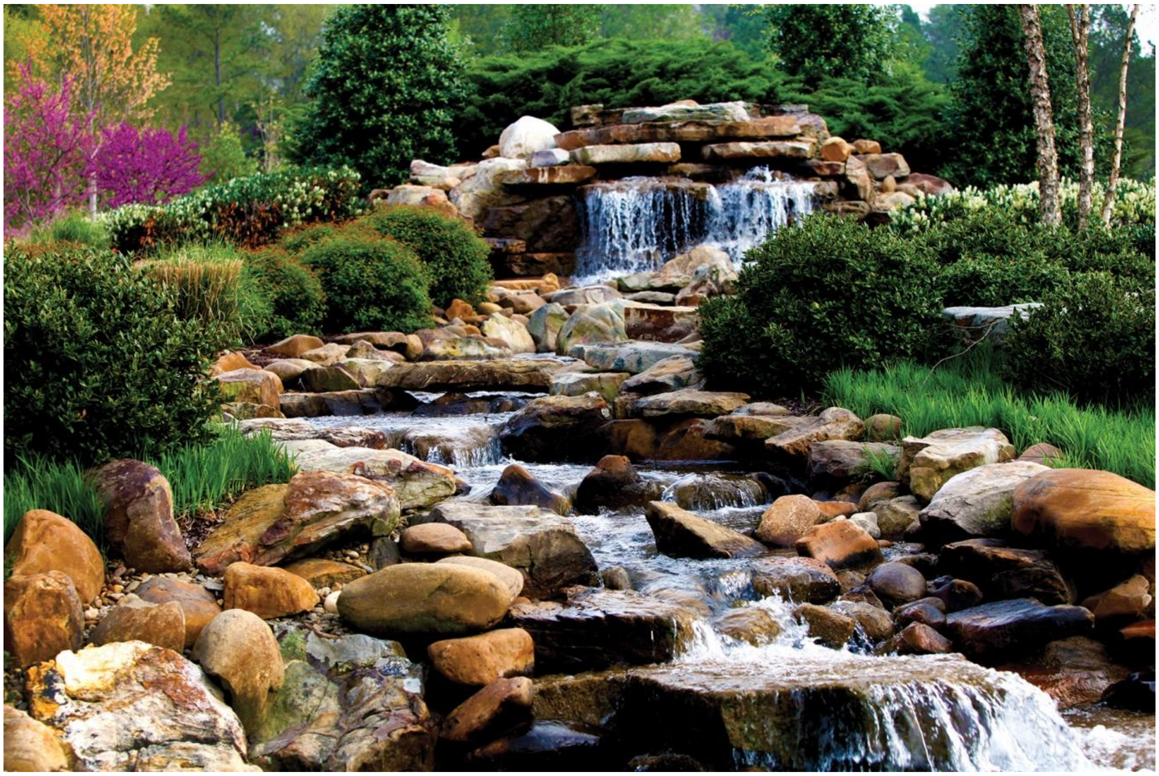
ORNL/SPR-253010

GPS Signal Monitoring Report



Amir Osman
Chris Cooper
Austin Albright

August 2026

ORNL/SPR- 253010

The Center for Alternative Synchronization and Timing (CAST)

GPS SIGNAL MONITORING REPORT

Amir Osman
Chris Cooper
Austin Albright

August 2026

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831
managed by
UT-BATTELLE LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

C/A	coarse acquisition
CAST	Center for Alternative Synchronization and Timing
DHS	US Department of Homeland Security
DOW	US Department of War
GET-CI	GPS Equipment Testing for Critical Infrastructure
GLONASS	Russia's Global Navigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
LNAV	Lateral Navigation
ORNL	Oak Ridge National Laboratory
PNT	position, navigation, and timing
PRN	Pseudorandom Noise
RF	radio frequency
S&T	Science and Technology Directorate

ABSTRACT

This report documents GPS/GNSS signal interference monitoring and resilience testing performed by the Center for Alternative Synchronization and Timing (CAST) participating at the U.S. Department of Homeland Security (DHS) Science and Technology Directorate's GPS Equipment Testing for Critical Infrastructure (GET-CI) event. Using a controlled, laboratory-based GNSS simulation approach (including live-sky signal distribution with injected threat waveforms and no over-the-air transmission), CAST evaluated how commercial timing/clock equipment behaves under representative jamming and spoofing conditions, including position jumps, position walks, time jumps, time ramps/accelerations, time walks, and navigation message (LNAV/ICD) manipulations. Results show that the embedded GNSS receivers in the tested clocks demonstrated limited capability to reliably detect interference, with jamming detected in only a minority of runs and spoofing detected rarely. The findings reinforce that spoofing presents a particularly high operational risk because it can quietly corrupt position and time without obvious loss of service; even microsecond-level timing deception can translate into hundreds of meters of position error. Based on these observations, the report recommends a multilayered resilience strategy combining improved receiver/firmware detection algorithms, redundant and cross-validated GNSS architectures, operational monitoring and incident playbooks, and the adoption of alternative timing sources. CAST's terrestrial timing and synchronization approach is presented as a complementary, GNSS-independent option to improve continuity of timing for critical infrastructure during GNSS disruptions.

1. INTRODUCTION

The **Global Positioning System (GPS)** is one of the most relied-upon yet least noticed technologies of our time, quietly powering the systems that keep society running. It guides airplanes safely across continents, steers cargo ships through crowded ports, enables ride-sharing apps, coordinates delivery fleets, synchronizes global financial transactions, and even supports autonomous vehicles. But this silent reliability comes with a hidden risk. Our dependence on GPS means that any disruption, whether caused by natural factors, technical failures, or deliberate interference, can have cascading effects across industries and communities. In recent years, deliberate interference in the form of **GPS jamming**, an intentional radio frequency interference with GPS signals, and **spoofing**, a fake GPS signal that falsely updates the receiver's location, time, or both, has increased, posing a threat to civilian and military navigation systems. These tactics can block or manipulate GPS signals, creating anything from minor navigation errors to serious safety hazards. Understanding the nuances of jamming and spoofing is crucial for any organization relying on precision GNSS technology. Safeguarding positioning and timing accuracy demands a clear grasp of these threats to develop a preemptive strategy.

