputy Assistant Secretary for Research & Technology (OST-R), U.S. Department of Transportation
1:10 PM	Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing (PNT) Services, EO 13905	Dr. Seth Jonas, National Security Council (NSC) Representative, Executive Office of the President
1:20 PM	Perspectives on PNT Resiliency for Transportation	Karen Van Dyke, Director, PNT and Spectrum Management, OST-R
1:30 PM	Maritime Perspective: How positioning, navigation, and timing supports maritime applications	Kevin Kohlmann, Director, Office of Safety, Maritime Administration Cameron Naron, Director, Office of Security, Maritime Administration Michael Emerson, Director, Marine Transportation Systems & Senior Arctic Policy Advisor, U.S. Coast Guard
2:15 PM	Break	

2:25 PM	What happens when PNT is denied, disrupted, or manipulated in a maritime environment	Captain William Westrem, APL Maritime Ltd., Master, *President Eisenhower* Captain Richard G. Hoey, Maersk Line, Limited, Master, *Maersk Montana* Dana Goward, President & Director, Resilient PNT Foundation CAPT Michael Glander, Commanding Officer, U.S. Coast Guard Navigation Center
3:15 PM	Options to reduce operational impact and increase PNT resiliency	Cameron Naron Captain William Westrem Captain Richard G. Hoey Dr. Andrew Hansen, OST-R/Volpe Center, Complementary PNT and GPS Backup Technologies Demonstration Team Representative
4:00 PM	Questions/Discussion and Next Steps	
5:00 PM	Adjourn	

1. INTRODUCTION

On December 3, 2020, OST-R and MARAD hosted a workshop on GPS jamming and spoofing in the maritime environment. The workshop focused on the following:

- How positioning, navigation, and timing (PNT) supports maritime applications;
- What happens when PNT is denied, disrupted, or manipulated in a maritime environment; and
- Options to reduce operational impact and increase PNT resiliency.

2. BACKGROUND

On February 12, 2020, the President issued Executive Order (EO) 13905, "Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services." The goal 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. USDOT and other Federal agencies are directed to achieve this aim 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.

USDOT, along with the Department of Energy and Department of Homeland Security, were directed to "develop plans to engage with critical infrastructure owners or operators to evaluate the responsible use of PNT services." Furthermore, these agencies were directed to complete pilot programs within a year of developing their engagement plans, with the results to be used to inform further research, development, and related efforts to strengthen PNT applications.

Given the ongoing events affecting GPS in the maritime environment, OST-R coordinated with MARAD to develop a plan for a pilot program to examine disruption to civil GPS use in the maritime context, particularly on GPS "jamming" and "spoofing." GPS jamming involves the use of a device to block or interfere with GPS signals; spoofing is deceiving a GPS device through fake signals. Both phenomena undermine the reliability of GPS and may have adverse consequences for maritime safety and commerce.

Activities within the USDOT Maritime Administration PNT Resiliency Pilot Program will be conducted through stakeholder engagement and evaluation of complementary PNT technologies that can be adopted to mitigate the impacts during these threat scenarios. The Workshop on GPS Jamming and Spoofing in the Maritime Environment was a key component of the 'stakeholder engagement' aspect of the PNT Resiliency Pilot Program.

3. WHY WE HELD THE WORKSHOP

As part of Executive Order 13905's directive(s) to raise awareness of transportation sector dependencies on PNT services and to engage the public and private sectors to promote the responsible use of PNT services. The workshop's focus was on the maritime sector. However, solutions emanating from this workshop and the subsequent "U.S. Department of Transportation / Maritime Administration PNT Resiliency Pilot Program Final Report" are potentially transferrable to other areas of the transportation sector (e.g., rail, aviation, surface, etc.).

4. WHO PARTICIPATED IN THE WORKSHOP

There was global/international participation, which included seven presenters and 419 registered attendees. A listing of workshop participant countries (29 in all) along with their corresponding organization types is shown below.

> **Country/Region (No. of Attendees):** Afghanistan (1); Australia (4); Belgium (2); Brazil (3); Canada (11); China (1); Cyprus (1); France (5); Germany (9); Greece (6); Hong Kong (4); India (2); Ireland (2); Israel (4); Japan (1); Lithuania (1); Myanmar (1); Nepal (1); Netherlands (1); Norway (8); Portugal (1); Singapore (2); Spain (1); Sweden (5); Switzerland (3); Thailand (1); United Kingdom (16); United States of America (321); and Vietnam (1).
>
> **Organization Type (No. of Attendees):** Academia/educational institution (33); U.S. Federal Government (119); international academia (5); international Government (16); international non-profit (2); international other (9); international private sector/industry (25); media (5); U.S. non-profit (20); U.S. other (20); U.S. private sector/industry (129); U.S. state government or agency (17); and U.S. city/local government or agency (4).

As shown above, the bulk of the participants in the workshop were from the U.S. Federal Government and U.S. private sector/industry sectors accounting for approximately 248 of the total 419 registered

attendees. Workshop presenters along with summaries of their presentations are detailed in the section to follow.

5. SUMMARIZED PRESENTATIONS

TOPIC: Introductions and Welcoming Remarks
Diana Furchtgott-Roth (Presenter)

BIO: Diana Furchtgott-Roth is the Deputy Assistant Secretary for Research and Technology at the U.S. Department of Transportation. She seeks to ensure that research, development and technology activities across the Department and the 40 University Transportation Centers are fully aligned with the Department's areas of interest. She manages the Department's spectrum interests, including GPS and the 5.9 GHz band. She oversees the Bureau of Transportation Statistics, the Volpe National Transportation Systems Center in Cambridge, Massachusetts, and the Transportation Safety Institute in Oklahoma City, Oklahoma.

Prior to joining USDOT, Diana was Acting Assistant Secretary for Economic Policy at the U.S. Department of Treasury. She has been a senior fellow and director of Economics21 at the Manhattan Institute for Policy Research and an adjunct professor of economics at The George Washington University. She previously served as Chief Economist of the U.S. Department of Labor; Chief of Staff of the President's Council of Economic Advisers; and Deputy Executive Secretary of the White House Domestic Policy Council. Ms. Furchtgott-Roth is the author or coauthor of six books and hundreds of articles on economic policy. She received her BA in economics from Swarthmore College and her M.Phil. in economics from Oxford University.

Summary of Ms. Furchtgott-Roth's Presentation
Ms. Furchtgott-Roth's presentation spoke to the purpose of the workshop, "collaboration to move us closer to remedies for the increasingly frequent occurrences of GPS jamming and spoofing." She began by noting the issuance of the Volpe Center's 2001 report, "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," which contained prescient warnings of the vulnerabilities of GPS.

Ms. Furchtgott-Roth noted that GPS provides inputs to a number of critical maritime-related shipboard systems including but not limited to the following: speed; steering; radar & targeting information; under keel clearance (UKC) monitoring; electronic chart display information systems (ECDIS); and the Automatic Identification System (AIS). Also noted in her presentation was that over 50 percent of all casualties at sea occurred due to navigation issues and that GPS interference touches every part of the maritime supply chain, including rail, trucking and port cargo handling (e.g., stolen cargo resulting from GPS jammers to defeat tracking systems). A number of high profile jamming/spoofing-related events were highlighted in her presentation:

- 2017, the Resilient Navigation Timing (RNT) Foundation's discovery of a pattern of GPS spoofing in the Black Sea. Hundreds of ships were reporting their locations in the middle of Russian airports (https://www.maritime-executive.com/article/gps-spoofing-patterns-discovered).
- 2018, the non-profit Center for Advanced Defense Studies (C4ADS) report of almost 3,000 ships affected by GPS jamming and/or spoofing in a two year period (https://www.c4reports.org/aboveusonlystars).
- 2019, North Atlantic Treaty Organization (NATO) military drills in the Baltic Sea involving 29 Nations & 40,000 troops experienced GPS jamming (https://www.reuters.com/article/us-norway-defence-russia/norway-says-it-proved-russian-gps-interference-during-nato-exercises-idUSKCN1QZ1WN).
- 2020, non-profit Sky Truth's documentation of ships in widely dispersed parts of the globe reporting that they were located off the Northern California coast and sailing in circles (https://www.maritime-executive.com/editorials/u-s-dot-marad-convene-panel-on-gps-jamming-and-spoofing).

In response to these threats, Ms. Furchtgott-Roth made note of current and future actions underway by USDOT and its stakeholders:

- The awarding of $2 million in research and technology grants to the newly created (at the time of this workshop) CARMEN UTC (https://utc.engineering.osu.edu/) to work on crucial anti jamming and anti-spoofing technologies;
- Creation of the office of Highly Automated Safety System Center for Excellence (HASS COE) within OST-R to analyze factors integral to resilient GPS/PNT as they relate to automated systems; and,
- As part of Executive Order 13905, the highlighting of the U.S. Department of Transportation's Pilot Program effort and today's workshop to evaluate complementary PNT technologies and ensure PNT resiliency in the maritime environment.

