Defense Systems Information Analysis Center

DSIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT

Resiliency of GPS/GNSS/PNT System Receivers

Report Number:

DSIAC-BCO-2023-466

Completed April 2025

DSIAC is a U.S. Department of Defense Information Analysis Center

MAIN OFFICE
4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443-360-4600

REPORT PREPARED BY:
Yeonjoon "Ethan" Park
Office: QinetiQ, Inc.

DSIAC is sponsored by the Defense Technical Information Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering. DSIAC is operated by the SURVICE Engineering Company.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
15-04-2025	Technical Research Report	

4. TITLE AND SUBTITLE

Resiliency of GPS/GNSS/PNT System Receivers

5a. CONTRACT NUMBER
FA8075-21-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Yeonjoon “Ethan” Park

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Defense Systems Information Analysis Center (DSIAC)
SURVICE Engineering Company
4695 Millennium Drive
Belcamp, MD 21017-1505

8. PERFORMING ORGANIZATION REPORT NUMBER

DSIAC-BCO-2023-466

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center (DTIC)
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

10. SPONSOR/MONITOR’S ACRONYM(S)

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

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution Statement A. Approved for public release: distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This report summarizes test and measurement methods and equipment to characterize the resiliency of various global navigation satellite systems, including the Global Positioning System (GPS) coarse acquisition code; P(Y) code; Selective Availability Antispoofing Module; GPS Block III M-code; and Link 16 multimodal position, navigation, and timing systems. In addition, basic working principles; spectral alignment; and conducted/radiated testing with multi-antenna configurations, including controlled reception pattern antenna tests, standard GNSS test parameters, and additional PNT systems such as the Southern Positioning Augmentation Network Satellite-Based Augmentation System are reviewed.

15. subject terms
global navigation satellite system; Global Positioning System receiver; test and measurement; position, navigation, and timing; resiliency

16. SECURITY CLASSIFICATION OF: U			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU	27	Ted Welsh, DSIAC Director
U	U	U			**19b. TELEPHONE NUMBER** *(include area code)* 443-360-4600

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Distribution Statement A. Approved for public release: distribution is unlimited.

About

DTIC and DSIAC

The Defense Technical Information Center (DTIC) preserves, curates, and shares knowledge from the U.S. Department of Defense's (DoD's) annual multibillion-dollar investment in science and technology, multiplying the value and accelerating capability to the Warfighter. DTIC amplifies this investment by collecting information and enhancing the digital search, analysis, and collaboration tools that make information widely available to decision-makers, researchers, engineers, and scientists across the Department.

DTIC sponsors the DoD Information Analysis Centers (DoDIAC), which provide critical, flexible, and cutting-edge research and analysis to produce relevant and reusable scientific and technical information for acquisition program managers, DoD laboratories, Program Executive Offices, and Combatant Commands. The IACs are staffed by, or have access to, hundreds of scientists, engineers, and information specialists who provide research and analysis to customers with diverse, complex, and challenging requirements.

The Defense Systems Information Analysis Center (DSIAC) is a DoDIAC sponsored by DTIC to provide expertise in 10 technical focus areas: weapons systems; survivability and vulnerability; reliability, maintainability, quality, supportability, and interoperability (RMQSI); advanced materials; military sensing; autonomous systems; energetics; directed energy; non-lethal weapons; and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). DSIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001.

TI Research

A chief service of the DoDIAC is free technical inquiry (TI) research limited to four research hours per inquiry. This TI response report summarizes the research findings of one such inquiry. Given the limited duration of the research effort, this report is not intended to be a deep, comprehensive analysis but rather a curated compilation of relevant information to give the reader/inquirer a "head start" or direction for continued research.

Abstract

This report summarizes test and measurement methods and equipment to characterize the resiliency of various global navigation satellite systems, including the Global Positioning System (GPS) coarse acquisition code; P(Y) code; Selective Availability Antispoofing Module; GPS Block III M-code; and Link 16 multimodal position, navigation, and timing systems. In addition, basic working principles; spectral alignment; and conducted/radiated testing with multi-antenna configurations, including controlled reception pattern antenna tests, standard GNSS test parameters, and additional PNT systems such as the Southern Positioning Augmentation Network Satellite-Based Augmentation System are reviewed.

Contents

List of Figures

List of Tables

1.0 TI Request

1.1 Inquiry

What are good methodologies for measuring the resilience of position, navigation, and timing (PNT) systems?

1.2 Description

The inquirer asked for vulnerability assessment techniques for global navigation satellite systems (GNSSs). Of interest is the impact on the end user of the equipment, with the ultimate objective of delivering a standard set of requirements to the inquirer to enable the specification and testing of GNSS vulnerabilities. The inquirer requested the search be limited to air, land, and sea domains for deployed military platforms and force elements, including the following areas of consideration: susceptibility, vulnerability, recoverability, and maintainability related to the valid operation of user equipment and the follow-on impact on platform systems and subsystems.

The focus should be on direct threats to the user equipment and the consequent impact on subsystems that rely on a data feed for the user equipment. This could also include technical capabilities, such as abilities to respond to threats/vulnerabilities and mitigate impacts to end users and the ability of intel centers to provide detailed and accurate updates rapidly enough to support forces in creating/enacting counters and mitigation strategies and tools, etc.

2.0 TI Response

A GNSS receiver is a common building block of PNT systems and guides modern vehicles (air/ground/sea/space), unmanned systems, and weapons. Therefore, it is important to understand and measure the resiliency of GNSS receivers in the presence of hostile interference conditions for the defense and security of U.S. and allied countries. This report addresses the scope of test and measurement methods of various GNSS receivers installed on moving vehicles, unmanned systems, and/or weapons, as per the original request. It does not cover the details of satellite constellation systems in space.

2.1 General Working Principles of Global Positioning Systems (GPS)/GNSS

GPS and more general GNSSs work with a time-of-arrival (TOA) method with a synchronized clock or a time-difference-of-arrival (TDOA) method without a synchronized clock. Most of the

GPS/GNSS receivers use the TDOA method to determine their position because the clocks synchronized to satellites are very expensive and, hence, generally limited in use to government and military equipment requiring robust and highly accurate PNT. In the TDOA method, the receiver can determine a two-dimensional (2-D) position on the ground with three satellite emitters and a three-dimensional (3-D) position, including altitude, with four satellite emitters. The satellites are synchronized and, at the same time, emit pulse signals that contain position data (Figure 1.) The receiver calculates a hyperbolic line from the time difference of t1–t2 and calculates another hyperbolic line from the time difference of t2–t3. The crossing point of two hyperbolic lines determines the receiver's 2-D position on the ground. Similarly, the receiver can get the 3-D position by the crossing point of hyperbolic surfaces from four satellites.

