Protecting Broadcast Infrastructure from GPS Jamming & Spoofing Attacks

Allan Armstrong, Leigh Whitcomb, Douglas Arnold, Geshan Wrosinghert, Matt Silver

Meinberg USA Inc., 111 Santa Rosa Avenue #401, Santa Rosa, CA 95404, USA

Mathias Kleinsorge, Daniel Boldt, Heiko Gerstung

Meinberg Funkuhren GmbH & Co. KG, Lange Wand 9, 31812 Bad Pyrmont, Germany

Abstract. *GPS is ubiquitous in our everyday lives and widely used and trusted for navigation and other services. GPS is also the fundamental source of time for most broadcast production and streaming networks. As such, broadcast networks depend on GPS for reliable operation. GPS is vulnerable to a long list of threats, including jamming & spoofing attacks. Jamming and spoofing is on the rise and a variety of technologies exist to protect broadcast infrastructure.*

The paper will

- *explain how jamming and spoofing attacks are executed,*
- *share surveys of global jamming and spoofing occurrences,*
- *contrast accidental vs. military or state-sponsored attacks,*
- *introduce technologies and tools to mitigate these problems,*
- *discuss effectiveness of mitigation technologies, and*
- *explain testing methods from in-lab testing to live-sky events.*

Tools discussed will include:

- *holdover oscillators,*
- *redundant receivers and remote antennas,*
- *anti-jamming antennas,*
- *terrestrial time transport,*
- *multi-constellation and multi-band receivers,*
- *GNSS consistency checks,*
- *cryptographic authentication, and*
- *alternative PNT sources.*

The paper will close by explaining how testing is done, share experience from lab & field testing, and recommend an approach to protecting infrastructure.

Keywords. GPS, GNSS, Galileo, OSNMA, jamming, spoofing, resilience, ST-2110, holdover oscillator, GET-CI, Jammertest, Live Sky.

The authors are solely responsible for the content of this technical presentation. The technical presentation does not necessarily reflect the official position of the Society of Motion Picture and Television Engineers (SMPTE), and its printing and distribution does not constitute an endorsement of views which may be expressed. This technical presentation is subject to a formal peer-review process by the SMPTE Board of Editors, upon completion of the conference. Citation of this work should state that it is a SMPTE meeting paper. EXAMPLE: Author's Last Name, Initials. Title of Presentation, Meeting name and location.: SMPTE. For information about securing permission to reprint or reproduce a technical presentation, please contact SMPTE at dpurrier@smpte.org or 914-205-2377 (445 Hamilton Ave., Ste. 601 White Plains, NY 10601).

Introduction

Broadcast networks rely on precise time synchronization to ensure lip sync – that audio and video are delivered simultaneously – and ST-2110 is making the problem more critical because audio, video, and ancillary essences are routed separately and must be resynchronized after processing. Most broadcast networks rely on GPS/GNSS as their fundamental source of time, yet GPS/GNSS is threatened by the increasing occurrence of jamming and spoofing, both accidental and intentional.

How Serious is GPS/GNSS Jamming and Spoofing?

Most jamming and spoofing incidents are accidental and/or caused by civilians. They are generally not very serious and good tools exist to cope with them. A small fraction of events is military-related and/or has malicious intent. These are much more serious but fortunately limited to conflict zones so far. The frequency of jamming and spoofing events is increasing, and network operators must prepare for a more challenging future.

In 2016, the European Agency for the Space Program (EUSPA) started a project to assess, characterize, classify, and map jamming & spoofing threats. [1] Called "STRIKE3", this project set up monitoring stations in 23 countries across the globe and tracked over 500,000 interference events over 3 years. The major finding was that the vast majority of events were of short duration. As seen in Table 1 below, only 0.001% of events exceeded one day in duration.

Fraction of Events	Duration
0.015	> 5 minutes
0.0022	> 30 minutes
0.0012	> 60 minutes
0.00001	> 1 day

Table 1. GPS/GNSS Interference Event Durations, source: EUSPA

Many broadcast facilities, particularly those in Los Angeles and New York, are in close proximity to freeways and regularly experience jamming. Major sporting events often experience jamming as well. [2] [3] Some multi-venue events have experienced jamming and have required overnight replacement of vulnerable receivers with resilient receivers.

Civilian Jamming

Most civilian jamming is accidental and caused by jamming devices inserted into the cigarette lighter power jack in commercial vehicles. The driver has no intent to jam critical infrastructure. The driver simply wants to conceal their location. For example, a commercial driver may not want their employer to know their location, or a car thief may not want authorities to track stolen vehicles. Such jamming devices are low-power, typically 10 mW, and have an effective radius of 1 km or less.

As trucks are generally moving, events are short duration, consistent with the STRIKE3 findings. For example, a truck moving at 100 km/h travels 1 km in 36 seconds. Therefore, traffic should only cause short-duration events. A truck parked at a loading dock can cause a problem for a longer time, so operators should be aware of nearby loading docks and consider protecting antennas appropriately.