Ms. Furchtgott-Roth ended her presentation with the following, "We are here not to curse GPS jamming and spoofing, but to provide resilience and backup."

TOPIC: Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing (PNT) Services, EO 13905
Dr. Seth Jonas (Presenter)

BIO: Dr. Seth Jonas is the Deputy Senior Director for Resilience Policy at the National Security Council, where he coordinates efforts to develop and implement integrated national strategies and policies that mitigate threats and hazards to the American people. These include efforts to strengthen the security and resilience of critical infrastructure, prepare communities for emergencies, facilitate effective

national response to disasters, and foster enhanced recovery from catastrophic incidents. Prior to joining the National Security Council, Dr. Jonas served as a member of the research staff at the IDA Science and Technology Policy Institute, where he focused on the intersection of hazards and technology, including space weather; positioning, navigation, and timing services; risk analysis; Federal Government continuity programs; emergency preparedness communications; cyber threats; and electromagnetic pulses.

Dr. Jonas was a 2017 U.S.-U.K. Fulbright Scholar serving as a visiting researcher at Rutherford Appleton Laboratory and Deputy Head of Resilience at the U.K. Government Office for Science. Dr. Jonas has held fellowships at Los Alamos National Laboratory, Brookhaven National Laboratory, and with the JASON scientific advisory group for U.S. national security. He holds an MA and a Ph.D. in physics from Johns Hopkins University, and two BS degrees from the University of Central Florida in physics and liberal science studies (math and chemistry).

Summary of Dr. Jonas's Presentation

Dr. Jonas's presentation focused on the need for all around resilience (e.g., Cyber, PNT Critical Infrastructure). He explained how applications of PNT data permeate our lives yet largely go unseen. In particular, how, on a daily basis, Americans depend on PNT services ranging from the use of smartphone applications, to critical infrastructure systems like power grids and transportation networks, including maritime transportation. Dr Jonas then explained the executive level steps underway to enhance America's critical infrastructure.

Executive Order 13905, directs Federal departments and agencies to develop guidance that mitigates the risks of disruption to critical infrastructure that rely on PNT services. One of the first actions identified in Executive Order 13905 is for the development of PNT profiles, which will, through engagements across the public and private sectors, seek the following:

- Better understand how PNT services are used by infrastructure systems, networks, and assets; and
- Identify which PNT services can best suit the needs for each application from commercial aviation, to maritime navigation to IT system applications.

Ultimately, the PNT profiles will enable critical infrastructure owners and operators to manage the associated risks to their systems, networks and assets that depend on PNT services. The PNT Profiles developed under Executive Order 13905 will work in conjunction with the Cybersecurity Profiles developed previously under Executive Order 13636 to enhance further the resilience of America's PNT/Critical Infrastructure. In closing, Dr. Jonas highlighted the USDOT Pilot Program and that he looked forward to continued success across departments, agencies, and stakeholders implementing Executive Order 13905.

TOPIC: Perspectives on PNT Resiliency for Transportation
Ms. Karen Van Dyke (Presenter)

BIO: Karen Van Dyke serves as the Director for Positioning, Navigation, and Timing (PNT) and Spectrum Management in the U.S. Department of Transportation Office of the Assistant Secretary for Research and Technology (OST-R). Ms. Van Dyke was involved in navigation-related programs at the Volpe National Transportation Systems Center for over 25 years and currently is responsible for overseeing the navigation program and development of policy positions on PNT and radiofrequency spectrum in coordination within the Office of the Secretary of Transportation at USDOT Headquarters in Washington, DC. Ms. Van Dyke received her BS and MS degrees in electrical engineering from the University of Massachusetts at Lowell. She is a Fellow of the Institute of Navigation and served as the organization's president from 2000–2001. She is a recipient of the Award for Meritorious Achievement (Silver Medal) from the Secretary of Transportation.

Ms. Karen Van Dyke's Presentation Summary
(Ms. Van Dyke's presentation is available at https://cms.dot.gov/pnt/perspectives-pnt-resiliency-transportation-vandyke, and individual slide numbers are referenced below as appropriate.)

That although this workshop is focused on the maritime community, USDOT and its stakeholders will be looking to leverage knowledge and lessons learned from this workshop and the Pilot Program towards the other modes of transportation (e.g., aviation, rail with positive train control, intelligence transportation system program (ITS-JPO) with automated vehicles) (see Slide No. 2). GPS jamming and spoofing is a multi-modal issue and the flow of knowledge and lessons learned is bi-directional. Therefore, USDOT will be looking to leverage the knowledge and lessons learned emanating the FAA's GPS Intentional Interference and Spoofing Study.

That GPS/GNSS signals are weak signals and as a consequence are susceptible to GPS/GNSS challenged environments (e.g., urban canyons, inaccurate/out-of-date maps) (see Slide No. 3). Transportation has some of the most demanding performance requirements (e.g., accuracy, availability, integrity). Acknowledgement and relevant still is the 2001 Volpe Center Report entitled, 'Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System.'

Spoofing can deny, degrade, disrupt, or deceive a receiver's operation and can have a range of effects from incorrect outputs of PNT to receiver malfunction (see Slide No 4). The ability to interfere with automated vehicles via jamming or spoofing was noted by the National Science Foundation Branch of the University of Virginia, which showed that you could actually guide a vehicle into oncoming traffic.

Acknowledgement of the Volpe Center's recent work (GPS Backup and Complementary PNT Demonstration effort) (see Slide No. 5). USDOT is looking to the future and will be focusing much of our research highly automated systems working with the Intelligent Transportation Systems Joint Program Office (ITS JPO) (see Slide No. 6).

Further enhancing our looking towards the future, USDOT has issued a grant to what the Center for Automated Vehicles Research with Multimodal AssurEd Navigation (CARMEN). This is a consortium of the Ohio State University, University of California Irvine, University of Texas Austin, and the University of Cincinnati. This UTC will be a great asset in being able to understand better PNT threat scenarios.

Ms. Van Dyke also acknowledged the creation of the Highly Automated Safety System Centers of Excellence (HASS COE) (see Slide No. 6) and noted how the Federal Radionavigation Plan ties in with National PNT R&D Plan (see Slide No. 7). In closing, Ms. Van Dyke urged that we recognize that PNT "is permeated throughout our critical infrastructure with dependencies, particularly for timing, in many of our IT networks" and that we need to understand all of the connectivity, cascading effects and components, from an architecture standpoint, needed to achieve PNT resiliency.

TOPIC: Panel Discussion, Maritime Perspective: How positioning, navigation, and timing supports maritime applications

Mr. Kevin Kohlmann (Presenter/Moderator)
BIO: Kevin Kohlmann is a graduate of Massachusetts Maritime Academy. He sailed for Exxon Shipping Company for 12 years and obtained an Unlimited Master's License. He then worked for Military Sealift Command in several positions including Military Sealift Command's Safety Manager in which he was responsible for the safe operations of over 50 ships. Kevin has been the Director of the Office of Safety for the U.S. Maritime Administration since 2014.

Michael Emerson (Panel Participant)
BIO: Mike Emerson is the Director for Marine Transportation Systems at Coast Guard Headquarters. He manages a broad portfolio of marine navigation, waterway, and bridge programs, and is responsible for a wide variety of Polar and Arctic safety and security initiatives. Mr. Emerson retired from the U.S. Coast Guard in 2014, after 30 years of service. His tours of duty included Senior Fellow for the CNO Strategic Studies Group in Newport, Rhode Island; Chief of Aviation Forces at Coast Guard Headquarters; Commanding Officer of Coast Guard Air Station Clearwater, Florida; Chief of Drug Interdiction at Coast Guard Headquarters; four tours in aviation as a C-130 pilot, and two tours at sea. Emerson graduated from the U.S. Coast Guard Academy in 1984 with a Bachelor of Science in Government Degree and has since received a Master's Degree in Military Studies from the Marine Corps University, and a Master's Degree in Business Administration from American Military University.

Captain Richard G. Hoey (Panel Participant)
BIO: Captain Richard G. Hoey is a graduate of SUNY Maritime College with a BS in metrology and oceanography as well as a Third Mate's License. He has experience sailing a variety of ships for several operating companies in most of the world's oceans. He is a member of the International Organization of

Masters, Mates, & Pilots, and holds a licenses from the United States Coast Guard as a Master of Steam or Motor Vessels of Any Gross Tons Upon Oceans. He has sailed as a master for over 20 years. He currently sails for Maersk Lines Limited, and has done so as a master since 2007.

Summary of Panel Discussion

Mr. Kohlmann conducted an interactive Q&A panel session that delved into the effects of GPS interference (e.g., jamming & spoofing) on maritime shipping via the real world experiences of Captain Hoey along with additional insights from Mr. Emerson of the USCG. The following are highlights from the discussion.