This report explains that, although GNSS (e.g., GPS, Galileo) provides essential timing for functions like phasor measurement and grid synchronization, jamming can deny these signals, and spoofing—being more dangerous—can deceive systems without triggering alarms. This bulletin underscores the vulnerability of relying solely on GNSS and the need for alternative time sources to ensure grid resilience

2. BACKGROUND

The U.S. Department of Homeland Security (DHS)'s Science and Technology Directorate (S&T) prioritizes accurate position, navigation, and timing (PNT) information for critical infrastructure. S&T runs a multiyear program addressing GPS vulnerabilities by conducting assessments, developing mitigations, exploring alternative technologies, and engaging with industry.

As part of outreach efforts, DHS S&T hosts evaluation opportunities for stakeholders to test equipment in controlled signal environments authorized by the U.S. government. The most recent of these events, the 2025 GPS Equipment Testing for Critical Infrastructure (GET-CI), allowed participants to test PNT equipment against jamming and spoofing in a unique environment that combined simulated signals to be combined with the live GNSS transmissions to create the closest possible signal environment to an over-the-air test. Due to the difficulty in conducting over-the-air GNSS jamming and spoofing, GET-CI provides a much-needed independent testing environment, which is as close as legally achievable to an actual over-the-air test event.

3. PURPOSE

The DHS event allowed manufacturers of commercial GPS receivers and critical infrastructure operators to evaluate their equipment under controlled adverse conditions. These tests provide a much-needed assessment of the resilience of PNT equipment in the market with a specific focus on equipment used within critical infrastructure. Participants are able to assess the behavior and performance of their equipment, identify vulnerabilities, raise awareness, and implement or validate mitigations. The event also supports testing of experimental and prototype equipment, new product lines with built-in resilience features, and new mitigation technologies.

4. GPS OR GNSS JAMMING AND SPOOFING

Jamming and spoofing are forms of **radio frequency (RF) interference** that involve the disruption of satellite communication signals, rendering devices compromised or completely incapable of effectively receiving information. The implications can be severe, especially for systems relying on accurate position data from GNSS/GPS. **Jamming** is all about disruption. Its goal is to overwhelm receivers with noise or warped data, interfering with signal transmission and degrading or disabling reception. **Spoofing** involves deceit. It introduces false signals that mimic legitimate ones, tricking receivers into using the illicit signals instead of accurate data. This can lead to incorrect position readings, misguided actions, or even system failures.

Essentially, jamming causes GNSS receivers to fail through interference, while spoofing leads them astray by feeding them incorrect information. Both present significant challenges, but their differing methodologies mean they require distinct approaches for detection and mitigation.

An analogy to compare jamming and spoofing is a robber cutting the security camera feed, so the guard sees gray static on the monitor screen (jamming), versus the robber replacing the feed with video that shows the same view from another time, making the security guard think all is well (spoofing). From a GNSS user perspective, spoofing is of greater concern because, unlike jamming, spoofing may not be detected.

4.1 GPS JAMMING

GPS jamming, a type of GNSS interference, involves transmitting high-powered radio signals on the same frequencies used by satellites, thereby overpowering legitimate signals and rendering GPS receivers unable to calculate accurate locations or times.

Jamming is done by overwhelming the GNSS receiver with higher power RF signals. Although illegal in most jurisdictions, low-power jammers known as “personal privacy devices” can be purchased and used for this purpose. Even a simple, low-power jammer can overpower GNSS signals within a large area, denying PNT.

The effectiveness of jammers primarily depends on their output power and range (distance to the target receiver). A low-power jammer close by could have the same effect as a high-power jammer transmitting from farther away. Other characteristics of a jammer is the form of the transmission it emits. Whether it is a target narrow continuous wave (CW) tone or a tone swept across a wideband (a chirp) or a pulsed on-off repeating cycle of the CW tone or chirp.

- **Intentional vs. unintentional:** Although satellite signals can be jammed unintentionally, and many cases are deliberate, often to prevent a device, vehicle, ship, or aircraft from being tracked. There are natural causes of interference such as space weather, e.g., solar flares, and unintended electromagnetic interference (EMI) from every day electrical equipment, such as a poorly installed household device or an aging piece of industrial equipment.

- **Vulnerability:** GNSS devices rely on weak RF signals from space, making them highly susceptible to disruption. Even modest interference can degrade the signals being used to calculate PNT data undermining the accuracy.

- **Risks:** Jamming can cause significant harm or economic loss across critical infrastructure sectors (e.g., finance, energy, communication), study estimate that the loss of GPS service would have a $1 billion per-day impact [8].

- **Targets:** Jamming targets aircraft, drones, ships, precision agriculture, financial networks, and time-stamping systems in digital infrastructure.

- **Ease of execution:** Only a weak interfering signal is needed to disable a GPS receiver and jamming devices can been found for sale on mainstream marketplaces.

Figure 1 shows examples of different types of GNSS jammers.

Figure 1. Various jamming systems. (left) A personal protection device, (middle) a car GPS jammer, (right) a military jamming system [7].

4.2 GPS SPOOFING

In GNSS systems, such as GPS, spoofing is an attack in which a receiver is deceived by fake signals that mimic legitimate transmissions, or by genuine signals that have been recorded elsewhere or at a different time and then rebroadcast.