Technologies to Mitigate Civilian Jamming

Two types of technologies are readily available to provide basic protection against jamming:

1. Anti-jamming filters
2. Holdover oscillators

Anti-Jamming Filters

Filters come in two types and are both available in commercial GPS/GNSS modules.

- Bandpass RF filters, usually implemented with SAW (surface acoustic wave) technology can be placed prior to the mixer in the receiver chip.
- IF notch filters can be implemented via DSP after the ADC and digitally tuned to remove identified interferers.

Figure 1 below is an example of RF and IF filters implemented in commercially available GPS/GNSS modules.

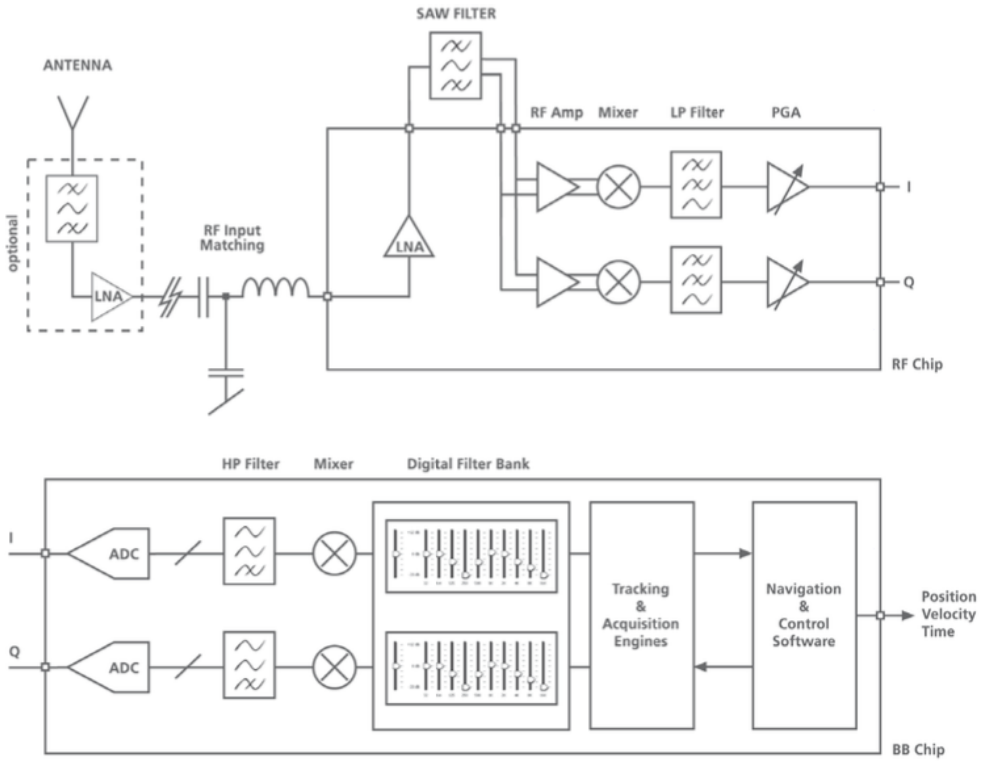


Figure 1. Bandpass RF SAW Filter and Digitally Controlled IF Notch Filters from a commercially available GPS/GNSS receiver module, source: uBlox

Such filters are a useful tool to reduce the number of jamming events but are not a complete solution to the problem. Jamming will still cause intervals where timing information is not received. To ensure uninterrupted operation, a holdover oscillator is necessary.

Holdover Oscillators

Much like the pendulum on a grandfather clock, a holdover oscillator provides stable timing during GPS/GNSS outages. Many technologies exist for holdover oscillators from simple Quartz XOs (crystal oscillators) to TCXOs (temperature-compensated crystal oscillators), OCXOs (oven-controlled crystal oscillators), and even atomic oscillators like Rubidium or Caesium. Higher accuracy generally comes with increased size and cost.

The holdover oscillator can be chosen by considering the required accuracy and the time needed to protect from GPS/GNSS outages and comparing this to holdover oscillator performance. Holdover oscillators do not prevent jamming; they only limits drift to an acceptable amount.

Table 2 below shows holdover oscillator performance of a range of different oscillator technologies. This table shows worst-case performance; some manufacturers specify typical performance. Some manufacturers test each oscillator in production before shipment, but most do not. The JT-NM Reference Architecture [4] specifies synchronization in the range of 1 to 10 µs. Most facilities share a common local clock and therefore the holdover performance of advanced OCXOs, such as the HQ and DHQ shown below, is generally sufficient.

Holdover Accuracy		**OCXO SQ**	**OCXO HQ**	**OCXO DHQ**	**Rubidium**
Frequency	1 day	5e-9	5e-10	1e-10	1e-11
	1 year	2e-7	5e-8	1e-8	5e-10
Time	1 day	±65 µs	±10 µs	±4.5 µs	±0.8 µs
	1 week	±9.2 ms	±1 ms	±204 µs	±34 µs
	1 month	±120 ms	±16 ms	±3.3 ms	±370 µs
	1 year	±4.7s	±788 ms	±158 ms	±8 ms

Table 2. Holdover Oscillator Performance, source: Meinberg

More stable atomic oscillators, such as Cæsium and Hydrogen Masers, are also available, but these are quite expensive, large, and require replacement every 10 years.