- **Comment:** Maritime transport accounts for roughly 80 percent of international trade, as opposed to other modes of transportation, according to UNCTAD in 2020.
- **Question:** Identification of the pieces of equipment that affected by a GPS jamming event?
    - **Answer:** ECDIS, AIS, Doppler Speed Log, Gyro Compass, RADAR, VDR, Other Comm. equip. reliant on GPS timing.
- **Question:** Is LORAN still in existence and the possibility of using LORAN as a backup or complement to GPS?
    - **Answer:** Not in the U.S. but available in China, Russia, South Korea, Japan, Saudi Arabia.
- **Question:** How do you know you're being spoofed?
    - **Answer:** Typically, from an instrumentation standpoint, you may not know but with visual aids (e.g., buoys, looking out a window, etc.) you can possibly detect.
- **Closing comment from Captain Hoey:** Keep the buoys, keep the ranges, and try to stress their use to younger mates/officers.

Topic: Maritime Perspective: How positioning, navigation, and timing supports maritime applications. Mr. Cameron Naron (Presenter)

BIO: Mr. Naron serves as Director of the U.S. Maritime Administration's Office of Maritime Security. He and his staff support the U.S. maritime transportation system, the U.S. Merchant Marine, and other elements of the U.S. maritime industry by facilitating the development and implementation of effective maritime security policies, procedures, practices, statutes, and training to protect U.S. citizens and maritime interests from maritime security threats including piracy, terrorism, regional conflict, criminal activity, and cyber-attack. He is responsible for providing maritime security information for U.S.-flag vessels, serves as the Department's principal coordinator for maritime domain awareness matters, and functions as the USDOT lead within the interagency Maritime Operational Threat Response crisis response and coordination process and the U.S. Maritime Alerts and Advisories System.

Mr. Naron also serves as USDOT's representative on the National Security Council's Maritime Security and Maritime Cybersecurity Policy Coordinating Committees and Counter Piracy Steering Group. He

serves as a key facilitator between maritime industry and government agencies and provides expert maritime security advice and assistance on issues involving the global maritime transportation system. Mr. Naron retired from the U.S. Coast Guard in 2014 following more than 30 years of military service.

Summary of Mr. Naron's Presentation
Mr. Naron focused on the activities/duties of his office along with information related to the newly established U. S. Maritime Alerts and Advisory System. MARAD's Office of Security works extensively within the Federal interagency. Key partners are the U.S. Coast Guard, the U.S. Intelligence Community, the Department of Defense, and the State Department. In addition, MARAD's Office of Security also interfaces with the maritime industry and specifically with company security officers within the maritime sector. The Office of Security works to bring those partners together to share information on a wide range of maritime security issues with PNT being one of them.

One of the information sharing methods is through the U. S. Maritime Alerts and Advisory System (www.maritime.dot.gov/msci-advisories), a U.S. Government Interagency System whose objective is to get information into the hands of maritime stakeholders. Specifically, the system instructs its users on how to report GPS interference-related information to the Coast Guard Navigation Center (NAVCEN). The remainder of Mr. Naron's presentation focused on details of and the specifics of using the U.S. Maritime Alerts and Advisories System.

Topic: Maritime Perspective: How positioning, navigation, and timing supports maritime applications
Captain William Westrem (Presenter)

BIO: Captain William Westrem began his career at sea at a young age, sailing on ships with his father on Moore-McCormack Lines, based in Brooklyn, New York. He is a graduate of the California Maritime Academy, now CSU-Maritime. Early in his sailing career, he worked on tankers, break-bulk & container ships as a third and second mate from 1989–1994. In 1995, a relief chief mate position led to acting as permanent chief mate on four ships with APL Maritime through 2009. This included container ships, government-chartered freighters, roll-on/roll-offs, and large, medium-speed roll-on/roll offs (LMSRs). He held his first relief master's job in 2002, first permanent master's job in 2004, and has been the permanent master of the *President Eisenhower* since 2018.

Summary of Captain Westrem's Presentation
(Captain Westrem's presentation is available at: https://www.transportation.gov/pnt/what-happens-when-pnt-denied-disrupted-or-manipulated-maritime-environment-westrem-1of2 and https://www.transportation.gov/pnt/what-happens-when-pnt-denied-disrupted-or-manipulated-maritime-environment-westrem-2of2. Individual slide numbers will be referenced as appropriate within this summary.)

Captain Westrem's presentation focused on his real-world experience of jamming/spoofing. He narrated that, upon arrival on the bridge of his ship at the Port of Shanghai, he observed the electronic bearing line on his radar screen going counterclockwise. He noted that although his ship was docked/stationary, his ECDIS chart display was showing his ship travelling 15 to 20 knots, in counterclockwise circle.

The spoofing affected multiple equipment types (e.g., iPhone w/GPS app; ARPA (Automatic Radar Plotting Aid) with an ECDIS overlay; ECDIS laptop).
Please see the following slides:

- File '... environment-westrem-1of2', Slide No. 2 (embedded video) and;
- File '... environment-westrem-2of2', Slide Nos. 2 through 6.

Captain Westrem concluded his presentation with the following observations: It would be advantageous if LORAN were more available and ubiquitous; and, the continued use of visual means as a crosscheck on electronic forms of navigation (e.g., keeping your eyes out the window).

Topic: Maritime Perspective: How positioning, navigation, and timing supports maritime applications
Captain Richard G. Hoey (Presenter)

BIO: Captain Richard G. Hoey is a graduate of SUNY Maritime College with a BS in Metrology and Oceanography as well as a Third Mate License. He has experience sailing a variety of ships for several operating companies in most of the world's oceans. He is a member of the International Organization of Masters, Mates, & Pilots. He holds licenses from the United States Coast Guard as a Master of Steam or Motor Vessels of Any Gross Tons upon Oceans. He has sailed as a Master for over 20 years. He currently sails for Maersk Lines Limited, and has done so as a Master since 2007. He is married and father of four.

Summary of Captain Hoey's Presentation
Captain Hoey's presentation was, in essence, a summary of his years of maritime experience. He stressed the need for young officers to be able to navigate without electronics (e.g., compass, sextant, and paper charts) and in particular when navigating ports of entry to "look out the window."

Topic: What happens when PNT is denied, disrupted, or manipulated in a maritime environment?
Mr. Dana A. Goward (Presenter)

BIO: Dana A. Goward is the President of the Resilient Navigation and Timing Foundation and a member of the US National Spaced-Based PNT Advisory Board. The Resilient Navigation and Timing Foundation is a scientific and educational charity dedicated to protecting GPS/GNSS signals and users. Mr. Goward is a

lifelong practical navigator, orienteering as scout, serving as a ship's navigator at sea, and using every means available in the air as a career U.S. Coast Guard helicopter pilot.

Mr. Goward retired in 2013 from the Senior Executive Service as the maritime navigation authority for the United States and now serves as a member of the U.S. National Space-Based PNT Advisory Board. He is also a senior advisor to Space Command's Purposeful Interference Response Team, is an emeritus Chairman of the Board for the Association for Rescue at Sea, and is the proprietor at Maritime Governance, LLC.

Summary of Mr. Goward's Presentation
(Mr. Goward's presentation is available at https://www.transportation.gov/pnt/what-happens-when-pnt-denied-disrupted-or-manipulated-maritime-environment-goward-rnt. Individual slides are referenced as appropriate within this summary.)

The subtopic or subject of Mr. Goward's presentation was entitled, "How to Steal a Ship." In his presentation, Mr. Goward first followed the progression of GPS/GNSS-related interference from jamming and finally into spoofing. PowerPoint presentation slide no. 3 highlights the readily available jamming devices along with notable worldwide jamming events reported in the news (e.g., Newark International Airport, North Korea, etc.).

Mr. Goward spoke on the adverse consequences of jamming in the maritime environment (e.g., shutting down of ports, aiding of cargo thefts by illegally blocking tracking mechanisms). Mr. Goward then proceeded to chronologically list notable GPS spoofing-related events (e.g., 2011 CIA Drone by Iran, 2013 UAV/Drone and $18 million yacht by Prof. Todd Humphries, 2015 U.S. Navy Boats by Iran, and 2017 Black Sea Event by Russia).

Mr. Goward continued by differentiating between the spoofing methods practiced by Russia and China (e.g., spoofing on a circle by China versus spoofing to airports practiced by Russia). (Worth mentioning here that Captain Westrem, in his presentation, experienced firsthand spoofing on a circle at the Port of Shanghai.) Mr. Goward explained further that spoofing technology development has followed the same path as most technologies, less expensive, more capable and easier to use (slide no. 12).

In conclusion, Mr. Goward offered a detailed checklist of dos and don'ts for increasing PNT resilience in the maritime environment (e.g., protection of GPS signals, toughening of users/equipment and augmentation with other signals & sources (PTA)).