Spoofing is often a two-step process that requires using a jammer to first disrupt the receiver from tracking authentic GNSS signals and then using a radio transmitter to send false GNSS signals to the target receiver. The false signals can either be created by a signal generator or a rebroadcast of recorded GNSS signals, called meaconing.

A simple example of spoofing is using a software-defined radio (SDR) to drive your smartphone's location calculation and cheat at Pokémon GO from the comfort of your recline. Conceptually, more serious spoofing attacks using sophisticated GNSS signal simulators are the same, but the consequences can be dire—like a plane landing where it should not or a ship sailing into unfriendly waters.

The following diagram in Figure 2 illustrates why jamming and spoofing protection has become a critical necessity of GNSS equipment.

- **Why spoofing works:** Satellite signals are already weak at the Earth's surface, making them easy to overpower with manipulated signals.

- **Consequences:** Spoofing can cause navigation accidents, environmental damage, loss of life, and substantial financial costs.

- **Detection difficulty:** Spoofed signals perfectly mimic authentic ones, and most receivers lack built-in defenses.

Figure 2 illustrates how a spoofed trajectory can deviate from the true trajectory.

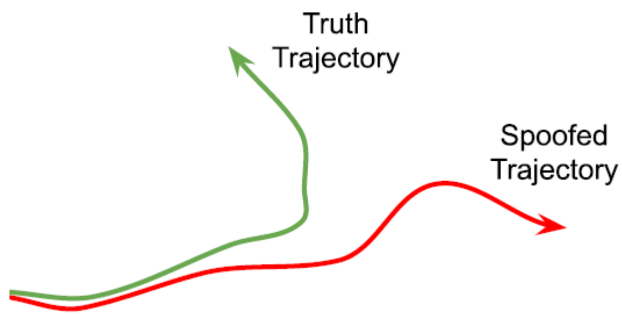


Figure 2. Spoofed trajectory vs. truth trajectory.

Figure 3 displays a map from the GPSJAM website showing GPS interference levels across the United States. Green indicates low interference, yellow shows medium, and red represents high interference that affects PNT and regional safety.

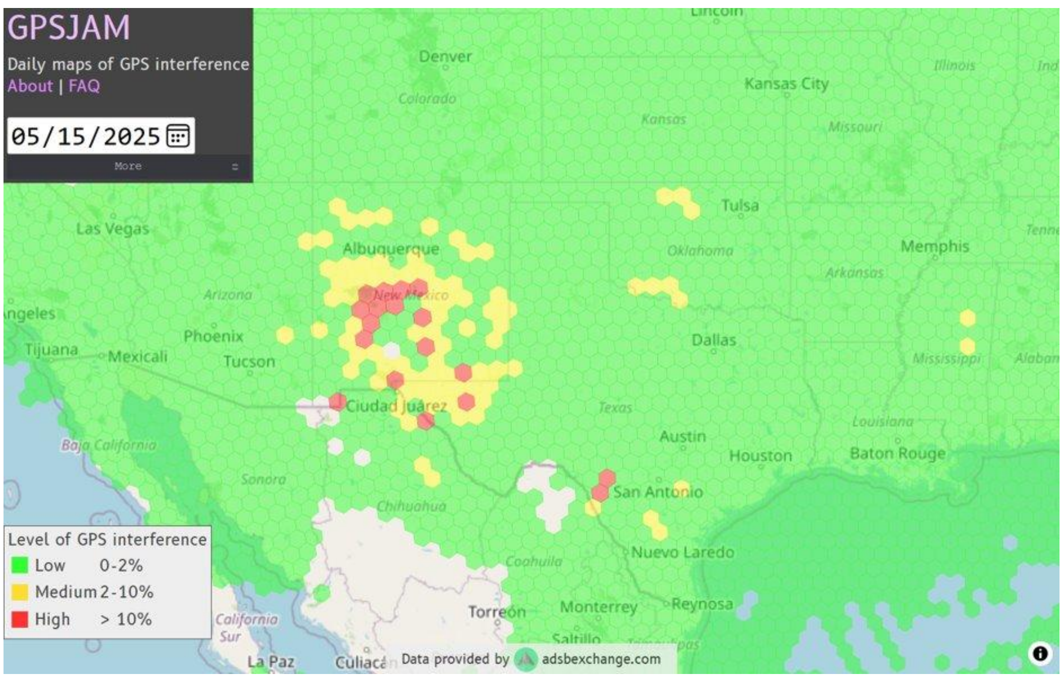


Figure 3. Levels of GPS interference in the American Southwest as determined from aircraft's GNSS signal quality reports [Image courtesy gpsjam.org].

5. JAMMING AND SPOOFING TEST

As previously discussed in Section 2, intentional GNSS interference transmissions are strictly regulated. Only the Department of War is authorized to conduct over-the-air jamming and spoofing within the United States. The only other method to test equipment for jamming and spoofing is using a GNSS simulation (e.g., Orolia GSG-8 Simulator or Spirent PNT-X Simulator) cabled directly to the antenna input ports of equipment under test. All the tests described in Section 6 involved using a GNSS simulator in combination with a live signal feed from a roof-top antenna and in some scenarios specially configured SDR hardware. The combination of these signals with the live antenna feed create the closest possible RF environment to an actual over-the-air test.

An example of what a commercial GNSS simulator looks like can be seen in Figure 4 which shows the Center for Alternative Synchronization and Timing (CAST) lab's Orolia (now Safran) GSG-8. Figure 5 illustrates the equipment setup for the jamming and spoofing tests at the GET-CI event.

Figure 4. The CAST Orolia GSG-8 simulator [7].