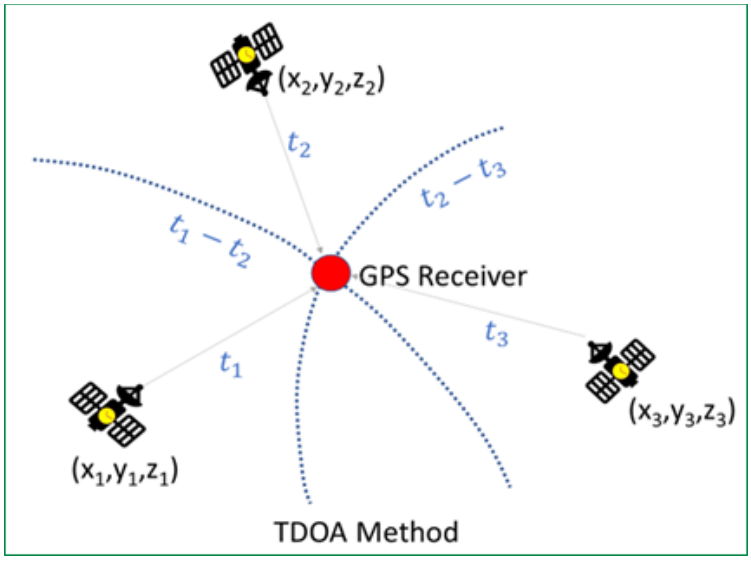

Figure 1. TDOA Method to Determine the Position of a GPS Receiver From Multiple Satellites *(Source: Y. Park).*

2.2 GPS Coarse Acquisition (C/A) Code and Military P(Y) Code

GPS C/A code is the most fundamental signal to provide the TOA and TDOA data. The encrypted military P(Y) code signal is 90° out of phase to C/A code signal and provides the additional accuracy and verification of the authenticity of C/A signal.

2.2.1 GPS Signal Power and Threats

GPS/GNSS signals on the ground are weak because the distance to the satellites is very long and the power source on the satellite is very limited. GPS signals are in the range of –125 to –155 dBmW in outdoor settings [1]. For comparison, 4G LTE cell phones have a range of –80 to –100 dBmW. This means GPS signals are 10,000× weaker than cell phone signals.

2.2.2 Power Spectral Density Diagrams

Figure 2 shows the signal power spectrum alignment of a C/A code and military P(Y) code, which is 90° out of phase from C/A code. For example, both are centered at 1575.42 MHz, the L1 center frequency, but their distribution of spectrum power on frequencies is different. Encrypted P(Y) code can verify the authentication of C/A code and improves the accuracy of the positioning.

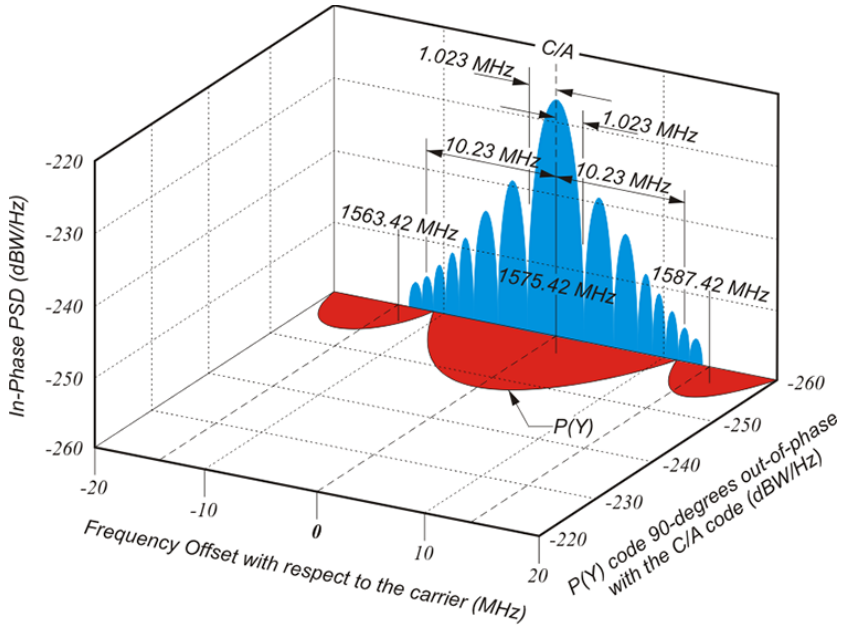

Figure 2. Power Spectral Density Diagram of C/A Code and P(Y) Code in a GPS Signal [2].

2.2.3 Selective Availability Antispoofing Module (SAASM)

SAASM is used by military GPS receivers to allow decryption of precision GPS observations. SAASMs allow "an approved government or military user to access the encrypted P(Y) signal transmitted by the GPS constellation" [3]. P(Y) gives better location precision compared with the C/A signal, "provid[ing] signal integrity assurance to protect against active spoofing attacks." A spoofer can simulate the standard C/A signal and, with time, pass the threshold needed to overpower the GPS signal strength. The spoofing signal "adjust[s] to make the attacked receiver report an incorrect position and time." The C/A GPS receiver accepts the spoofing communication instead of declining it.

SAASM allows satellite authentication, over-the-air rekeying, and contingency recovery. "SAASM systems can be updated with an encrypted 'black key' that may be transmitted over unclassified channels. All military receivers deployed after the end of September 2006 must

use SAASM" [2]. It does not provide any additional antijam capability; however, the higher data (chipping) rate of P(Y) code can provide a higher processing gain, which will provide better tracking performance in a jamming environment. Later GPS upgrades, such as M-code, provide additional improvements to antijam capabilities.

2.3 Types of GNSS and Radio-Frequency (RF) Spectrum Structure

After the success of U.S. GPS systems for military, civilian, and commercial applications, several similar GNSS systems were developed by other countries: the Global Navigation Satellite System (GLONASS) (Russia), BeiDou (China), Galileo (European Union), Quasi-Zenith Satellite System (Japan), and Navigation With Indian Constellation (India) [4].