TOPIC: What happens when PNT is denied, disrupted, or manipulated in a maritime environment?
Captain Michael Glander (Presenter)

BIO: Captain Mike Glander serves as commanding officer of the U.S. Coast Guard Navigation Center in Alexandria, VA. The Navigation Center is responsible for creating and managing informational products and services for the public that enhance the safety, security, and efficiency of the U.S. maritime transportation system. One such service includes receiving and distributing reports from the users of GPS about disruptions to service. Captain Glander also serves as Deputy Chair of the Civil GPS Service Interface Committee (CGSIC), which exchanges information between GPS users worldwide and U.S. government authorities.

Summary of Captain Glander's Presentation
(Captain Glander's presentation is available at https://www.transportation.gov/pnt/what-happens-when-pnt-denied-disrupted-or-manipulated-maritime-environment-glander. Individual slide numbers are referenced as appropriate within this summary of Captain Glander's presentation.)

Captain Glander's presentation (slide no. 2) focused on the role of the U.S. Coast Guard's Navigation Center (NAVCEN) in the GPS Problem Reporting process and the interplay between the NAVCEN and other USG agencies (e.g., FAA, FCC, DHS, and DoD). In addition to the above mentioned agencies, Captain Glander explained that, depending on the nature of the reported problem, other entities may also get involved (e.g., MARAD, intelligence offices/watches, Global MOTR Coordination Center (GMCC), Purposeful Interference Response Team (PIRT) Group, and international partners). Captain Glander continued with a detailed breakdown of Worldwide GPS Problem Reports sent to the NAVCEN in 2019 and 2020 (see slide nos. 3 and 4).

In conclusion, Captain Glander spoke of the need to understand better the nature of the short duration types of GPS interference typically experienced in the continental United States and mentioned a joint project between NAVCEN, FAA, FCC, U.S. Navy, and the Port of Virginia that was established. It is a small-localized GPS interference detection network, in the Virginia Tidewater area and led by the FAA that has the ability to spot and record even small instances of GPS, jamming and disruption signals in real time.

TOPIC: Panel Discussion, Options to reduce operational impact and increase PNT resiliency.
Mr. Cameron Naron (Presenter /Moderator)
Captain Richard G. Hoey (Panel Participant)
Dr. Andrew Hansen (Panel Participant) (Dr. Hansen represented the OST-R/ Volpe Center Complementary PNT and GPS Backup Technologies Demonstration Team Representative.)

Summary of Panel Discussion
Mr. Naron conducted an interactive Q&A session (slides not presented) involving the above participants. The focus of the Q&A was on the effects of GPS interference, in particular spoofing on ship operations,

and on the various methods for mitigation. Captain Hoey spoke on his personal experiences with GPS jamming/spoofing while Dr. Hansen spoke to GPS jamming and spoofing mitigation methods.

Q&A discussions took place on the effects of GPS interference on ship communications (e.g., INMARSAT & VHF radios) and navigation (e.g., Houston Ship Channel). In the communications example, Captain Hoey noted that INMARSAT radios are susceptible due to their reliance on GPS timing while VHF radios are not affected. Captain Hoey then explained that, in the event of GPS interference in for example, the Houston Ship Channel, communications with Vessel Traffic Service (VTS) would be possible with a VHF radio. In addition, Captain Hoey spoke on his personal experiences with jamming & spoofing. In particular how jamming is more easily detected than spoofing. Per Captain Hoey, with spoofing, its difficulty to detect, “GPS signal goes into an off thing… it just drifts away.”

Dr. Hansen discussed available complementary PNT methods and techniques for increasing the resilience of maritime GPS dependent shipboard systems such as the incorporation PNT information from other PNT sources (e.g., other GNSS, LEOs, Loran, and NDGPS ranging) on the service provider side, to the use of technologies and techniques on the host or user side (e.g., CRPA antenna technologies and GNSS signal analysis techniques). Please see the below figure.

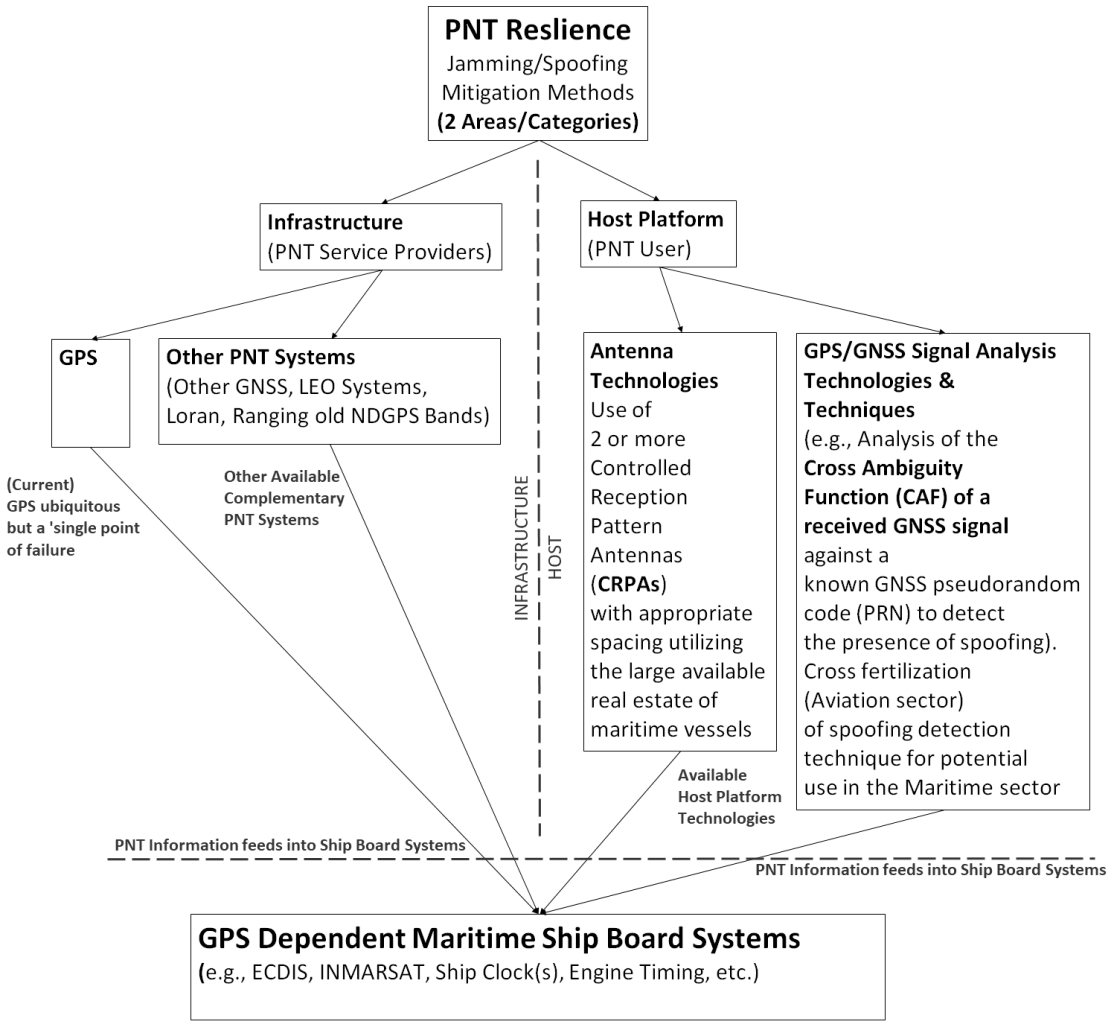


Figure A-1: Notional Graphic of Methods For Increasing Shipboard PNT Resilience in the Maritime Sector (by Dr. Andrew Hansen)

Dr. Hansen also noted that incorporation of other complementary PNT information feeds into 'some' existing shipboard maritime equipment (e.g., ECDIS, INMARSAT radios, etc.) will take time. Still, on a positive note, a couple of the PNT technologies mentioned in the above graphic are readily available for incorporation now with minimal modification to existing MARAD maritime systems.

TOPIC: Options to reduce operational impact and increase PNT resiliency.
Dr. Andrew Hansen (Presenter)

BIO: Dr. Hansen is a principal technical advisor at the USDOT Volpe Center on Aviation Modeling and System Design. He joined the Volpe Center in 2005 bringing innovation to safety, environmental, and

economic aspects of transportation. His experience over the last 30 years ranges across academia, industry, government service, and small business ownership with expertise in computational mathematics, signal processing, navigation systems, and airspace architecture. Dr. Hansen currently focuses on developments at the intersection of vehicle autonomy and resilient navigation service. In addition, Dr. Hansen serves as USDOT liaison to the USSF for GPS and as a USDOT delegate to the International Committee on GNSS furthering the use of open GNSS services in national and international arenas. Dr. Hansen is also a member of IEEE and ION. He received his BSEE (1991) and MSEE (1992) from Worcester Polytech Institute and his Ph.D. (2002) in electrical engineering from Stanford University.

Summary of Dr. Hansen's Presentation

(Dr. Hansen's presentation is available at https://www.transportation.gov/pnt/options-reduce-operational-impact-and-increase-pnt-resiliency-hansen.)