The combination of a holdover oscillator with RF & IF filters is generally sufficient in most regions of the world. Some parts of the world, however, are subject to military jamming.

Redundant Receivers & Remote Antennas

Most broadcast infrastructure uses redundant networks, blue and amber/red. Each network should have its own time server, and each time server should have its own antenna. The antennas should be placed as far away from each other as possible, for example on opposite corners of the roof. This gives some protection from near-field interferers.

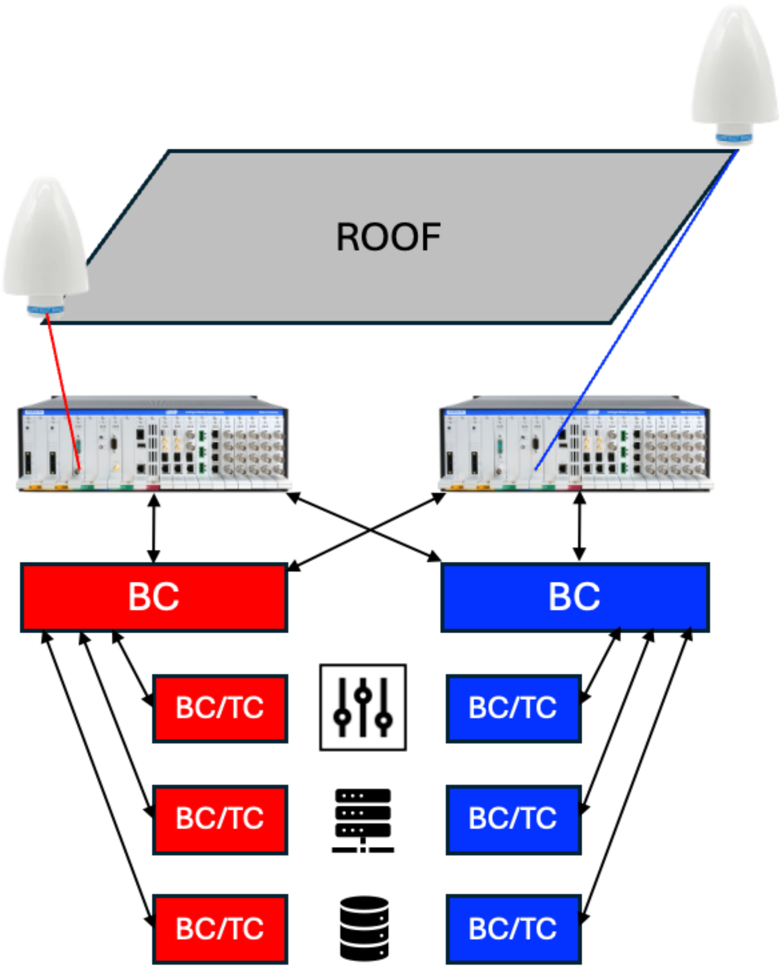


Figure 2. Redundant Receivers & Remote Antennas

Depending on the type of cable used, cables can be as long as 150m. With in-line amplifiers, cables can be extended beyond this limit. Fiber-optic converters can go even further, for example 2 km with MMF and 20 km or longer with SMF.

Reporting About Jamming & Spoofing Events

Victims and instigators of jamming often do not want public knowledge of jamming, so reporting has been limited to incomplete collections of anecdotes. More recently, websites have sprung up that analyze civil aviation date and infer that jamming is likely when ADS-B data disagrees with GPS. Such websites publish maps and record this data so you can go back and see history. One such example is shown below in Figure 3.