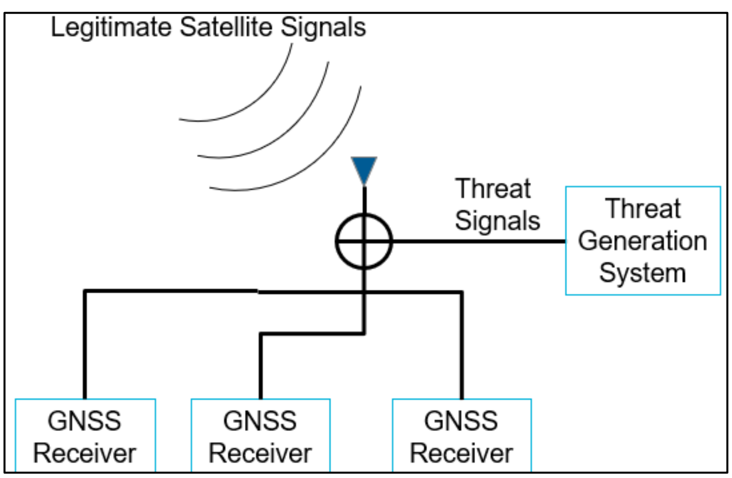


Figure 5. Simulator setup for the jamming and spoofing tests.

- A single antenna receives live-sky signals and distributes the signal to all participants.
- Threat signals are combined with the live-sky signals using cables and an RF signal combiner.

– Nothing is broadcast over the air
– 15 feeds available for participants
– Bring Your Own (BYO) (C)able

– Live-sky feed from L1/L2/L5 GNSS Signals antenna, 3 dB passband 1,503–1,623 MHz, 1,152–1,312 MHz

During the event, CAST tested various clocks to evaluate their resilience against jamming and spoofing attacks. The tests included a broad variety of scenarios such as position jumps, time jumps, and time ramps, with varying results in detecting these threats. Figure 6 shows a diagram of the CAST setup at the event, and Figure 7 shows a detailed view of the jamming and spoofing simulator setup.

.

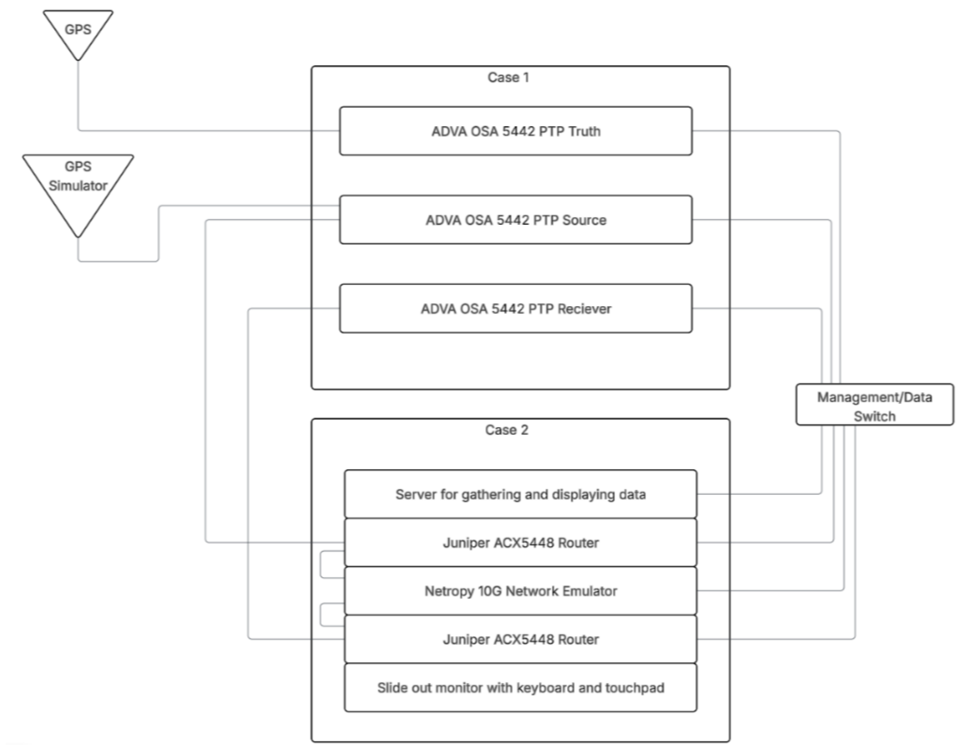


Figure 6. CAST clock-testing setup at the GET-CI event.

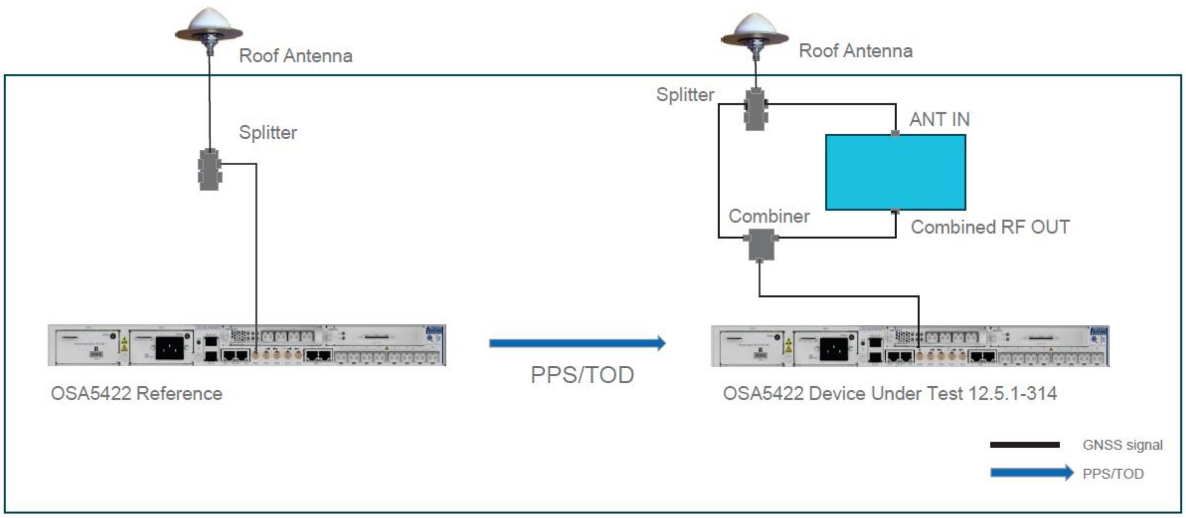


Figure 7. Detail view of the jamming and spoofing simulator setup.