Dr. Hansen's presentation focused on slides four and five of his presentation, entitled "Complementary PNT Technology Considerations for Resilient PNT Service." He spoke to specifics of the USDOT Complementary PNT Demonstration relating to the technologies demonstrated along with their associated "high" Technology Readiness Levels (TRLs). Referencing slide no. 4, 11 technologies were demonstrated that included two LEO commercial satellite technologies; two LORAN or eLORAN terrestrial RF systems; four terrestrial RF, medium and high frequency bands; two technologies using 802.11 (Wi-Fi) spectrum; and two, fiber-optic time-transfer based technologies. In conclusion, Dr. Hansen noted that many of the technologies from the demonstration have receivers that are capable of being integrated into existing platforms due to their high TRLs and there are many possibilities for utilization of these available complementary PNT technologies within the maritime sector.

Summary of Final Question and Answer Session

Question	Response (Panel Members Responding)
1. Why is GPS spoofer equipment not considered illegal by various organizations?	U.S. law makes selling and using them illegal, but not possessing them. (Goward)
2. What are your thoughts on widespread use and promotion of alternative navigation systems (e.g., GLONASS or other GNSS; inertial systems; or automated celestial systems)?	Panel agreement. Diverse, alternative, complementary, system-of-systems, and a multiple Phenomenology approach to PNT is a good choice and encouraged. But, from a National Security perspective, caution needs to be exercised as it relates to foreign GNSS (e.g., GLONASS). (Goward, Van Dyke, Hansen, Naron)

Question	Response (Panel Members Responding)
3. Can you comment on the financial centers demo that used eLORAN testing 2–3 years ago? For the stock market?	Successful demonstration that "high" power, "low" frequency eLORAN signals, transmitting from Wildwood, NJ, were able to penetrate the New York Stock Exchange and provide timing accuracy of approximately 70 nanoseconds. (Goward)
4. Would a spoof show a high HDOP, or does it look normal?	Spoofing looks like the constellation itself, so HDOP would not be impactful. (Hansen)
5. What about using an encrypted mesh network within the buoy network to act as a differential positioning network? Can this be used as a means of checks and balance on GPS?	"The question is what size, weight, power, cost, and the degree of positioning and accuracy each system would give you? A lot of things can be done…we just need to do some of them!" (Goward) "…working with industry on what solutions will work best, but it's really to say it's not acceptable to, if you're going to be impacted by the risk to not choose anything to mitigate it. Lots of things we can do. We just need to start actually executing on them." (Van Dyke)
6. Are there options on the radar to tum off the AIS layers or things that would be spoofed?	"Yes, if you have a radar that is equipped to take AIS inputs, you almost certainly have the ability on that radar to tum those inputs off if you found them to be spoofed or just otherwise confusing." (Naron)
7. Do we know how large an area a single spoofing event would cover? Are we talking a radius of 10 miles or 1,000 miles?	"The opportunities (spoofing area wise) are probably nearly endless." (Goward)
8. Does WAAS correct jamming or spoofing errors?	"WAAS only corrects the performance of the differential corrections. It won't provide an anti-spoofer as currently designed." (Hansen)
9. Have you looked at using inertial navigation systems aided by Doppler velocity logs (DVLs) to aid ships navigation in GPS denied/spoofed areas?	Yes, integrated navigation systems are available and equipped to take a variety of inputs, including Doppler. They have the ability to generate a DR (dead reckoning) position but not a safe way to navigate long-term per maritime authorities (e.g., IMO). (Goward, Naron)
10. Has there been any discussion concerning wind towers as additional fixed supplemental NAV aids?	"No, there are other alternatives that can provide more complete coverage, more maritime coverage." (Furchtgott-Roth)
11. Are there any products out there that compare GPS-derived timing to GPS-independent timing (rubidium normal)? Could be a way to detect spoofing, or more precisely: mix the 10 MHz signal of both devices.	Panel agreement. At present "No, not in the maritime environment." (Goward, Hansen)

Question	Response (Panel Members Responding)
12. Does spoofing affect all GPS inputs? For example, if you were on the U.S. GPS satellites and switched to GLONASS, would you still be affected by a targeted spoof?	Yes, current spoofing capability would attack all GNSS at the same time. (Van Dyke, Hansen, Furchgott-Roth)
13. Have there been any recent spoofing incidents, specifically on the Great Lakes?	Panel agreement. "No." (Hansen, Naron, Glander, Furchtgott-Roth)

Appendix B: Maritime GPS Anomalies Collected by the U.S. Department of Transportation Spectrum Monitoring Operations Center in 2021

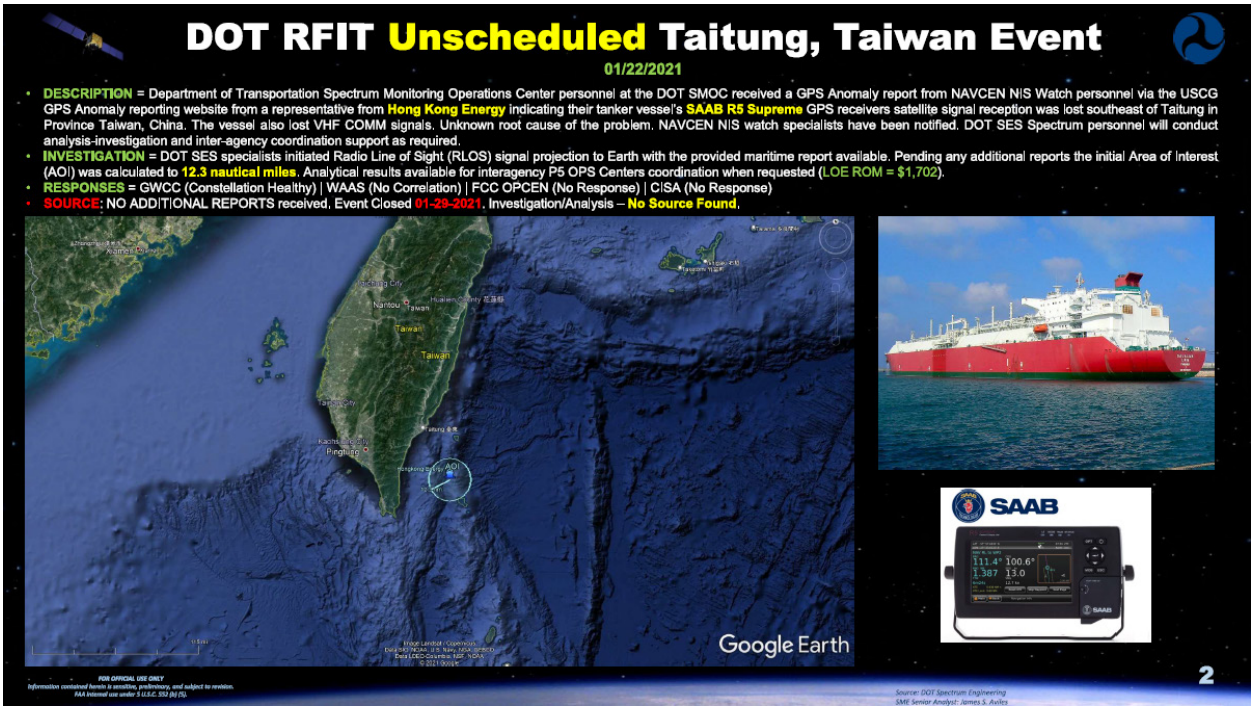
Maritime GPS Anomalies Collected by the U.S. Department of Transportation Spectrum Monitoring Operations Center in 2021

Background

The Department of Transportation Spectrum Monitoring Operations Center (SMOC) maintains a record of GPS anomalies reported in the Transportation Systems Sector, including within the maritime domain. These reports are compiled from submissions made to the GPS anomaly reporting websites maintained by the U.S. Coast Guard Navigation Center (NAVCEN) or the Federal Aviation Administration (FAA) Air Traffic Control System Command Center (ATCSCC). Each anomaly report includes:

- Event Date (start- and end-dates and times)
- Location (latitude and longitude, and closest proximate nation)
- Equipment used (e.g., GPS, including receiver model and affected frequencies)
- Reporting source (e.g., USCG NAVCEN or FAA ATCSCC)
- Contact information of reporting source (including names of reporting individual and vessel)
- Description of anomaly (e.g., duration, details observed, etc.)

Anomaly reports are shared with Federal interagency partners, and subsequently analyzed and investigated by USDOT, FAA, USCG, and other agencies responsible for GPS monitoring. USDOT also uses the report data is used to create a synopsis of each anomaly, including its location, reporting vessel, GNSS receiver, and other pertinent information (see Figure B-1).