2.4 GNSS Receiver Output

A GNSS receiver can output data in various formats, but the National Marine Electronics Association (NMEA) data format is most widely used.

2.4.1 NMEA Data Formats and Specifications

A GNSS receiver uses NMEA data-format output with various ports including universal asynchronous receiver-transmitter (uART), recommended standard (RS)-232C, universal serial bus (USB), etc. The following shows a GPS NMEA message format in detail:

> Message Headers: $GPGGA, $GPGSV, $GPGLL, $GPVTG…each carries different information.
>
> $GPGGA,202530.00,5109.0262,N,11401.8407,W,5,40,0.5,1097.36,M,-17.00,M, 18,TSTR*61
>
> Label,UTC-time,Latitude(DDmm.mm),N/S,Longitude,E/W,Quality,#Sats, hdop,Altitude,unit,undulation,u-units,age,base-station-id,*Check-Sum

Figure 3 provides an example of the $GPGGA message.

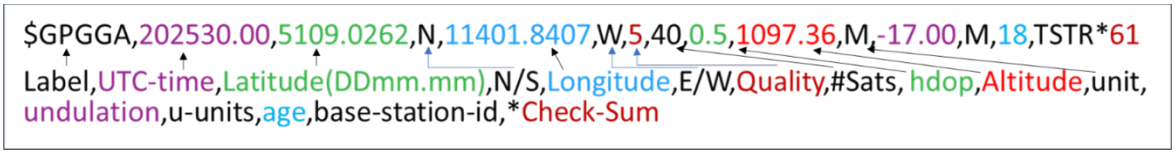

Figure 3. $GPGGA Message Example *(Source: Y. Park).*

The following describes a basic real-time monitoring of GPS signal health from NMEA messages, with examples in Table 1.

Table 1. Example of GPS NMEA Sentences [5]

NMEA Sentence	Meaning
GPGGA	GPS Fix Data (Time, Position, Fix-Type Data)
GPGLL	Geographic Position, Latitude, Longitude
GPVTG	Course and Speed Information Relative to the Ground
GPRMC	Time, Date, Position, Course, and Speed Data
GPGSA	GPS Receiver Operating Mode, Satellites Used in the Position Solution, and Dilution-of-Precision Values
GPGSV	Number of GPS Satellites in View Satellite Identification (ID) Numbers, Elevation, Azimuth, and Signal-to-Noise Ratio (SNR) Values
GPMSS	SNR, Signal Strength, Frequency, and Bit Rate From a Radio Beacon Receiver
GPTRF	Transit Fix Data
GPSTN	Multiple Data ID
GPXTE	Cross-Track Error, Measured
GPZDA	Date and Time (Pulse per Second [PPS] Timing Message, Synchronized to PPS)
150	Okay to Send Message

- Most GPS receiver's $GPGGA data packet contains quality factor, number of satellites, horizontal dilution of precision (HDOP), and relative accuracy. These can be the measurement factors in real time to monitor the health of GNSS signals.

  For example, the data (Quality, # of Sats, HDOP) can show the overall quality of the GPS signal. The accumulated counting of the last element Check-Sum verification shows the health of communication because the erroneous data packet does not match Signal the Check-Sum.

  $GPGGA,202530.00,5109.0262,N,11401.8407,W,5,40,0.5,1097.36,M,-17.00,M,18,TSTR*61

  Label,UTC-time,Latitude(DDmm.mm),N/S,Longitude,E/W,Quality,#Sats,hdop,Altitude,unit,undulation,u-units,age,base-station-id,*Check-Sum

- Most GPS receiver's $GPGSV data packet contains GPS satellite information and SNR information in the eighth data field (the first 42 in the following example) in decibels (00–99 dB) with null value for "not tracking."

  $GPGSV,4,3,16,31,11,329,42,05,10,169,42,24,07,212,44,04,01,033,*7C

- An advanced GPS receiver chip has additional data packets such as $GPMSS, which contains SNR, signal strength, frequency, and bit rate. These data can be used to monitor the health of a GNSS signal.

- A multiconstellation GNSS receiver uses similar data formats with different starting labels. For example, GLONASS uses $GL*** and GALILEO uses $GA*** instead of $GP***. A configuration policy setting can be used to select valid signals and reject hostile signals. For example, a GNSS receiver can be configured to use GPS and Galileo signals and reject other signals, such as GLONASS and BeiDou.

2.4.2 GPS Navigation Messages

Multiple GPS messages have been introduced. Table 2 summarizes subframe and data message specifications for each system variation [6].

Table 2. Summary of Subframe and Data Message Specifications

Name of System	System Specifications
"Legacy" L1 C/A Navigation Message (Civil)	• Subframe 1: satellite health, clock status • Subframes 2 and 3: contain satellite ephemeris • Subframe 4: ionospheric model parameters, universal coordinate time (UTC) information, part of the almanac, antispoofing activation information • Subframe 5: Almanac data and constellation status; quick satellite detection; 25 frames needed to complete almanac
L2-CNAV (Civil)	• Messages broadcast in a flexible order with variable repeat cycles • Messages composed of fixed data • Forward error correction (FEC) and advanced error detection (such as a cyclic redundancy check) are used to achieve better error rates and reduced data collection times
L5-CNAV (Civil)	• Modulated onto the L5I signal component • Essentially the same information data as L2-CNAV • Message structure is the same as L2-CNAV, but its content may vary slightly
CNAV-2 (Civil)	• Modulated onto the L1C signal and consists of: o Subframe 1: (9 bits) provides time of internal o Subframe 2: (600 bits) provides clock and ephemeris data o Subframe 3: (274 bits) provides other navigation data, which is commutated over multiple pages

Note: CNAV = civil navigation.

2.5 Single-Antenna GNSS Receiver Test and Measurement

Most common GPS receivers use a single antenna to receive a GPS signal. Multiple RF signals from numerous satellites can be received by a single antenna.

2.5.1 Test Configuration: Conducted Test and Radiated Test

A GPS receiver test is divided into two configurations: (1) conducted test and (2) radiated test (Figure 4). A conducted test has a direct connection between the GPS signal generator and the RF input port of the GPS receiver, and it is used to test the GPS receiver chip alone without an antenna's effects. A radiated test has a standard transmit antenna and a GPS receiver antenna to characterize the GPS receiver chip and receiver antenna together. Multiple antennas can be installed and tested if the GPS receiver chip supports multi-antenna configuration.