6. JAMMING AND SPOOFING TEST SCENARIOS

Table 1 lists the test scenarios and the key parameters of each test, which are the specific GNSS constellations being spoofed, the type of spoofing, the rate change or in the case of fixed offsets the size of the offset, and whether the spoofing was preceded by knock-off jamming. Knock-off jamming transmitted at a high power to guarantee that an unprotected receiver will lose its lock on any GNSS signals in use prior to the knock-off jamming be activated. Note that for GET-CI, GLO is the abbreviation used for the Russian GLONASS GNSS constellation and GAL is the abbreviation used for the European Union's Galileo GNSS constellation.

Table 1. Test scenarios run by DHS.

Test ID	Description	Knock-off jammer	Rate/size	Spoofed Constellations	Spoofing Power Advantage
PJ1	Position jump	Yes	3 km	GPS+GLO+GAL	+6 dB
PJ2	Position jump	Yes	1 km	GPS+GLO+GAL	+6 dB
ES1	Position + time jump	Yes	100 km	GPS+GLO+GAL	Variable, peak +16 dB
PW1	Position walk	No	10 m/s	GPS+GLO+GAL	+6 dB
PW2	Position walk	No	10 m/s	GPS+GLO+GAL	+10 dB
PW3	Position walk	No	10 m/s	GPS	+3 dB
PA1	Position walk	No	1 m/s^2	GPS+GLO+GAL	+6 dB
TJ1	Time jump	Yes	10 µs	GPS+GLO+GAL	+6 dB
TJ2	Time jump	Yes	1 µs	GPS+GLO+GAL	+6 dB
TJ3	Time jump	No	1 ms	GPS+GLO+GAL	+6 dB
TA1	Time ramp	No	3.3 ns^2	GPS+GLO+GAL	+3 dB
TA2	Time ramp	No	3.3 ns^2	GPS+GLO+GAL	+6 dB
TA3	Time ramp	No	10 2 ns/s	GPS+GLO+GAL	+6 dB
TR1	Time ramp	No	10 ns/s	GPS+GLO+GAL	+6 dB
TR2	Time ramp	No	10 ns/s	GPS+GLO+GAL	+10 dB
TW1	Time walk	No	10 ns/s	GPS+GLO+GAL	+6 dB

TW1a	Time walk	No	10 ns/s	GPS+GLO+GAL	+6 dB
TW2	Time walk	No	−25 ns/s	GPS+GLO+GAL	+6 dB
TRN1	Time ramp	No	10 ns/s	GPS+GAL+GLO	+6 dB
DM1	Interface control document (ICD)	Yes	n/a	GPS	+6 dB
DM2	ICD	Yes	n/a	GPS	+6 dB
DM3	ICD	Yes	n/a	GPS	+6 dB
VSCW	Various Swept CW Jamming	Yes	n/a	GPS+GAL+GLO	

The following subsections provide detailed information about the scenarios used to test jamming and spoofing. The scenarios are listed in the order they were executed during GET-CI.

6.1 SCENARIO PW1

- **Position walk (PW)** is a term used to describe the gradual and subtle changes in the reported position of a GPS receiver due to spoofing. Unlike a position jump, where the location suddenly shifts, position walk involves a slow drift, making it harder to detect.

  - **Scenario details:**
- Type: Position walk
- Rate: 10 m/s
- Signals: GPS+GAL+GLO
- Power advantage: 6 dB
- Notes: Moves due north

6.2 SCENARIO TR1

- **Time ramp (TR)** refers to a gradual and continuous shift in the time data received by a GPS device due to spoofing. Unlike a sudden time jump, a time ramp involves a slow and steady change in the perceived time, making it more challenging to detect.

  - **Scenario details:**
- Type: Linear time ramp
- Rate: 10 ns/s
- Signals: GPS + GAL + GLO
- Power advantage: 6 Db

6.3 SCENARIO TA1

Time Acceleration (TA) refers to constant time acceleration

  - **Scenario details:**
- Type: Constant time acceleration
- Rate: 3.3 ns/s^2
- Signals: GPS + GAL + GLO
- Power Advantage: 3 dB

6.4 SCENARIO TJ3

- **Time jump (TJ)** refers to abrupt changes in the time data received by a GPS device due to jamming or spoofing.

  - **Scenario details:**
- Type: Position walk
- Rate: 10 m/s
- Signals: GPS + GAL + GLO
- Power advantage: 10 dB
- Notes: Moves due north

6.5 SCENARIO PW2

  - **Scenario details:**
- Type: Position walk
- Rate: 10 m/s
- Signals: GPS + GAL + GLO
- Power advantage: 10 dB
- Notes: Moves due north

6.6 SCENARIO TJ1

- **Scenario details:**
  - Type: Time jump
  - Size: 8 μS
  - Signals: GPS + GAL + GLO
  - Power advantage: 6 dB

6.7 SCENARIO TW1

- **Time walk (TW)** is a specific type of spoofing evaluation designed to determine if a receiver can be subtly "led away" from the correct time, once the receiver "locks" onto the spoofer's signal, the attacker gradually shifts the time (the "walk") in small increments—often sub-microsecond steps.