(Source: USDOT Spectrum Monitoring Operations Center)

Figure B-1: Sample DOT Radio Frequency Interference Tracking System Record

Maritime GPS Anomalies Reported in 2021

In 2021, 55 maritime GPS anomalies were reported via the USCG NAVCEN and one report was received via the FAA ATCSCC; see Table B-1. Of the 56 reported GPS anomalies, the majority (43 anomalies) were in the Mediterranean Sea, reported by vessels operating in the waters of Cyprus (10), Egypt (10), Greece (2), Italy (10), Lebanon (1), Malta (6), Tunisia (2), and Turkey (2). The remaining anomalies were reported in the Persian Gulf (2-Bahrain, 2-Saudi Arabia), South Atlantic (3-Brazil), and the Pacific Ocean (1-Taiwan, 1-Guam), with four reported in United States waters (2 off Florida, 2 off Massachusetts). All 56 GPS anomalies that were reported affected the GPS L1 band (1575.42 MHz). The GNSS equipment in use at the time included 25 different GNSS receiver models. The most commonly installed models were manufactured by Saab AB (19 units, 2 models) and Furuno Electric Co., Ltd (17 units, 6 models).

Table B-1: Synopsis of GPS Anomalies Reported in 2021

DATE	LATITUDE LONGITUDE	NATION / WATERWAY	RECEIVER	SUMMARY
1/22/2021	22.2615 121.4201	Taiwan Pacific	SAAB R5 Supreme	A report from a representative from Hong Kong Energy indicating their tanker vessel's SAAB R5 Supreme GPS receiver's satellite signal reception was lost southeast of Taitung in Province Taiwan, China. The vessel also lost VHF COMM signals. Unknown root cause of the problem.

DATE	LATITUDE LONGITUDE	NATION / WATERWAY	RECEIVER	SUMMARY
1/22/2021	26.5791 51.2951	Bahrain Persian Gulf	JRC JLR-8400	A report from mariner aboard the MT Maersk Misaki vessel's JRC JLR-8400 GPS receiver's satellite signal reception was lost en route from Qatar to Bahrain off shore approximately 44 nautical miles northeast of Manama 1 hour after departing Mesaieed. The issue continued occurring for over 12 hours and the vessel experienced GPS loss from 1-5 minutes at each occurrence. The vessel is presently at anchor off Bahrain about 44 nm offshore.
1/25/2021	28.2733 -79.1300	U.S. (FL) Caribbean	FUGRO 9205	A report from a mariner aboard their off shore oil rig supply vessel's Fugro 9205 GPS receivers with Trimble GA830 antenna lost satellite signal reception for about 45 minutes from the Melbourne, FL coast. The receiver plot display shows satellites in-and-out causing the position to be erratic and unusable. The same problem was observed at the same time on 1-23-2021.
1/26/2021	26.2088 50.6231	Bahrain Persian Gulf	Furuno GP37	A report from mariner indicating their vessel's Furuno GP37 GPS receivers lost signal reception while transiting in the Bahrain TTW off shore approximately for 1 to 3 minutes. The GPS signal losses are occurring from 2 minutes to 3 hours apart. The vessel experienced the same while moored at Alghurayfah homeport.
2/4/2021	37.0452 11.8905	Italy Mediterranean	SAAB R4	A report from a representative from mariner personnel aboard the *Maersk Pittsburgh* indicating their vessel's SAAB R4 GPS receivers lost signal reception while navigating in the Mediterranean Sea just north of the Pantelleria Island, Italy. The vessel is bound from Algeciras, Spain to Port Said, Egypt. The GPS signal loss started to occurred intermittently but continued until reaching east of Malta. Unknown root cause of the problem.
2/7/2021	37.9585 16.5050	Italy Mediterranean	Furuno GP-150	A report from mariner personnel aboard the *Ocean Gladiator* heavy lift indicating their vessel's Furuno GP-150 GPS receivers lost signal reception and shows low HDOP while navigating in the Mediterranean Sea just east of Bovalino, Italy. The vessel showed 16 losses of signal reception on the logs. Unknown root cause of the problem.
2/10/2021	32.0327 31.6505	Italy Mediterranean	Leica MX-420	A report from 2nd officer aboard the *Bernhard Schulte* container ship indicating their vessel's Simrad GN33 GPS receivers lost signal reception while navigating in the Mediterranean Sea between Malta and Sicily, Italy. Unknown root cause of the problem.
2/10/2021	36.5816 13.7618	Italy Mediterranean	Simrad GN33	A report from captain aboard the *Stena Primorsk* tanker ship indicating their vessel's Leica MX-420 DGPS receivers lost signal reception while navigating in the South Mediterranean Sea between 25 to 50 nautical miles off Port Said, Egypt. Problems ranged from intermittent disturbance to complete loss of signal. Other vessels in the area confirmed loosing GPS signal over VHF radio comms. Unknown root cause of the problem.

DATE	LATITUDE LONGITUDE	NATION / WATERWAY	RECEIVER	SUMMARY
3/9/2021	41.6340 -70.8762	U.S. (MA) North Atlantic	Furuno SC30	Mariner reported GPS signals on their Furuno SC-30 and several marine manufacturer GPS and satellite compasses were losing fixes mainly occurring between 1500-1700 local time. GPS signal strength were coming and going with no discernible pattern on a multitude of fishing vessels in New Bedford, MA harbor. Unknown root cause of the problem. Initially sent this info to the FCC, they responded by saying it should go to FAA. FAA ATSS WAAS specialists have been notified. DOT SES Spectrum personnel will conduct analysis-investigation and inter-agency coordination support as required.
4/13/2021	36.0986 16.9659	Malta Mediterranean	Furuno GP-170	A report from captain aboard the *Fairfax 223* vessel indicating their Furuno GP-170 and SAAB R5 GPS receivers lost signal reception while navigating in the East Mediterranean Sea approximately 117 nautical miles east from Marsaskala, Malta. Signal to Noise Ratio (SNR) of all satellites changed continuously from 0 to less than 30 for all satellites. Both GPS receivers were alarming, indicating a "loss of signal." Other vessels in the area transmitted via VHF COMM indicating also loosing GPS signal. Unknown root source of signal jamming.
4/24/2021	21.4648 39.0988	Saudi Arabia Persian Gulf	Furuno GP-150	A report from captain aboard the *APL Fullerton* vessel indicating their Furuno GP-150 GPS receiver lost signal reception while at 3 nautical miles before the port limit of the Port of Jeddah in Saudi Arabia. During the 19 hours length of the vessel stay at port GPS signal reception was intermittent or no reception at all. Unknown root source of GPS signal reception problems.
4/26/2021	36.4083 14.6701	Malta Mediterranean	JRC NWZ-4740	A report from captain aboard the OC MV *Oldendorff* vessel indicating their JRC NWZ-4740 GPS receiver lost signal reception for several minutes while navigating in the East Mediterranean Sea in the channel of Malta approximately 30 nautical miles north of Pembroke, Malta. Two vessel reports were filed with NAVCEN reporting website. Unknown root cause of GPS signal reception problems.
4/29/2021	31.5166 32.2343	Egypt Mediterranean	Furuno GP-150	A report from captain aboard the *Master Ocean Freed* vessel indicating their Furuno GP-150 GPS receiver experienced GPS spoofing for approximately 12 hours upon departure from Port Said. GPS signal shifted numerous times and position was 6 to 8 miles off. Unknown root source of GPS signal spoofing.
5/2/2021	27.8315 -82.8197	U.S. (FL) Caribbean	Garmin GPSMAP 76CX	A report from boater indicating the Garmin GPSMAP 76cx GPS receiver experienced complete loss of GPS signal reception for approximately 10 minutes in the north end of the Boca Ciega Bay near St. Petersburg, FL. GPS signal reception restarted after 10 minutes. Unknown root source of GPS signal loss.