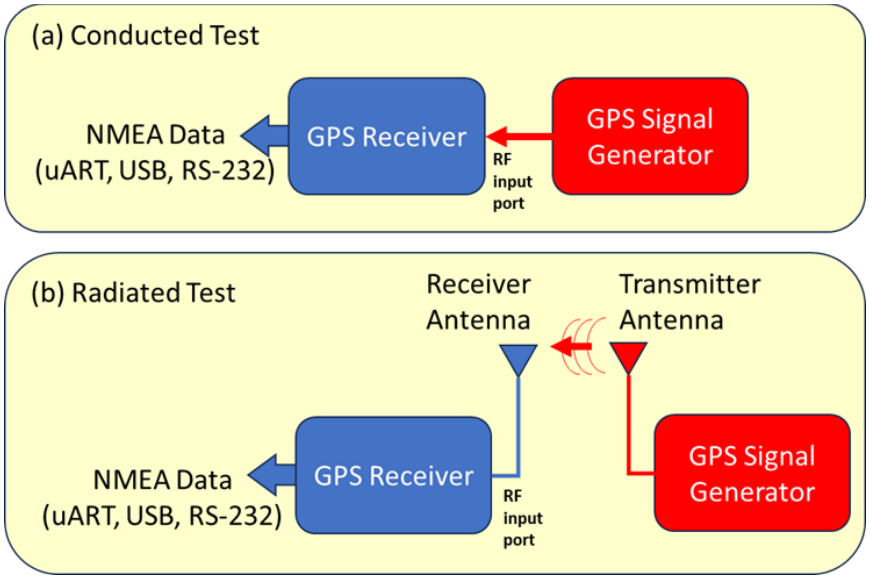

Figure 4. Two Test Configurations of a GPS Receiver *(Source: Y. Park)*.

2.5.2 GPS Simulators

Commercial GPS simulators were developed to broadcast L1 and L2 signals simultaneously. For example, a Keysight N7609B GPS simulator generates C/A code, navigation data, and P code and mixes them to L1 carrier and L2 carrier to generate simulated, multiband GPS signals, as shown in Figure 5.

Modern GPS simulators can create a multitude of emulated GPS signals based on the theoretical position of a receiver and satellite constellations at a different position and times and mix additional interference signals, such as a jamming signal whose intensity changes by the position of the jammer and receiver as well. Some GPS simulators support the simulation of a moving receiver along a predefined path with a fixed/moving jammer position.

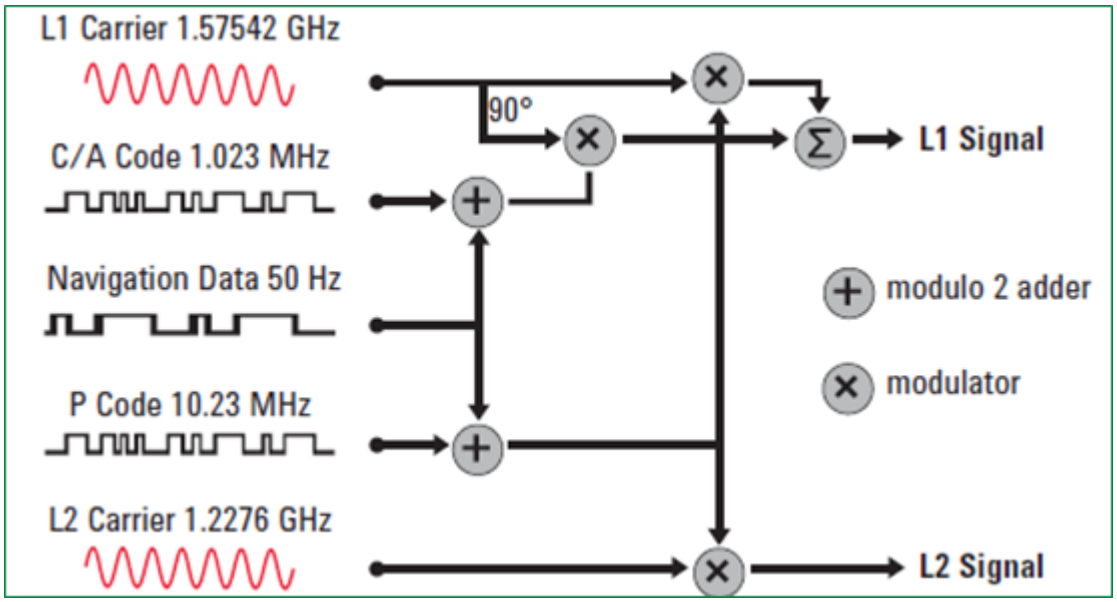

Figure 5. Signal Modulation Diagram of a GPS Simulator, Keysight N7609B [7].

2.5.3 Standard Test Parameters

The following three parameters of GPS resiliency are measured with standard tests.

1. Susceptibility: Sensitivity test of a GPS receiver with weak signals in different environments, such as an urban condition with partially blocked signals and multipath interference.
2. Vulnerability: GPS receiver test with a user-defined jamming and spoofing. Jamming/spoofing power/type/source position and receiver position can be inserted into a GPS simulator.
3. Recoverability: GPS receiver test under a moving condition with fixed-point jamming and/or spoofing. Tracking accuracy and deviation are measured as the receiver moves toward and away from the jamming/spoofing source position.

Modern GPS simulators measure the following parameters as a standard to characterize GPS receivers. GPS test parameters involve time to first fix (TTFF), location accuracy, reacquisition time, and sensitivity testing.

2.5.3.1 TTFF. According to KeySight Technologies [7]:

> When a receiver is turned on, it must do some searching to find the satellite signals—this process is called acquisition. It must then track the signals and compute a position. The time from turn on to the availability

> of the first valid location fix is called time to first fix, or TTFF. TTFF is a critical parameter for testing GPS receivers. It relates directly back to a user desire, which is to have a location fix as soon as possible.

The terms hot start, cold start, and warm start are used when referring "to the data that is available to the receiver when it is turned on." These data are used "as a 'hint' to make it easier to search for active satellite signals" [7].

KeySight Technologies refers to hot start as [7]:

> If the receiver has been off for a short time (less than an hour or two) and has not moved much (100 meters or less), it will have fairly accurate information on satellites and can typically use this information to acquire satellite signals and compute a position relatively rapidly. This scenario is termed a hot start and may be the case that results from a short power interruption or a battery change.