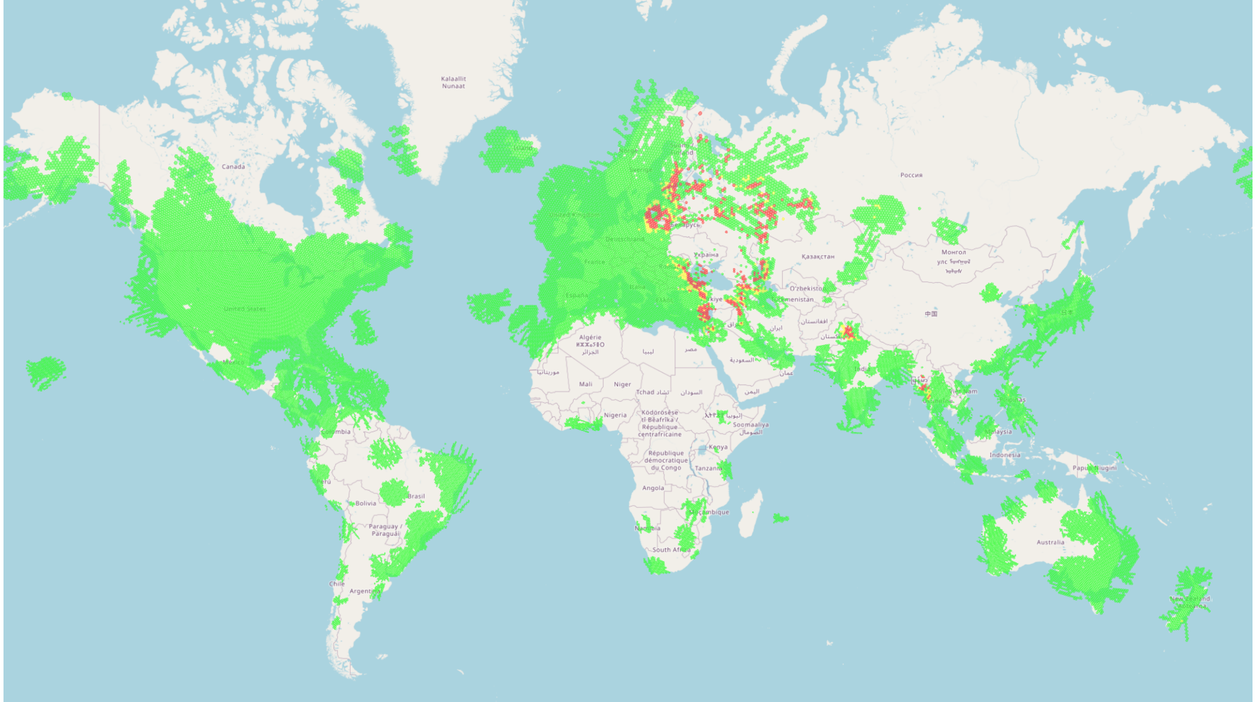


Figure 3. GPS Jamming Map comparing ADS-B to GPS Data
source: gpsjam.org January 20, 2025

From these maps, one can easily conclude that GPS jamming is rife in conflict areas, particularly just west of Russia.

Such maps are quite instructive but only offer a snapshot in time. Maps also exist that combine ADS-B/GPS data with additional information. For example, Figure 4 below aggregates reports over 30 days in 2024. [5] Much of the additional jamming identified is due to military operations.

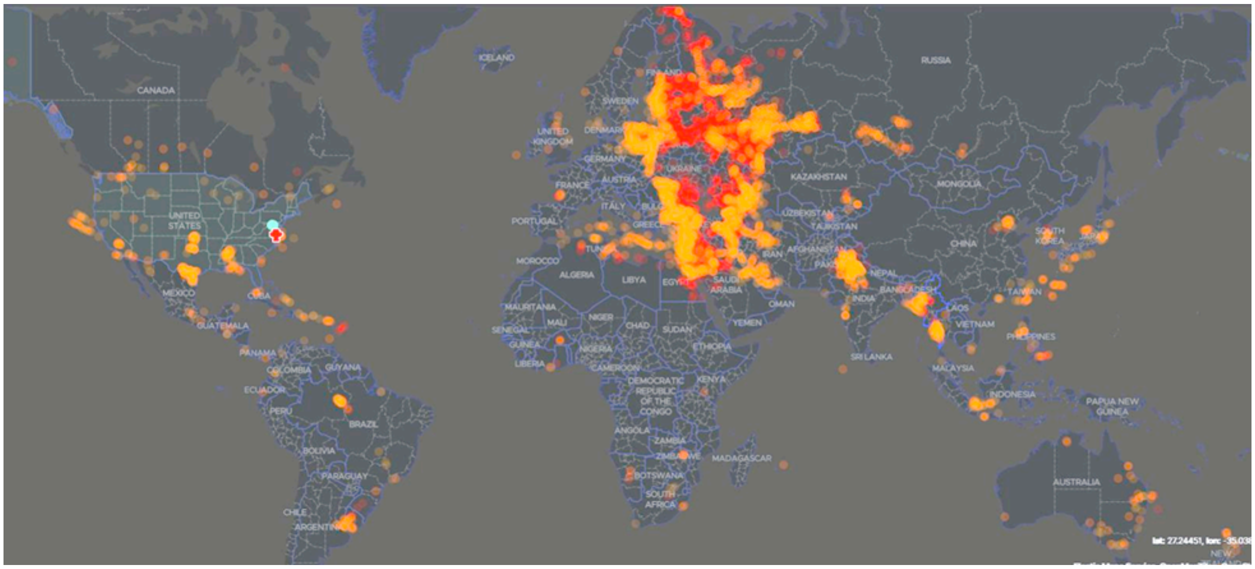


Figure 4. 30 Days of GPS Interference in 2024, source: US DoT & DoD

Military Jamming

Military jamming is far more serious than civilian jamming. While a cigarette lighter jammer may have a power of only 1 mW and a unidirectional antenna, achieving a range of < 1 km, military jamming equipment can be high power with directional antennas and achieve range of up to 100 km or even more. Figure 5 below shows a photograph of a Russian “POLE-21” military jamming system. Unfortunately, the Russian Defense Ministry does not provide a datasheet.