DATE	LATITUDE LONGITUDE	NATION / WATERWAY	RECEIVER	SUMMARY
5/3/2021	37.0900 12.1333	Italy Mediterranean	SAAB R4	A report from staff captain aboard the *Anthem of the Seas* cruise ship indicating their two SAAB R4 GPS receivers experienced GPS signal loss intermittently but repeatedly for approximately 5 to 10 seconds between 1957 UTC to 0732 UTC while cruising north of Panteleria Island, Italy. Unknown root source of GPS signal loss.
5/5/2021	35.3833 19.3517	Greece Mediterranean	SAAB R4	A report from captain aboard the *Anthem of the Seas* cruise ship indicating their two SAAB R4 GPS receivers experienced GPS signal loss approximately 145 nautical miles southwest of Peloponnisos, Greece while cruising east in the Mediterranean Sea. Unknown root source of GPS signal loss.
5/8/2021	34.6517 33.0167	Cyprus Mediterranean	SAAB R4	A report from captain aboard the *Anthem of the Seas* cruise ship indicating their SAAB R4 GPS receivers experienced GPS signal loss while at dock side at the port in Zakaki Limassol, Cyprus. The GPS Signal loss cleared after an undetermined time span. Unknown root source of GPS signal loss.
5/14/2021	41.3331 -70.4258	U.S. (MA) North Atlantic	U-Blox Neo-7P	A report from Marine Surveying Engineer with Geo Marine Survey Systems B.V. based in the Netherlands indicating four vessels using the U-Blox NEO 7P GNSS receiver module experienced GPS signal loss in the vicinity of Martha's Vineyard, MA. GPS satellite signal was lost for the Fugro Go Liberty, Fugro Go Pursuit, Zephyr Marine Westerly, and the Brooks McCall. Unknown root source of GPS signal loss.
5/22/2021	34.0283 23.7850	Greece Mediterranean	Furuno GP-150	A report from the captain of the *Linda Oldendorff* vessel indicating their Furuno GP-150 GPS receivers experienced complete GPS signal loss while navigating the East Mediterranean and south of the island of Gavdos, Greece approximately 50 nautical miles from the Kastri town. Unknown root source of GPS signal loss.
5/24/2021	38.0774 17.4928	Italy Mediterranean	SAAB R5	A report from mariner aboard an unknown type vessel indicating their SAAB R5 Supreme GPS receivers experienced complete GPS signal loss while navigating the Mediterranean sea east of the Riace Marina in Italy. The GPS satellites shown with complete signal loss where 2, 6, 10, 12, 13, 15, 17, 19 and 24. Unknown root source of GPS signal loss.
5/25/2021	13.4260 144.6627	U.S. (Guam) Pacific	SAAB R5	A report from second mate with Stabbert Maritime indicating their SAAB R5 Supreme GPS receivers experienced SBAS differential correction loss from PRN #137 for approximately 30 minutes while the vessel was at dock side in the port at Guam. The same problem occurred a second time from the same PRN #137 around 19:42 local time. Unknown root source of the SBAS differential loss.

DATE	LATITUDE LONGITUDE	NATION / WATERWAY	RECEIVER	SUMMARY
5/26/2021	36.7333 13.1667	Malta Mediterranean	SAAB R4	A report from captain of the Team Tanker International vessel indicating their SAAB R4 GPS receiver and several other GPS receivers experienced complete loss of signal at 2320 local and intermittent GPS signal loss later while navigating in the Mediterranean sea northwest in the Malta channel approximately 64 nautical miles from Għarb, Malta. Unknown root source of GPS signal loss.
6/4/2021	36.8617 12.6283	Italy Mediterranean	Furuno GP-150	A report from the captain of the *Margret Oldendorff* vessel indicating their Furuno GP-150 GPS receivers experienced complete GPS signal loss while at sea in the Mediterranean south of Sicily, Italy approximately 45 nautical miles from the Sciacca town in Sicily. Unknown root source of GPS signal loss.
6/5/2021	37.5700 11.8833	Italy Mediterranean	Leica MX 420	A report from captain aboard *MLL Seletar* vessel indicating their Leica MX 420 GPS receivers experienced complete GPS signal loss while at sea in the Mediterranean west of Sicily, Italy approximately 30 nautical miles from the Marsala town in Sicily, Italy. Unknown root source of GPS signal loss.
6/5/2021	36.8617 12.6283	Italy Mediterranean	Furuno GP-150	A report from the captain of the *Stena Surprise* vessel indicating their Furuno GP-150 GPS receivers experienced complete GPS signal loss while at sea in the Mediterranean south of Sicily, Italy approximately 36 nautical miles from the Agrigento town in Sicily. Other vessels in the area also indicated loosing GPS signal reception. Unknown root source of GPS signal loss.
6/23/2021	35.8833 16.0201	Malta Mediterranean	Furuno GP170	A report from the captain of the *Albatros Island* vessel indicating their Furuno GP-170 GPS receiver and several other GPS dependent units experienced loss of signal at 0040 local while navigating in the Mediterranean sea approximately 70 nautical miles east from Valletta, Malta. Confirmed via VHF radio other ships in the area also experienced the same issues. Unknown root source of GPS signal loss but signal was recovered at 0710 local.
6/26/2021	35.8167 16.4400	Malta Mediterranean	SAAB R4	A report from the captain of the *Maersk Pittsburgh* vessel indicating their SAAB R4 GPS receiver experienced loss of signal for space vehicles 5, 7, 8, 13, 14, 15, 17, 19, 24, 28, 30 while navigating in the Mediterranean sea approximately 75 nautical miles east from Zurrieq, Malta. The vessel was bound from Algeciras, Spain to Port Said, Egypt. Unknown root source of GPS signal loss.
6/30/2021	30.9043 32.3150	Egypt Mediterranean	Furuno GP-150	A report from the captain of the *Mathilde Oldendorff* vessel indicating their Furuno GP-150 GPS receiver experienced loss of signal while navigating along the Suez Canal in Port Said, Egypt. The vessel experienced the signal loss at 1530 UTC but the outage cleared. Other vessels in the vicinity confirmed GPS signal loss. Unknown root source of GPS signal loss.

DATE	LATITUDE LONGITUDE	NATION / WATERWAY	RECEIVER	SUMMARY
7/2/2021	37.4416 10.7834	Tunisia Mediterranean	SAAB R4	A report from captain aboard the *Maersk Atlanta* vessel indicating their SAAB R4 and their Furuno GP-150 GPS receivers experienced loss of signal and alarms with NO FIX indication at 1100 UTC while navigating in the northwest corner of Tunisia in the Mediterranean sea approximately 48 nautical miles northeast from Tunis, Tunisia. By 1300 UTC both GPS units completely lost GPS signal. Unknown root source of GPS signal loss.
7/3/2021	31.2332 32.3500	Egypt Mediterranean	JRC JLR-7800	A report from the captain of the TFR *Kristainsand* vessel indicating their JRC JLR-7800 GPS receiver experienced loss of signal while navigating along the entry point of the Suez Canal in Port Said, Egypt. The vessel experienced the signal loss at 1930 Egypt Standard Time and the following satellites were out 24, 12, 2, 6, 19, 25, 15, 29, 32, and 13. Other vessels in the vicinity confirmed GPS signal loss. Unknown root source of GPS signal loss.
7/8/2021	31.2163 32.3416	Egypt Mediterranean	Leica MX 420	A report from captain aboard the *Maersk-Seletar* vessel indicating their Leica MX 420 GPS receiver experienced loss of signal the vessel was just finishing up transiting the Suez Canal in Port Said, Egypt. The vessel experienced the signal loss for about 5 minutes then it would come back for about 5 minutes. Other vessels in the vicinity confirmed GPS signal loss. Unknown root source of GPS signal loss.
7/9/2021	32.6327 32.6082	Egypt Mediterranean	Garmin GRC	A report from captain aboard the *Western Tokyo* vessel indicating their Garmin GRC GPS receiver experienced loss of signal while the vessel was approximately 86 nautical miles north of Port Said, Egypt. The vessel experienced the GPS signal loss at 1800 UTC. Other vessels in the vicinity confirmed GPS signal loss. Unknown root source of GPS signal loss.
7/15/2021	31.2243 32.3445	Egypt Mediterranean	Leica MX 420	A report from captain aboard the *Maersk-Seletar* vessel indicating their Leica MX 420 GPS receiver experienced loss of signal when passing buoys KM2.9 northbound near the breakwater at the Suez Canal in Port Said, Egypt. The vessel experienced the GPS signal loss for about 45 minutes then signal came back with no issues since. Unknown root source of GPS signal loss.
7/29/2021	33.5650 29.9675	Egypt Mediterranean	JRC JRL-4341	A report from captain aboard an unknown vessel indicating their JRC JRL-4341 GPS receiver experienced loss of signal when at the Mediterranean Sea approximately 182 nautical miles sailing inbound to Port Said. While at an anchorage position in the Suez canal in Port Said the interference keeps occurring at intervals of about 10 minutes. Unknown root source of GPS signal loss.
7/30/2021	31.8900 31.4500	Egypt Mediterranean	SAAB R5 Supreme	A report from the captain of the *CMA CGM A Lincoln* vessel indicating their SAAB R5 Supreme GPS receiver experienced loss of signal reception when approximately 10 nautical miles northwest of Damietta, Egypt. The vessel experienced the GPS signal loss on 7/29/2021 at 1430 GMT. Unknown root source of GPS signal loss.