Warm start is when the receiver is off longer than a hot start "or moved farther while it was powered off" [7]. The receiver knows "what time it is (approximately) but it doesn't really know where it is."

Finally, cold start refers to when GPS receivers "are started up with no data as to what time it is or where the satellites are located" [7].

KeySight Technologies notes that [7]:

> In this mode, the receiver's first job is to acquire satellite signals. In order to do this, it must search each of the available [code-division multiple-access] CDMA codes, as well as the frequency space over a range of ±5000 Hz of Doppler shift. This is a fairly difficult task, which requires signals of relatively strong amplitude and may take quite a long time. In older receivers, it may take several minutes. In newer receivers, the timeframe has been reduced so that it is on the order of 10 to 20 seconds. With a cold start, the receiver must receive at least 18 seconds of good data from each satellite in order to receive an accurate description of the satellite's orbit (known as ephemeris data). Once done, the receiver will have sufficient information to compute its first location fix. TTFF for cold-start conditions are typically longer than either

hot-start or warm-start conditions. Modern receivers can achieve the TTFF in less than a minute. Cold-start TTFF is an important parameter for GPS receivers and is typically one of the first parameters to test in a GPS receiver.

2.5.3.2 Location Accuracy. This "refers to the ability to achieve a location fix that is as close as possible to the desired position, both in repeatability and accuracy" [7]. There are three variations: (1) a relative location accuracy test, (2) the absolute location accuracy test, and (3) moving or dynamic location accuracy tests.

Relative location accuracy tests compare "the location fixes obtained by cold/warm/hot starting, while at the same time locating and comparing the variation between fixes" [7]. Accurate location fixes occur with low variations, useful when a user "want[s] to return to the same location, using the same receiver—but [does not] care…about how close the longitude/latitude/altitude numbers are to the actual location." Absolute location accuracy tests compare "the location fixes obtained by cold/warm/hot starting, while at the same [time are] locating and comparing the variation between the location fixes and the ideal location provided by the scenario." Finally, moving/dynamic location accuracy tests "simulate movement of the receiver while conducting the accuracy tests" mentioned earlier.

2.5.3.3 Reacquisition Time. The performance of a receiver "in a scenario where the signal is greatly reduced or interrupted for some short period of time and is then restored" is referred to as reacquisition time [7]. Results are typically "compared with signals above the minimum sensitivity levels (good signal conditions)."

2.5.3.4 Sensitivity. There are two sensitivity levels for GPS receivers: (1) acquisition and (2) tracking sensitivity [7]:

> [Acquisition sensitivity] refers to the minimum signal level that allows the receiver to successfully perform a cold start TTFF within a specified timeframe. During the signal acquisition process, the signal level must be higher than during the tracking process because the time synchronization is not known. An example of this may be identified as the minimum power level to allow a successful cold-start TTFF of 100 seconds or less.
>
> [Tracking sensitivity is] the minimum signal level that allows the receiver to maintain a location fix within some specified degree of accuracy. This is generally a much lower signal level than the acquisition sensitivity level.

As the signal level is reduced, the ability of the receiver to recover the navigation message data stream will decrease and bit errors will be induced. However, since the Doppler frequency and the timing of the signal are known, the tracking loops can still operate successfully. As signal levels continue to decrease, eventually the noise will be so great that it will introduce noise into the tracking loops and the time and/or frequency synchronization will degrade. These conditions will begin to impact the accuracy of the location fix. As the signal level continues to decrease, the system will incrementally lose the ability to track satellites until eventually the receiver is not able to compute a location fix.

Some GPS simulators, such as the VIAVI GPSG-1000 and Safran Skydel GNSS simulators, can accept a predefined moving path file with a velocity of a GPS receiver and generate theoretical GPS signals at the receiver on the move. Doppler shift by the moving velocity of the receiver can be included in the signal generation.

2.6 Controlled Reception Pattern Antenna (CRPA) Test for Multi-Antenna Directional Anti-Jamming GPS Receivers

An advanced GPS receiver can have multiple directional antennas to distinguish true satellite signals from environmental noise or man-made RF-jamming signals. A CRPA test is intended to characterize these kind of directional anti-jamming GPS receivers.

2.6.1 Working Principle

In typical situations, GPS signals come from the sky but the jamming signal comes from a horizontal direction from something like an enemy's electronic warfare jammer on the ground. Figure 6 shows a simple, hypothetical CRPA antenna's working principle. CRPA uses multiple directional antennas to receive a jamming signal from the horizontal direction for noise sampling and to receive a combined signal of GPS and jamming signals from the above antenna. A fast processor then subtracts the jamming signal from the combined signal so that it can retrieve the pure GPS signals. This working principle is very like a directional noise-canceling microphone. The process can be described in simple mathematics with each antenna's signal coupling factors α, β.

$$\text{Input From Horizontal Directional Antenna} = \alpha \cdot \text{Jamming Signal}$$
$$\text{Input From Above Directional Antenna} = \text{GPS signals} + \beta \cdot \text{jamming signal}$$

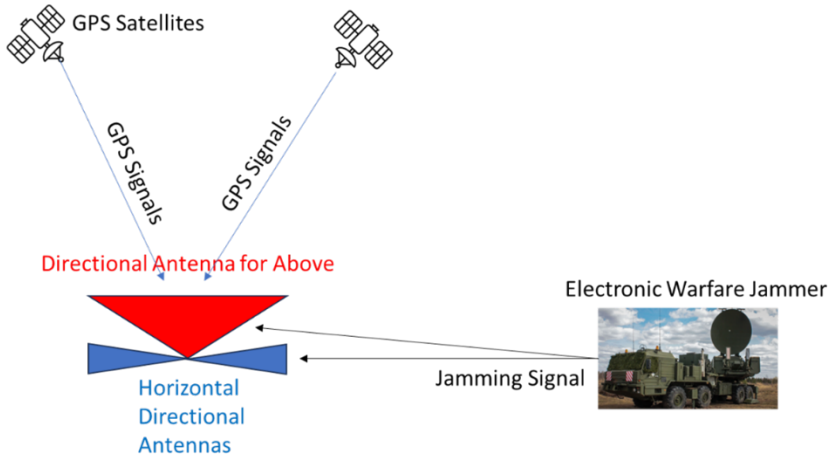

Figure 6. Multidirectional CRPA Antennas Receiving a GPS Signal From Above and Jamming Signals From the Ground *(Source: Y. Park)*.