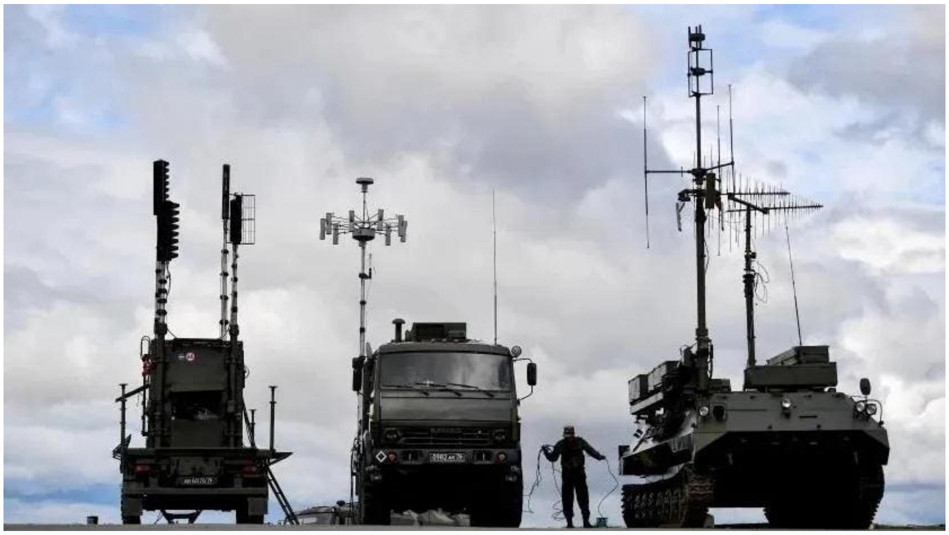


Figure 5. POLE-21 Military Jamming System, source: Russian Defense Ministry

Technologies to Mitigate Military Jamming

Anti-Jamming Antennas

Two types of antennas have been developed to combat jamming:

1. Controlled Radiation Pattern Antennas (CRPAs)
2. Horizon-Nulling Antennas

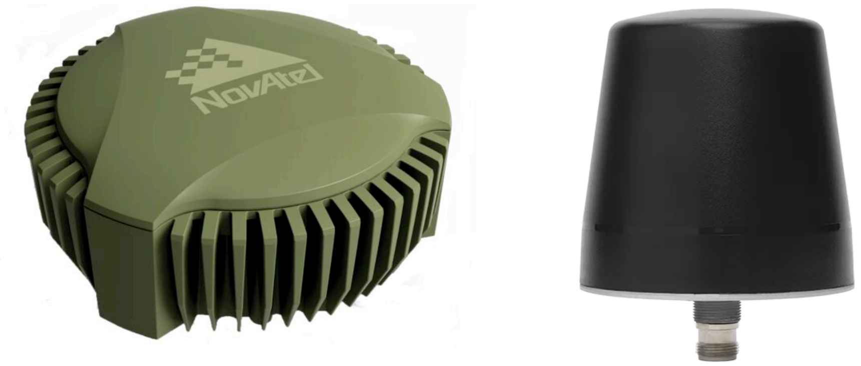


Figure 6. Anti-Jamming Antennas:
(a) Controlled Radiation Pattern Antenna (CRPA), source: Hexagon/NovAtel
(b) Horizon-Nulling Antenna, source: Tallysman/Calian

CRPAs use a phased-array antenna and direction-finding technology to determine the position of interferers and then tune a multi-channel receiver to “throw a null” in the direction of interfering signals. Such antennas are widely used for battlefield navigation applications. They are expensive and until recently have been subject to export restrictions. Battlefield navigation applications do not have the luxury of holdover oscillators or terrestrial time transport, so CRPAs are a useful technology.

Horizon-Nulling Antennas can be used to reduce the incidence of jamming and are a good choice for fixed sites. They operate by reducing their sensitivity to signals at the horizon and increasing their sensitivity to the zenith or sky. As satellites are in the sky and jammers are on the horizon, such antennas can decrease the incidence of jamming. Most jamming sources are weak signals, so reducing horizon sensitivity reduces both the number of jamming events and their power. For moving jammers, like vehicles, reducing power also reduces their duration. [6]

It may also be possible to reduce sensitivity to terrestrial interference by placing antennas behind roof shields.

While horizon-nulling antennas can be helpful, they do not replace normal countermeasures like RF & IF filters, holdover oscillators, and terrestrial time transport.

Terrestrial Time Transport

Because jamming is usually localized, bringing time in from another site is a very effective method to provide resilience. Such a method, called terrestrial time transport requires:

1. A remote source of time, for example a national lab (NIST, USNO, or international labs like NPL in the UK or PTB in Germany), a TaaS (time as a service) provider such as datacenters or stock exchanges (AWS, Equinix, Hoptroff), or another broadcast location,
2. A means of transport, e.g. an internet link, and
3. A time transport technology.