DATE	LATITUDE LONGITUDE	NATION / WATERWAY	RECEIVER	SUMMARY
7/31/2021	30.8950 32.3150	Egypt Mediterranean	SAAB R4	A report from the captain of the *Maersk Pittsburgh* vessel indicating their SAAB R4 GPS receiver experienced loss of signal while navigating along the Suez Canal in Port Said, Egypt bound for Algeciras Spain. The vessel experienced the signal loss at 1500 EEST - Egypt Standard Time on 7/28/2021. Other vessels in the vicinity confirmed GPS signal loss. Unknown root source of GPS signal loss.
8/11/2021	31.3785 32.3374	Egypt Mediterranean	JRC JLR-7700 MK II	A report from captain aboard the *Maersk Norfolk* vessel indicating their two JRC JLR-7700 MK II lost DGPS signal due to heavy interference while navigating just north of the Suez Canal in Port Said, Egypt. The vessel experienced the signal loss at 0300 LT and had to be factory reset and rebooted several times before it was able to acquire satellites later in the day. Unknown root source of GPS signal loss.
8/14/2021	37.5386 10.5885	Tunisia Mediterranean	Furuno GP-150	A report from the captain of the M.V. *Nootka Island* vessel indicating their Furuno GP-150 GPS receiver experienced loss of signal and alarms codes 212 indicating no fix at 1800 EEST while navigating offshore in the Mediterranean sea approximately 38 nautical miles northeast from Bizerte, Tunisia. Unknown root source of GPS signal loss.
8/16/2021	36.8617 12.6283	Italy Mediterranean	Simrad MX610	A report from the captain of the *Abaouz Jamal* vessel indicating their two Simrad MX610 GPS receivers experienced complete GPS signal loss while at sea in the Mediterranean south of Sicily, Italy approximately 18 nautical miles from the Sciacca town in Sicily. Satellite signal is lost and then comes back for few minutes then is lost again for 2 hours. Unknown root source of GPS signal loss.
9/9/2021	34.6953 33.1975	Cyprus Mediterranean	SAAB R5 Supreme	A report from the captain of the super luxury *Seabourn Encore* cruise ship indicating their SAAB R5 Supreme GPS receivers experienced intermittent GPS signal loss while off shore 7 nautical miles east from Limassol, Cyprus. The GPS Signal continues working intermittently. Unknown root source of GPS signal loss.
9/19/2021	33.2068 32.6406	Cyprus Mediterranean	Cobham Sailor 900	A report from engineer with NSSL Global vessel satellite equipment manufacturer indicating that numerous vessels using their Cobham Sailor 900 with built-in dual GNSS/GPS receivers are experiencing loss of GNSS signals and position in a polygon rectangular area 200 nautical miles south from Larnaca, Cyprus. The GNSS signal loss has been occurring since September 3. Unknown root source of signal loss.
9/20/2021	34.6865 33.1651	Cyprus Mediterranean	SAAB R5 Supreme	A report from captain of the P&O Cruises ships indicating their SAAB R5 Supreme GPS receivers experienced GPS signal loss of 11 satellites that where being tracked while off shore 5 nautical miles east from Limassol Bay, Cyprus. The GPS Signal reception loss is on-going and is a common issue in the area. Unknown root source of GPS signal loss at this time.

DATE	LATITUDE LONGITUDE	NATION / WATERWAY	RECEIVER	SUMMARY
9/25/2021	-3.6633 -38.4317	Brazil South Atlantic	JRC JLR-7700MK II	A report from captain indicating their vessel JRC JLR-7700MK II GPS receivers experienced GPS signal loss of 8 satellites and position fluctuated on the ECDIS. Position was verified using a second GPS on the ship and the vessel position shifting by 6-9 cables automatically while approximately 7 nautical miles northeast of Fortaleza Anchorage, Brazil. Unknown root source of GPS signal loss at this time.
9/29/2021	34.4897 35.5001	Lebanon Mediterranean	Furuno GP-150	A report from captain with one of the Anglo Eastern vessels indicating their Furuno GP-150 GPS receivers experienced erratic behavior on various navigation equipment on 9/25/2021. Both GPS installed onboard lost satellite signals and the gyro compass started showing an error of around 14 degrees while off shore 17 nautical miles from Tripoli, Lebanon. Unknown root source of GPS signal loss.
10/5/2021	34.6865 33.1651	Cyprus Mediterranean	JRC JLR-7500	A report from captain of Athens based Minerva Marine ships indicating their JRC JLR-7500 GPS receivers experienced GPS signal spoofing with Alarms 001 NO FIX while off shore 70 nautical miles southeast from Paralimni, Cyprus. The GPS Signal reception loss was restored at position 35 13.8' N and 34 48.4' E at 13:06 LT after one hour. Unknown root source of GPS signal loss at this time.
10/8/2021	34.6953 33.1975	Cyprus Mediterranean	SAAB R5 Supreme	A report from captain of the *Seabourn Encore* cruise ship indicating their SAAB R5 Supreme GNSS receivers experienced signal loss of 22 satellites that where being tracked while off shore 2.5 nautical miles due south from Moni off shore to Limassol Bay, Cyprus. The GPS Signal reception loss is ongoing and is a common issue in the area. Unknown root source of GPS signal loss at this time.
10/11/2021	34.6953 33.1975	Cyprus Mediterranean	SAAB R5 Supreme	A report from captain of the *Seabourn Encore* cruise ship indicating their SAAB R5 Supreme GNSS receivers experienced recurring GNSS signal loss of satellites that where being tracked while off shore 3.6 nautical miles southeast of the town Agios Tychon off shore in Cyprus. The GPS Signal reception loss is on-going lasting approximately 5 minutes each time. Unknown root source of GPS signal loss at this time.
10/13/2021	40.8502 28.8076	Turkey Mediterranean	JRC JLR-7800	A report from captain with Roxana Shipping Singapore indicating their JRC JLR-7800 GPS receivers experienced signal loss of satellites that where being tracked while off shore in the Sea of Marmara 12.3 nautical miles southwest of Istanbul, Turkey. The problem is ongoing. Unknown root source of GPS signal loss at this time.
10/25/2021	40.9500 28.9167	Turkey Mediterranean	Furuno GP-170	A report from mariner with Oldendorf Shipping indicating their Furuno GP-170 GPS receiver experienced signal loss of GPS satellites being tracked while off shore in the Sea of Marmara near the Istanbul Strait 2.5 nautical miles south of Zeytinburnu, Turkey. Multiple other ships reported the same problem. Unknown root source of GPS signal loss at this time.

DATE	LATITUDE LONGITUDE	NATION / WATERWAY	RECEIVER	SUMMARY
11/4/2021	35.8276 14.5456	Malta Mediterranean	Furuno GP-32	A report from captain aboard the *Balluta Bay* vessel indicating his Furuno GP-32 GPS receiver experienced GPS signal outage while navigating in the port bay of Marsaxlokk, Malta. The outage cleared and signal was recovered. Unknown root source of GPS signal loss at this time.
11/5/2021	34.6953 33.1975	Cyprus Mediterranean	SAAB R5 Supreme	A report from captain of the *Seabourn Encore* cruise ship indicating their SAAB R5 Supreme GNSS receivers experienced intermediate to complete GNSS signal loss of satellites that were being tracked while off shore 1 nautical mile south of the town Argaki Tis Moni off shore in Cyprus. The GPS Signal reception loss is ongoing and showing in all 3 on-board GNSS units. Unknown root source of GPS signal loss at this time.
11/7/2021	34.6983 33.1733	Cyprus Mediterranean	SAAB R5 Supreme	A report from captain of the *Seabourn Quest* cruise ship indicating their SAAB R5 Supreme GNSS receivers experienced complete GNSS signal loss of satellites that where being tracked while off shore 1.5 nautical miles southwest of the town Moni Mov Anchorage off shore in Cyprus. The GPS Signal reception loss is on-going and showing in all 3 on-board GNSS units. Quest crew suspects GPS signal loss is being caused by military vessels in the area at this time.
11/15/2021	34.6953 33.1975	Cyprus Mediterranean	SAAB R5 Supreme	A report from captain of the *Seabourn Encore* cruise ship indicating their SAAB R5 Supreme GNSS receivers experienced complete GNSS signal loss of satellites that where being tracked while off shore 2.8 nautical miles due south of the town Pyrgos in Cyprus. The GPS Signal reception loss is on-going. Unknown root source of GPS signal loss at this time.
11/23/2021	21.4648 39.0988	Saudi Arabia Persian Gulf	Furuno GP90	A report from captain aboard the *Britoil-64* tug vessel indicating their Furuno GP-90 GPS receiver lost signal reception while at 3.8 nautical miles southeast running up and down north of RTE-7 anchorage/east of tanker anchorage Ras Tunara in Saudi Arabia. Crew checked the area and many vessels indicate the same problem. Unknown root source of GPS signal reception problems at this time.
12/11/2021	-23.8023 -45.3811	Brazil South Atlantic	JRC JLR-7800	A report from Senior Dynamic Positioning Officer indicating their *Eagle Texas* capture vessel JRC JLR-7800 GPS receiver experienced GPS position shift on the ECDIS to bearing 039T, 0.47 nautical miles off actual position. Position was approximately 1.5 nautical miles east of Sao Sebastiao, Brazil. Unknown root source of GPS position shift at this time.
12/27/2021	-8.0252 -26.4578	Brazil South Atlantic	Furuno GP-170	A report from OSM Maritime Officer indicating their *Ghillie* crude oil tanker vessel Furuno GP-170 GPS receiver experienced GPS position fluctuations shown on the ECDIS shifting by 2.5 to 3 cables automatically from its actual position. Position was approximately 500 nautical miles east of Recife, Brazil. Unknown root source of GPS position shift at this time.

U.S. Department of Transportation
John A. Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142-1093

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

DOT-VNTSC-OSTR-21-03