A noise-canceling process subtracts the jamming signal from the horizontal antenna with a proper weighting factor, *W*:

$$\text{Processed Data} = \text{GPS Signals} + \beta \cdot \text{Jamming Signal} - W \cdot \alpha \cdot \text{Jamming Signal}$$
$$= \text{GPS Signal} \ \ (\text{When } W \cong \frac{\beta}{\alpha})$$

A commercial CRPA anti-jamming antenna, such as Hexagon NovAtel anti-jam antenna systems Global Positioning System anti-jam technology, can get the GPS signal with 40 dB of noise power suppression. CRPAs adapt in response to jamming or spoofing signals.

2.6.2 Test Configuration

The CRPA test uses a radiated test in an anechoic chamber with multiple transmit antennas to emulate GNSS signals and jammer signals. Fixed-chamber and zoned-chamber configurations are available [8].

2.6.3 CRPA GPS Testers and Antennas

Several vendors provide CRPA GPS testers. The following is a list of CRPA GPS testers and antenna [8]:

- Spirent GNSS Simulator With Zoned Chamber
  - GSS9000 Advanced Multi-Element GNSS Simulation System
  - GSS9790 GNSS Signal Simulator
  - GSS7000 GNSS Signal Simulator
  - GSS7765 Interference Generator
  - SimGEN Software

  - Sim3D
  - SimINERTIAL
- CAST Navigation Fixed Reception Pattern Antenna/CRPA Tester
- Safran Skydel Anechoic Simulator System
- CRPA Anti-Jam Antenna Systems by NovAtel

2.7 GPS Block III Signals

"GPS Block III (previously Block IIIA) consists of the first 10 GPS III satellites and is used to keep the Navstar GPS operational. Lockheed Martin designed, developed, and manufactured the GPS III Nonflight Satellite Testbed and all 10 Block III satellites" [9].

Table 3 shows the GPS Block III satellites in operation and those available for future use.

Table 3. List of GPS Block III Satellites [9]

Satellite	USA Designation	SVN	Name	Launch Date (UTC)	Rocket	Status
GPS III-01	USA-289	74	Vespucci	23 December 2018 (13:51)	Falcon 9 Block 5	In Service
GPS III-02	USA-293	75	Magellan	22 August 2019 (13:06)	Delta IV M+ (4,2)	In Service
GPS III-03	USA-304	76	Matthew Henson	30 June 2020 (20:10)	Falcon 9 Block 5	In Service
GPS III-04	USA-309	77	Sacagawea	5 November 2020 (23:24)	Falcon 9 Block 5	In Service
GPS III-05	USA-319	78	Neil Armstrong	17 June 2021 (16:09)	Falcon 9 Block 5	In Service
GPS III-06	USA-343	79	Amelia Earhart	18 January 2023 (12:24)	Falcon 9 Block 5	In Service
GPS III-07	—	80	Sally Ride	May 2024	Vulcan Centaur VC0S	Available for Launch
GPS III-08	—	81	Katherine Johnson	February 2025	Vulcan Centaur TBA	Available for Launch
GPS III-09	—	82	Ellison Onizuka	FY2026	TBA	Available for Launch
GPS III-10	—	83	Hedy Lamarr	FY2026	TBA	Available for Launch

2.7.1 Military M-Code Signal

A major component of the modernization process, a new military signal called M-code was designed [9]:

> …to further improve the antijamming and secure access of the military GPS signals. The M-code is transmitted in the same L1 and L2 frequencies already in use by the previous military code, the P(Y) code.

The new signal is shaped to place most of its energy at the edges, away from the existing P(Y) and C/A carriers. Unlike the P(Y) code, the M code is designed to be autonomous, meaning that users can calculate their positions using only the M-code signal. P(Y) code receivers must typically first lock onto the C/A code and then transfer to lock onto the P(Y)-code.

In a major departure from previous GPS designs, the M-code is intended to be broadcast from a high-gain directional antenna, in addition to a wide-angle (full Earth) antenna. The directional antenna's signal, termed a "spot beam," is intended to be aimed at a specific region (i.e., several hundred kilometers in diameter) and increase the local signal strength by 20 dB (10× voltage field strength, 100× power). A side effect of having two antennas is that, for receivers inside the spot beam, the GPS satellite will appear as two GPS signals occupying the same position.

Other M-code characteristics are [9]:

- Satellites will transmit two distinct signals from two antennas: (1) one for whole-Earth coverage and (2) one in a spot beam.
- It has binary offset carrier modulation.
- It occupies 24 MHz of bandwidth.
- It uses a new military navigation (known as MNAV) message, which is packetized instead of framed, allowing for flexible data payloads.
- There are four effective data channels; different data can be sent on each frequency and on each antenna.
- Pit can include FEC and error detection.
- The spot beam is ~20 dB more powerful than the whole-Earth coverage beam.
- M-code signal at Earth's surface: –158 dBW for whole-Earth antenna, –138 dBW for spot-beam antennas.

Figure 7 shows that the M-code signal is located at the edge of C/A-code, at the minimum intensity point of P(Y) code. The left image of Figure 7 shows the normal condition, and the right image shows the jamming condition in which the jamming signal blocks the C/A signal. Note that the M-code signal is still not blocked by the spot jamming signal targeted at C/A code because M-code is away from the center of C/A signal.

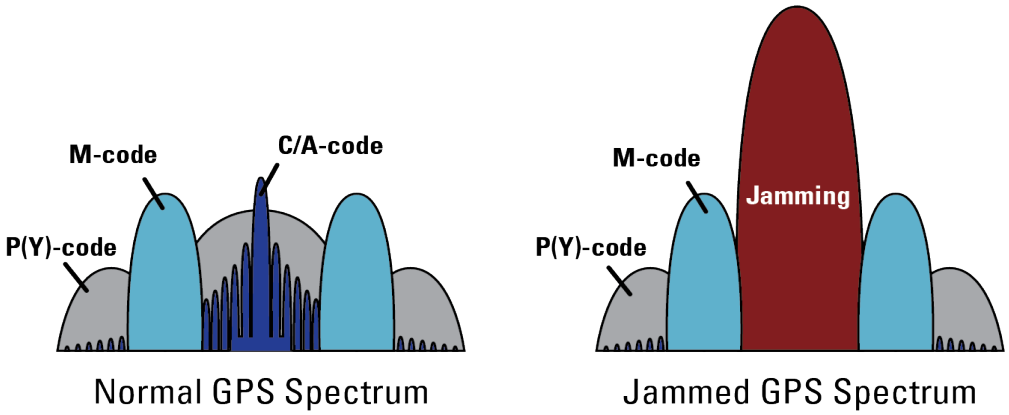

Figure 7. Power Spectrum of M-Code Signal in Normal Condition (Left) and Jamming Condition (Right) [10].