Three terrestrial time transport technologies are in use today:

1. **ITU G.8275.1** [7] can achieve ±1.1 µs accuracy given specified network conditions called “Full Timing Support (FTS)”. Specifically, all switches in the path must be PTP-aware (boundary clock or transparent clock) and the number of hops must be limited. Such network paths are not common in existing networks and upgrading the paths can be expensive.
2. **ITU G.8275.2** [8] can also achieve ±1.1 µs accuracy with so-called “Partial Timing Support (PTS).” Unfortunately, its performance depends on topology and traffic conditions, its asymmetry calibration is frequently not accurate enough, and it depends on local GNSS, so it is not a backup for jamming.
3. **PTN (Precision Time Network)** adds asymmetry calibration and route compensation to G.8275 to improve accuracy and resilience. [9] It is in the early stages of standardization by the ITU as ePTS (enhance Precision Time Support) and has demonstrated excellent results in a trial by NetInsight achieving ≤ ±200 ns among 17 sites in an existing 1500-km MPLS network in Türk Telekom’s network with military jamming and no on-path support. [10]

GPS/GNSS Spoofing

Jamming refers to transmitting a signal at a power high enough to block reception of a signal. Jamming is generally easy to do and common, but it only causes outages which are easily dealt with by using filters and holdover oscillators for most cases and terrestrial time transport for extreme cases.

Spoofing is a more serious, but less frequent problem. Spoofing refers to transmitting a malicious radio signal to trick receivers into doing something dangerous. While there are many reports of spoofing occurring in navigation applications, spoofing has been rare in timing applications. Nonetheless, occurrences of spoofing are increasing and there is much we can do to protect timing infrastructure from spoofing before it becomes a critical problem.

On first inspection spoofing seems to be quite difficult. Satellite signals are complex and spoofing a GNSS receiver would require multiple coordinated RF signals.

Unfortunately, spoofing isn't that hard. Sophisticated software-defined radios (SDRs) exist with capable hardware – 256 or 1024 QAM with EVM (error vector magnitude) < 1 LSB – and low prices – about $300. Satellite signals and protocols are well-documented and these inexpensive SDRs can easily do the job. Worse yet, open-source spoofing software is available on Github. So, it doesn't take a nation-state actor; a playful hacker can create a lot of mischief.

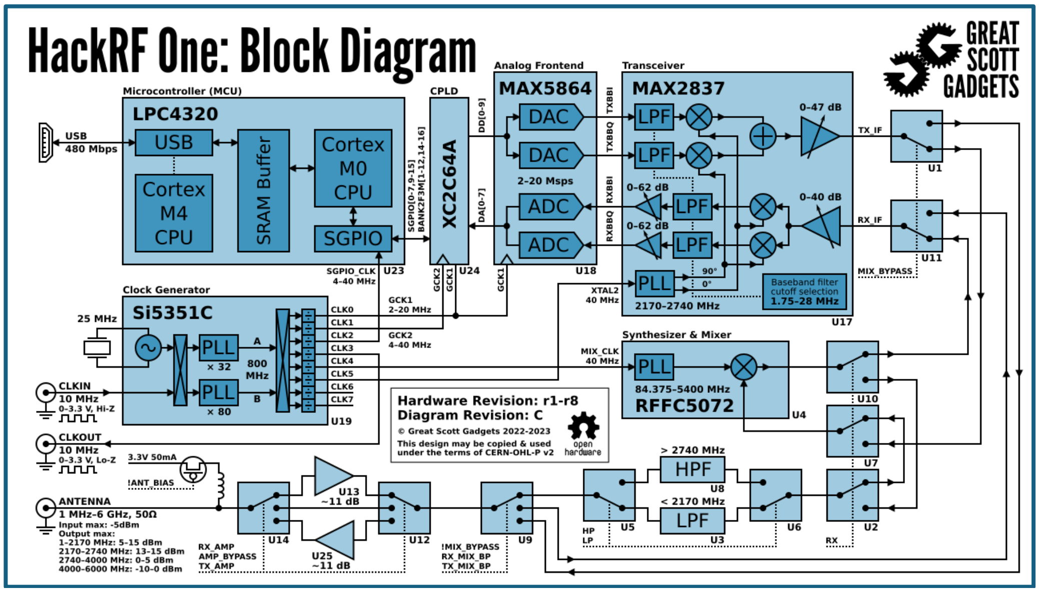


Figure 7. Schematic of a Commercially-Available Inexpensive Software-Defined Radio (SDR), source: Great Scott Gadgets

Fortunately, there is a strong portfolio of anti-spoofing technologies that can provide an effective defense.

Technologies to Mitigate GPS/GNSS Spoofing

Technologies to mitigate GNSS spoofing can be divided into three categories:

1. multi-constellation & multi-band receivers,
2. consistency checks (anomaly recognition), and
3. authentication (cryptography).

The first two technologies are widely available and should be employed. Authentication is just recently becoming available.