  - **Scenario details:**
- Type: Time linear ramp + Gaussian walk
- Rate: 10 ns/s mean + 10 ns σ steps
- Signals: GPS + GAL + GLO
- Power advantage: 6 dB

6.8 SCENARIO PA1

  - **Scenario details:**
- Type: Constant position acceleration
- Rate: 1 m/s^2
- Signals: GPS + GAL + GLO
- Power Advantage: 6 dB
- Notes: Moving due east

6.9 SCENARIO DM1

The **interface control document (ICD)** for GPS or GNSS systems typically outlines the technical specifications and protocols for communication between different components of the system. When it comes to **jamming** and **spoofing**, the ICD may include details on the following:

- **Signal structure**: Information on how the signals are transmitted and received; this is crucial for understanding how jamming and spoofing can interfere with these signals.

- **Detection and mitigation**: Guidelines and techniques for detecting and mitigating the effects of jamming and spoofing.

- **Security measures**: Protocols and encryption methods to protect against unauthorized access and manipulation of the signals.

These documents are essential for developers and engineers working on GPS/GNSS systems to ensure they can build robust systems that can withstand such threats.

- **Scenario details:**
  - Type: Modified Lateral Navigation (LNAV) data, LNAV is aviation, navigation method providing horizontal, or "left-right," guidance along a defined flight path without vertical guidance
  - Rate: n/a
  - Signals: GPS coarse acquisition (C/A) only
  - Power advantage: 6 dB

6.10 SCENARIO ES1

- **Scenario details:**
  - Type: “Errant simulator”
  - Rate: 100 km position offset and 100 km equivalent signal delay
  - Signals: GPS + GAL + GLO
  - Power advantage: Variable, peak 18 dB (see figure below)

Figure 8 shows a plot of power advantage vs. elapsed time for a position + time jump.

The "power advantage" starts slightly negative, quickly peaks at +18 dB around 280–300 s, then drops, returning to 0 dB near 420–450 s, and slowly declines to about −7 to −8 dB by 1200 s. This pattern involves an initial high-power burst to overwhelm a receiver's Automatic Gain Control (AGC) or to initiate a takeover, followed by reduced power operation to maintain the deception while avoiding immediate detection.

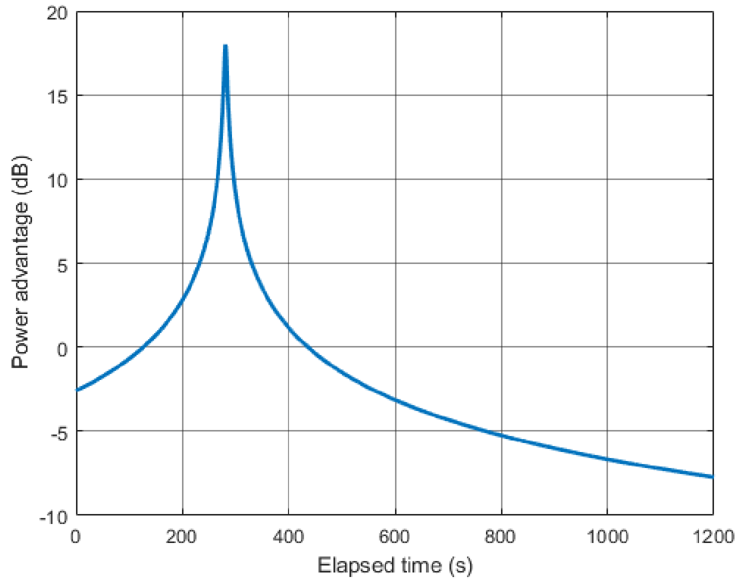


Figure 8. shows a plot of power advantage vs. elapsed time for a position + time jump.

6.11 SCENARIO TJ2

- **Scenario details:**
  - Type: Time jump
  - Size: 1 μs
  - Signals: GPS + GAL + GLO
  - Power advantage: 6 dB

6.12 SCENARIO TW2

- **Scenario details:**
  - Type: Linear time ramp plus Gaussian walk
  - Rate: −25 ns/s mean + 10 ns Standard deviation(σ) steps
  - Signals: GPS + GAL + GLO
  - Power advantage: 6 dB

6.13 SCENARIO TA2

- **Scenario details:**
  - Type: Constant time acceleration
  - Rate: 3.3 ns/s^2
  - Signals: GPS + GAL + GLO
  - Power Advantage: 6 dB
  - Notes: Stops accelerating once ~160 ns/s rate reached

6.14 SCENARIO PJ1

- **Scenario details:**
  - Type: Position jump
  - Size: 3 km offset
  - Signals: GPS + GAL + GLO
  - Power advantage: 6 dB

6.15 SCENARIO PW3

- **Scenario details:**
  - Type: Position walk
  - Rate: 10 m/s
  - Signals: GPS C/A only
  - Power advantage: 3 dB
  - Note: Moves due north

6.16 SCENARIO PJ2

- **Scenario details:**
  - Type: Position jump
  - Size: 4.3 km offset
  - Signals: GPS + GAL + GLO
  - Power advantage: 6 dB

6.17 SCENARIO TR2

- **Scenario details:**
  - Type: Time ramp
  - Rate: 10 ns/s
  - Signals: GPS + GAL + GLO
  - Power advantage: 10 dB

6.18 SCENARIO TR1N

- **Scenario details:**
  - Type: Linear time ramp
  - Rate: 10 ns/s
  - Signals: GPS + GAL + GLO
  - Power advantage: 6 dB
  - Note: No added noise