2.7.2 M-Code GPS Testers

GPS Block III M-code is securely encrypted so that a normal GPS simulator cannot generate the M-code signal in real time. Therefore, in the testing, a prerecorded M-code is used (Safran MNSA M-code tester [11]) or an official pre-encrypted M-code is used (Spirent SDS M-code tester [12]).

2.8 Satellite-Based Augmentation System (SBAS)

A regional SBAS can amplify and improve the performances of GNSSs by [13]:

> …improving the accuracy and reliability of GNSS information by correcting signal measurement errors and providing information about the accuracy, integrity, continuity, and availability of its signals.
>
> SBAS uses GNSS measurements taken by accurately located reference stations deployed across an entire continent. All measured GNSS errors are transferred to a central computing center, where differential corrections and integrity messages are calculated. These calculations are then broadcast over the covered area using geostationary satellites that serve as an augmentation, or overlay, to the original GNSS message.

Figure 8 shows the existing SBASs worldwide, which include [13]:

- United States: Wide-Area Augmentation System (WAAS)
- Japan: Michibiki Satellite Augmentation System (MSAS)
- India: GPS-Aided Geostationary Orbit-Augmented Navigation (GAGAN)

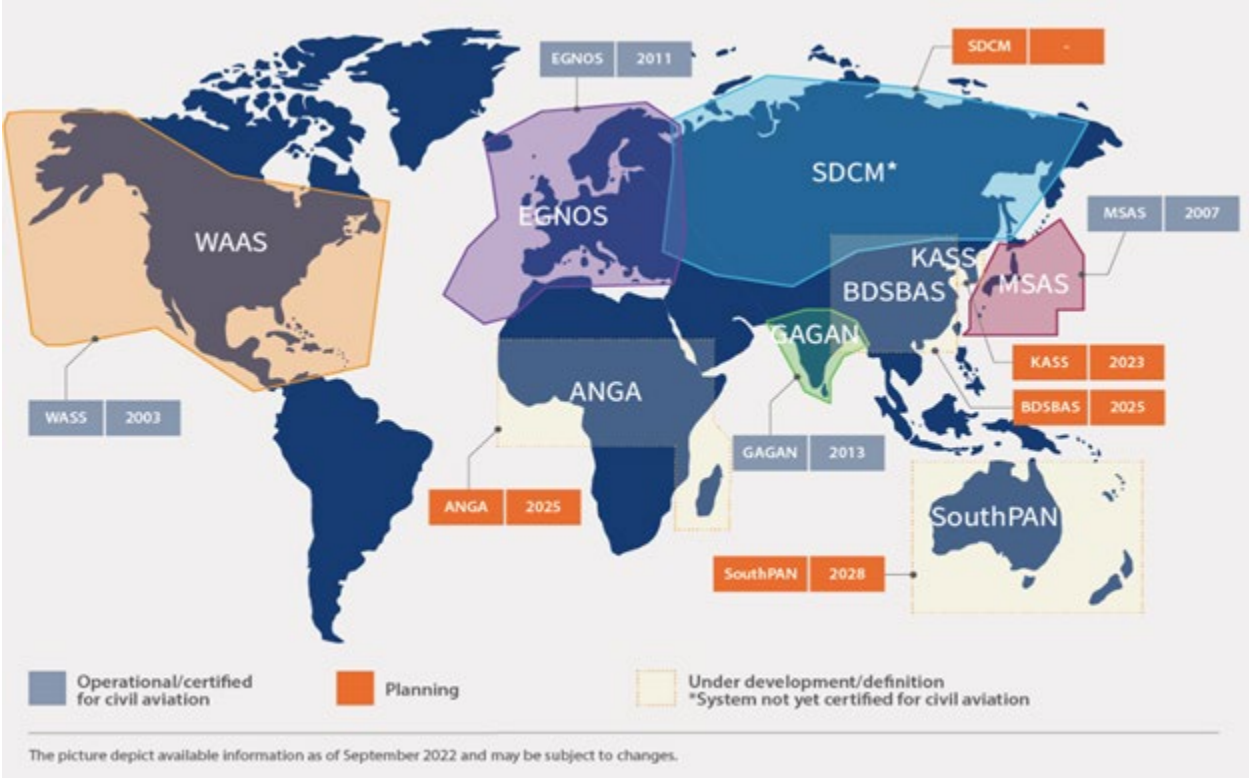

Figure 8. SBAS Indicative Service Area [13].

- China: BeiDou Satellite-Based Augmentation System (BDSBAS) (in development)
- South Korea: Korea Augmentation Satellite System (KASS) (in development)
- Russia: System for Differential Corrections and Monitoring (SDCM) (in development)
- Africa and Madagascar (the Agency for Aerial Navigation Safety in Africa and Madagascar [ASECNA]): Augmented Navigation for Africa (ANGA) (in development)
- Australia and New Zealand: Southern Positioning Augmentation Network (SouthPAN) (in development)

SouthPAN is a "joint initiative of the Australian and New Zealand governments that provides a SBAS for Australia and New Zealand" and will implement the following services [14]:

- L1 SBAS: L1 SBAS augments GPS and is an aeronautical radio navigation service (ARNS). This signal will be used for safety-of-life applications and, therefore, needs to

be certified by the National Aviation Authorities (i.e., the Australian Civil Aviation Safety Authority and New Zealand Civil Aviation Authority).

- Dual-Frequency Multiconstellation (DFMC) SBAS: DFMC SBAS is a future ARNS that is defined in an International Civil Aviation Organization Annex 10 Amendment 93 [15]. This service will have the potential to be certified as a safety critical system for aviation and other sectors in the future.
- Precise Point Positioning via SouthPAN (PVS): PVS service will provide horizontal accuracies of 15 cm (95% confidence) to a range of industries following a convergence time in the tens of minutes. The PVS service will be open access and able to be incorporated into mass-market GNSS devices across Australia and New Zealand and their maritime zones.