Multi-Constellation & Multi-Band Receivers

Consider three levels of receiver technology.

- **Single-Band GPS Receivers** – Most existing infrastructure receives only GPS and only on the L1 band. Typically, 8-10 satellites are in view at any one time, so a spoofer must simulate 10 signals simultaneously and in-phase.
- **Multi-Constellation Receivers** – In addition to GPS, there are three other global constellations, Galileo (European), GLONASS (Russian), and Beidou (Chinese) as well as local constellations, QZSS (Japanese) and IRNSS (Indian). If the timing receiver can receive multiple constellations and compare their outputs, the spoofer must simulate 4 times as many signals and spoof these signals in synchrony.
- **Multi-Constellation Multi-Band Receivers** – Each constellation broadcasts in 3 different bands. If the timing receiver can receive and compare all three bands from all constellations, the spoofer must generate and simulate as many as 120 signals simultaneously.

Multi-band multi-constellation receivers are widely available today. Using them raises the degree of difficulty for attackers.

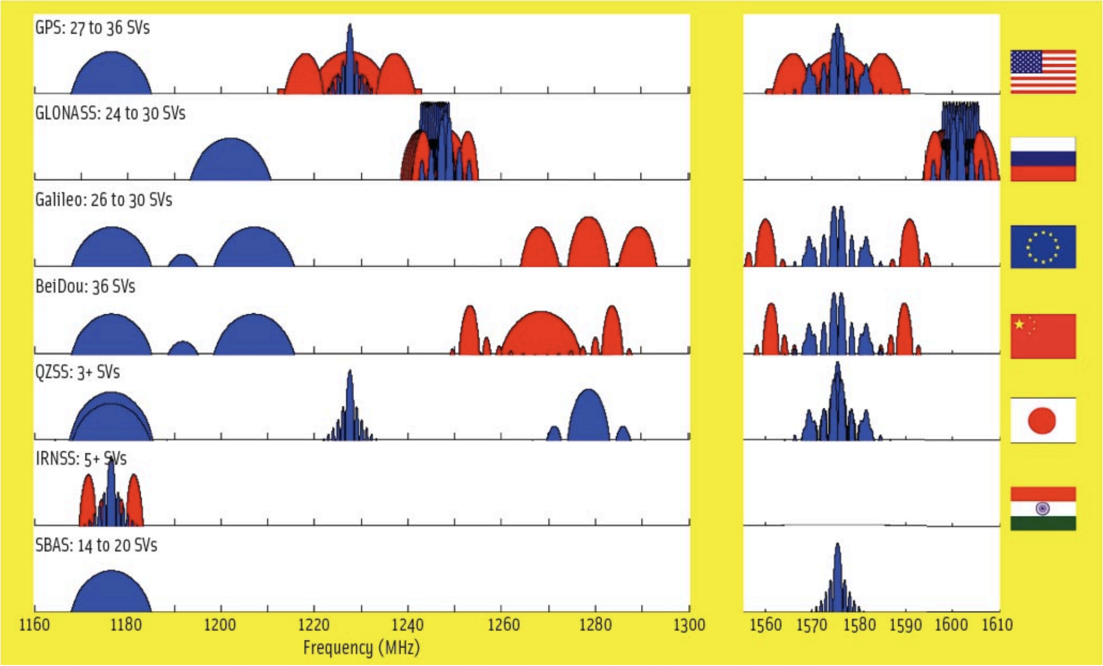


Figure 8. Radio Frequency Bands for GNSS Constellations, source: Inside GNSS

Consistency Checks

Timing receivers can be built with software to recognize anomalous signals. Often called consistency checks, these features are sometime branded with acronyms such as RAIM (Receiver Autonomous Integrity Monitoring) or such. Receivers can check many signal parameters:

- **Modulation** – receivers can check the modulation envelope of the incoming GNSS signal, but GNSS signals are well documented and SDRs are very capable, so this check, while sophisticated sounding, is easy to defeat.
- **Satellite Count** – Satellites are constantly moving so the number in view will change with time. Unusual changes in satellite count can be flagged.
- **Position –** Timing receivers are almost always fixed-site installation. Therefore, position should not be moving. If the measured position moves, it is a good indication of spoofing.
- **Power** – Receivers are at the earth’s surface and satellites are at fixed distances with fixed powers. Therefore, received power should fixed and known. Spoofers must overpower the existing GNSS signal but may not know their exact distance and cannot observe the receiver to see if the increased power is effective. So, they may use too much power, which can easily be detected. Also, as mentioned earlier, dual receivers make hitting the power window at both simultaneously very difficult.
- **Time** – To damage infrastructure, a spoofer must move time by a large amount, 10s or 100s of µs. a timing receiver with a stable reference, for example a Rubidium reference with stability better than 1 µs per day, can compare received time to the reference. If the received time drifts more than the reference, it can be flagged as spoofing. If a spoofer drifts less than the reference, it either isn’t dangerous or the spoofer must spoof for a very long time, risking detection.