6.19 SCENARIO TW1A

- **Scenario details:**
  - Type: Time linear ramp + Gaussian walk
  - Rate: 10 ns/s mean + 10 ns Standard deviation (σ) steps
  - Signals: GPS + GAL + GLO
  - Power advantage: 6 dB

6.20 SCENARIO DM2

- **Scenario details:**
  - Type: Modified LNAV data
  - Rate: n/a
  - Signals: GPS C/A only
  - Power advantage: 6 dB
  - Notes: Broadcast UTC A0 parameter is 1 s

6.21 SCENARIO TA3

- **Scenario details:**
  - Type: Constant time acceleration
  - Rate: 2 ns/s^2
  - Signals: GPS + GAL + GLO
  - Power advantage: 6 dB
  - Stops at ~100 µs offset

6.22 SCENARIO DM3

- **Scenario details:**
  - Type: GPS LNAV data modification
  - Rate: N/A
  - Signals: N/A
  - Power advantage: 6 dB
  - Notes: Pseudorandom Noise (PRN) 5 claims all other signals are unhealthy via almanac data

6.23 VARIOUS SWEPT CONTINUOUS WAVEFORM JAMMING

- **Two swept continuous waveform jamming:**
  - J1: 36 MHz bandwidth at 1,594 MHz, 1 ms chirp period
  - J10: 36 MHz bandwidth at 1,594 MHz, 10 ms chirp period

- **Two jammer power profiles (S30, S100)**

- **Test will be**
  - J1 × S30 (4 min on, 2 min off), repeated 3 times
  - J1 × S100 (4 min on, 2 min off), repeated 2 times
  - J10 × S30 (4 min on, 2 min off), repeated 3 times
  - J10 × S100 (4 min on, 2 min off), repeated 2 times

- **Total of ~60 min**

7. JAMMING AND SPOOFING TEST RESULTS

Table 2 summarizes the GET-C1 test results for the CAST clocks.

Table 2. CAST clock test results.

Description	ID	Constellation	Jamming Detected	Spoofing Detected
Position jump	PJ1	GPS+GLO+GAL	NO	NO
Position jump	PJ2	GPS+GLO+GAL	NO	NO
Position + time jump	ES1	GPS+GLO+GAL	NO	NO
Position walk	PW1	GPS+GLO+GAL	YES	NO
Position walk	PW2	GPS	YES	NO
Position walk	PW3	GPS+GLO+GAL	NO	NO
Position walk	PA1	GPS+GLO+GAL	YES	NO
Time jump	TJ1	GPS+GLO+GAL	NO	NO

Time jump	TJ2	GPS+GLO+GAL	NO	YES
Time jump	TJ3	GPS+GLO+GAL	NO	NO
Time ramp	TR1N	GPS+GLO+GAL	NO	NO
Time ramp	TR2	GPS+GLO+GAL	NO	NO
Time ramp	TA1	GPS+GLO+GAL	YES	NO
Time ramp	TA2	GPS+GLO+GAL	YES	NO
Time walk	TW1	GPS+GLO+GAL	NO	NO
Time walk	TW1a	GPS+GLO+GAL	NO	NO
Time walk	TW2	GPS	YES	NO
Time ramp	TA3	GPS+GLO+GAL	NO	NO
ICD	DM1	GPS	NO	NO
ICD	DM2	Yes	NO	NO
ICD	DM3	GPS	NO	NO
Time walk	TW1a	GPS+GLO+GAL	NO	NO
Various Swept CW Jamming/	VSCWJ	GPS+GLO+GAL	NO	NO

8. RESULTS ANALYSIS

The GNSS receivers inside the clocks show a very low percentage of detecting jamming and spoofing and require major software updates to increase confidence that they will be able to detect such events which is the first step to being able to withstand the events.

Figure 9 displays the test results for jamming and spoofing detection. The chart shows that jamming was not detected in 17 tests and was detected only 6 times. Spoofing, which is challenging to detect, was detected only once out of 23 tests.