2.9 Advanced GNSS Receiver Chip

Advanced GNSS receivers must support multiconstellations, SAASM with C/A code and P(Y) code together, and the connection to the CRPA anti-jamming antenna. One example is the QinetiQ Q40 GNSS receiver, which was specifically developed with resiliency in mind to support high-assurance PNT for mission-critical applications in challenged environments.

References

[1] Spirent Federal Systems, Inc. "Fundamentals of GPS Threats." Spirent Whitepaper DWP0003, Issue 1-02, https://www.spirent.com/assets/wp-fundamentals-of-gps-threats, 2023.

[2] Van Sickle, J. "The Legacy Signals and Power Spectral Density Diagrams." John A. Dutton e-Education Institute, College of Earth and Mineral Sciences, The Pennsylvania State University, V3 Consultants, Lakewood, CO, https://www.e-education.psu.edu/geog862/node/1861, accessed on 21 August 2023.

[3] Safran. "GPS Security With SAASM." https://safran-navigation-timing.com/gps-security-with-saasm/, accessed on 10 April 2025.

[4] Wikimedia Foundation, Inc. "Satellite Navigation." Wikipedia, https://en.wikipedia.org/wiki/Satellite_navigation, accessed on 21 August 2023.

[5] RF Wireless World. "GPS Sentence/NMEA Sentences/GPGCA GPLL GPVTG GPRMC." https://www.rfwireless-world.com/Terminology/GPS-sentences-or-NMEA-sentences.html, accessed on 21 August 2023.

[6] Sanz Subirana, J., J. M. Juan Zornoza, and M. Hernández-Pajares. "GPS Navigation Message." University of Catalunia, Spain, https://gssc.esa.int/navipedia/index.php/GPS_Navigation_Message, 2011.

[7] Keysight Technologies. "GPS Receiver Testing: Application Note 5990-4943EN." https://www.keysight.com/us/en/assets/7018-02367/application-notes/5990-4943.pdf, accessed on 21 August 2023.

[8] Spirent Communications. "Characterizing CRPAs and Other Adaptive Antennas." Spirent Whitepaper DWP0015, Issue 1-01, https://www.spirent.com/assets/white-paper-testing-crpas-and-other-adaptive-antennas, March 2021.

[9] Wikimedia Foundation, Inc. "GPS Block III." Wikipedia, https://en.wikipedia.org/wiki/GPS_Block_III#:~:text=%2DGPS%2D200.-,Military%20(M%2Dcode),the%20P(Y)%20code, accessed on 21 August 2023.

[10] Simmonds, A. "Can GPS Be Trusted? Part 2." Mercury: Blogs and Podcasts, https://www.mrcy.com/company/blogs/can-gps-be-trusted-part-2, 28 October 2018.

[11] Safran Electronics and Defense. "# Use Cases: MNSA M-Code Testing in Defense Applications." Safran, https://safran-navigation-timing.com/mnsa-m-code-testing-in-defense-applications/, accessed on August 2023.

[12] Spirent Federal Systems, Inc. "SDS M-Code Tester: Testing M-Code Using Simulator Data Sets." Spirent Federal Systems, https://spirentfederal.com/products/sds-m-code/, accessed on 21 August 2023.

[13] European Union Agency for the Space Programme. "What Is SBAS?" EUSPA, https://www.euspa.europa.eu/european-space/eu-space-programme/what-sbas, accessed on 21 August 2023.

[14] Geoscience Australia. "Southern Positioning Augmentation Network (SouthPAN)." Australian Government: Geoscience Australia, https://www.ga.gov.au/scientific-topics/positioning-navigation/positioning-australia/about-the-program/southpan, 19 June 2023.

[15] International Civil Aviation Organization. "Aeronautical Telecommunications, Volume 1–Radio Navigation Aids." Annex 10, Amendment 93, Montreal, Canada, forthcoming publication, https://store.icao.int/en/annexes/annex-10, accessed on 21 August 2023.

Biography

Dr. Yeonjoon Park received his Ph.D. in Engineering from the University of California at Berkeley in 2003. He supported the National Aeronautics and Safety Administration (NASA) Langley Research Center as a staff researcher at the National Institute of Aerospace for 12 years. He designed and built a 20-ft-sized solar-and-microwave-powered airship drone under a U.S. Department of Transportation-NASA collaboration. Recently, he advised and supported a counter-unmanned aircraft system team at the U.S. Department of Homeland Security (DHS) Customs and Border Patrol (CBP) for three years as a subject matter expert working for QinetiQ Inc. Dr. Park is a distinguished inventor, with over 30 U.S. and international patents and is a recipient of the R&D 100 Award (United States), Solar Industry Award (European Union), and High Effectiveness Award from DHS CBP.

Bibliography

BAE Systems. "Link 16 Products." https://www.baesystems.com/en/product/link-16-terminals, accessed August 2023.

Cast Navigation. "Dynamic GNSAS/INS Simulation Systems." https://castnav.com/, accessed August 2023.

Cast Navigation. "GNSS Modeling and Simulation." https://castnav.com/gnss-capabilities/, accessed August 2023.

L3Harris Technologies, Inc. "Link 16 Tactical Data Links," L3Harris: Fast. Forward., https://www.l3harris.com/all-capabilities/link-16-tactical-data-links, accessed August 2023.

NovAtel, Inc. "Anti-Jam Antenna Systems (GAJT)." HEXAGON/Novatel, https://novatel.com/products/anti-jam-antenna-systems-gajt, accessed August 2023.

RACELOGIC Ltd. "LabSat: Compact Yet Powerful GNSS Testing Solutions." LabSat, https://www.labsat.co.uk/index.php/en/, accessed August 2023.

Safran Electronics and Defense. "Skydel GNSS Simulation Software." Safran, https://safran-navigation-timing.com/product/skydel-simulation-engine/?model_interest__c=Skydel&product_interest___single_select=GNSS+Simulation, accessed August 2023.

Safran Electronics and Defense. "Skydel Anechoic: Anechoic Chamber Simulator System." https://safran-navigation-timing.com/product/skydel-anechoic/?model_interest__c=Skydel&product_interest___single_select=GNSS+Simulation, accessed August 2023.

Spirent Communications. "Position, Navigation, and Timing." Spirent, https://www.spirent.com/products/positioning-navigation-timing-testing, accessed August 2023.

Viasat, Inc. "Link 16 Equipment and Accessories." Viasat, https://viasatprod-63.adobecqms.net/products/software-and-services/link-16-accessories/, accessed August 2023.