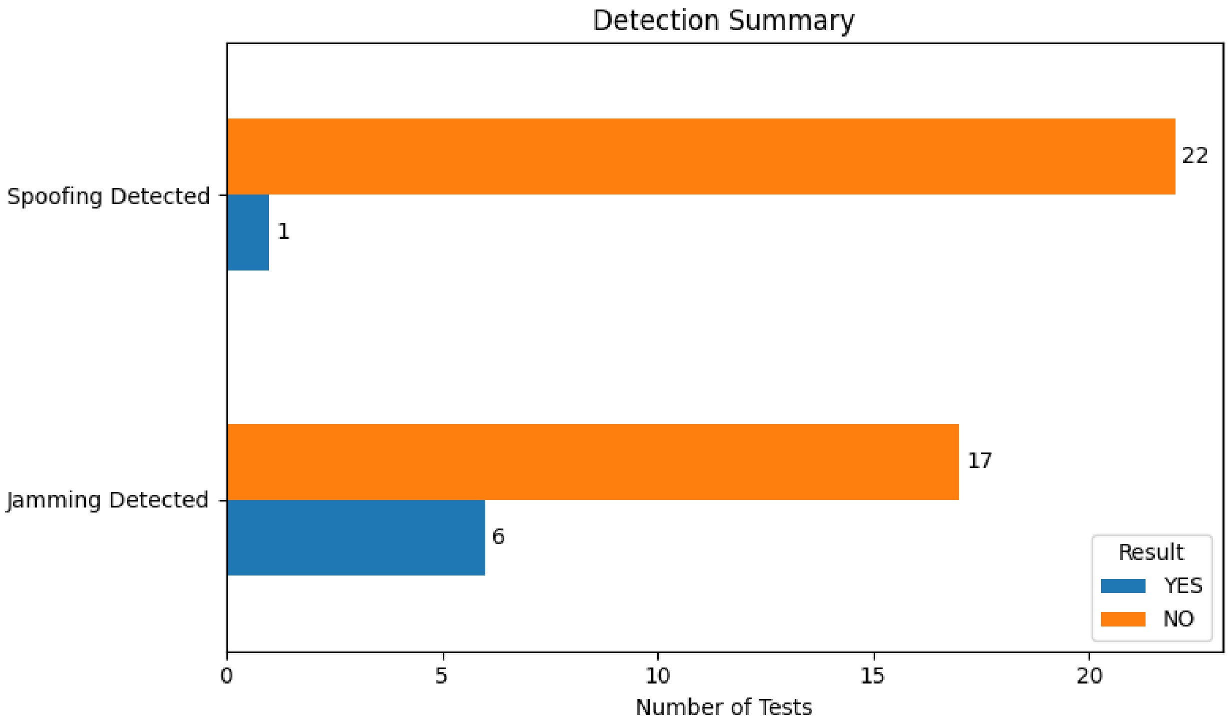


Figure 9. Jamming and spoofing detection for the GET-C1 tests.

9. LESSONS LEARNED AND FUTURE DIRECTIONS

The report emphasizes the need for improved resilience against jamming and spoofing, suggesting the use of dual GNSS receivers and the importance of analyzing collected data for feedback to manufacturers.

After the jamming and spoofing tests, CAST shared the results with the clock manufacturers, and they are working to improve their software, and we at CAST are working with clocks manufactures to implement the following improvements:

- Galileo Open Service Navigation Message Authentication Software version 13.1.1 this will ensure you are receiving the GNSS signal from Galileo satellites to mitigate the spoofing
- For ADVA OSA54x2 clocks equipped with the multiband (MB) GNSS receiver option, new receiver firmware with much better spoofing detection is being tested
- Enhanced Machine Learning (M)L algorithms for Mosaic Network Controller (MNC)
- PTN Layer 3 SyncJack protection for Jamming and Spoofing
- Adopt DHS/DOD PNT resilience standards
- Share test data with manufacturers for algorithm improvements
- Invest in detection technologies and alternative timing sources
- Develop playbooks for GNSS disruption events
- Train operators on GNSS anomaly recognition

CAST recommends the following to improve GNNS resilience against jamming and spoofing:

- Multilayer detection: Signal authentication, angle-of-arrival checks
- Alternative PNT: eLoran, fiber timing, inertial navigation
- Redundancy: Mult-constellation, multi-frequency GNSS receivers with cross-validation
- Hardening: Firmware updates, receiver autonomous integrity monitoring, configurable alerts
- The best operational practices: Monitoring, incident response, training
- Policy engagement: Standards adoption, data sharing, regulation
- Future directions: AI-based anomaly detection, crowdsourced monitoring

10. CAST NETWORK AS AN ATERNATIVE SOLUTION

This report highlights the imminent threat of jamming and spoofing to GNSS. Most GNSS receivers and clocks lack complete protection against these threats, making the source of timing information vulnerable in our infrastructure that cannot afford timing disruptions. We cannot solely rely on GNSS. CAST exists to provide timing and synchronization independent of GNSS, using terrestrial infrastructure through the Precision Time Protocol (PTP).

11. CONCLUSIONS

This report highlights a critical reality: modern infrastructure is deeply dependent on GPS/GNSS for PNT, yet these systems are vulnerable to **jamming** and **spoofing attacks**. Testing under controlled conditions revealed that many devices fail to detect these threats, especially spoofing, which can silently mislead systems without triggering alarms.

To address these risks, organizations must adopt a **multi-layered resilience strategy** that includes the following:

- Advanced detection mechanisms
- Diversified timing sources
- Redundant GNSS solutions
- Hardened firmware and operational best practices
- Industry collaboration and policy alignment

The findings underscore an urgent need for **proactive measures**—not only technological upgrades but also operational readiness and regulatory frameworks—to ensure continuity and safety in critical infrastructure.

12. REFRENCES

1. **Hexagon | NovAtel**. Spoofed or jammed? Understanding GNSS Threats and Mitigation Strategies. Hexagon Positioning Intelligence White Paper.

2. **Arnold, D.** (2020, April 12). GNSS Jamming and How to Mitigate It. Meinberg Time Synchronization Blog. Retrieved from: https://blog.meinbergglobal.com/2020/04/12/gnss-jamming-and-how-to-mitigate-it/

3. **Arnold, D.** (2020, April 14). GNSS Spoofing and How to Mitigate It. Meinberg Time Synchronization Blog. Retrieved from: https://blog.meinbergglobal.com/2020/04/14/gnss-spoofing-and-how-to-mitigate-it/

4. **Department of Homeland Security (DHS)**. (2025). GPS Equipment Testing for Critical Infrastructure (GET-CI) Participant Reference Booklet. August 2025 Edition.

5. **Trimble Positioning Services**. (n.d.). Understanding GPS Jamming Versus GPS Spoofing. https://positioningservices.trimble.com/blog/positioning/en-US/article/understanding-gps-jamming-versus-gps-spoofing.

6. **Oscilloquartz**. (2025). PlugFest DHS 2025: Results and Analysis of GNSS Spoofing and Jamming Tests.

7. **Orolia.** (2024). GNSS simulation training modules: Module 4—Advanced jamming / spoofing.

8. **O'Connor**. (2019). "Economic Benefits of the Global Positioning System (GPS)". RTI Project Number 0215471, June 2019, https://www.rti.org/sites/default/files/gps_finalreport618.pdf.