Surprisingly, simple consistency checks are generally more effective than the complex ones. The last two, power and time, are the most effective.

Authentication

Quite recently, cryptography has been applied to authenticate satellite signals. This is a very effective tool to mitigate spoofing. Two authentication systems are now available:

- OSNMA (Open-Service Navigation Message Authentication) – OSNMA [11] uses the TESLA protocol, one-way has functions, and asymmetric cryptography to authenticate Galileo satellite messages. On 24 July 2025, OSNMA became fully operational. [12] OSNMA applies to Galileo only, not other constellations like GPS, GLONASS, and Beidou.
- Fugro AtomiChron NMA (Navigation Message Authentication) – Fugro maintains a network of about 100 ground reference stations that authenticate satellite signals and broadcast a hash through the Inmarsat constellation. While Galileo OSNMA is free but works only for Galileo, Fugro AtomiChron NMA [13] works for all four global constellations but charges a subscription fee.

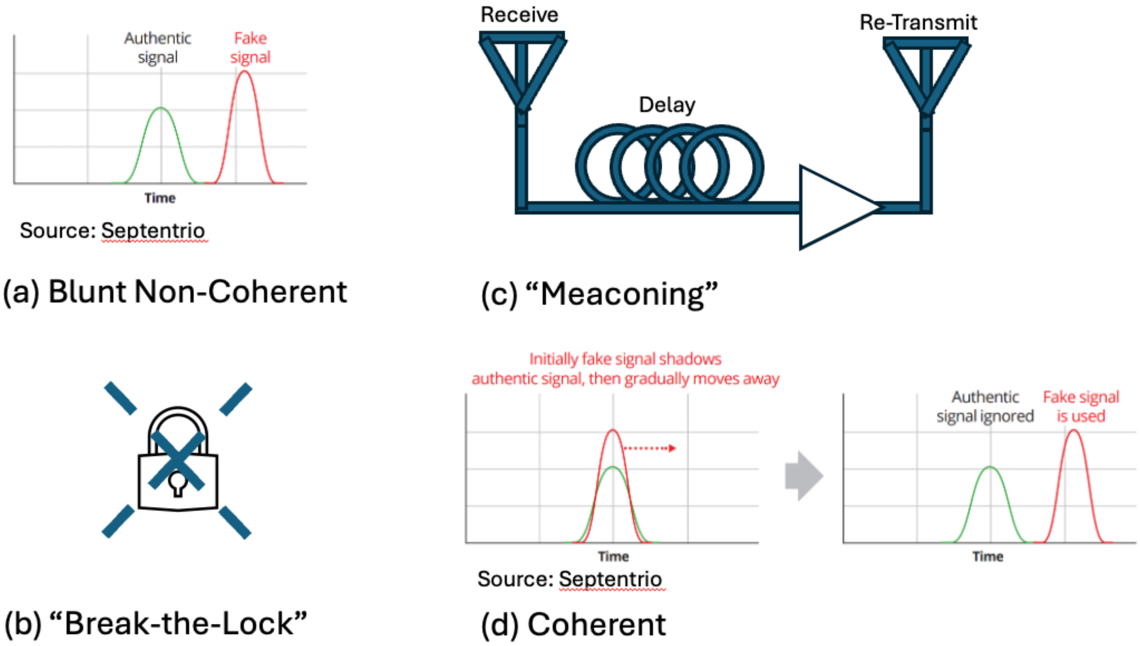
Receivers for both Galileo OSNMA and Fugro AtomiChron NMA are available now.

The combination of multi-band multi-constellation receivers, consistency checks, and authentication by cryptography offers very strong protection against spoofing.

Types of Spoofing Attacks

Spoofing attacks may be classified into four types, listed in order of severity:

1. Non-coherent blunt attack, where a spoofer simply sets up and starts a spoofing transmitter. Receiver-based consistency checks are generally effective against such attacks.
2. “Break the lock” or “knockoff jammer” attacks, where the spoofer jams first and then starts spoofing, with the hope that the receiver will acquire the new signal. Receiver-based checks are also effective against these attacks.
3. “Meaconing” where the spoofer transmits a delayed version of a received or recorded GNSS signal. Consistency checks are effective against meaconing, especially time.
4. Coherent attacks, where the spoofing transmitter first mimics the existing GNSS signal, then drifts away. The best defense against coherent attacks is authentication or time consistency checks.



Source: Septentrio

(a) Blunt Non-Coherent

(c) “Meaconing”

(b) “Break-the-Lock”

Source: Septentrio

(d) Coherent

Figure 9. Four Types of Spoofing Attacks

Testing

Testing of timing receivers is essential to find out how they behave in the presence of jamming and spoofing. Understanding the results allows developers to improve their hardware and firmware and make more resilient devices. Lab and field testing are essential to the development process.

In-Lab Testing

Devices can be tested in the development lab with a GNSS simulator. Such simulators are expensive, around $250k. This testing has the advantage that software developers can optimize and verify their algorithms. Also, the GNSS simulator can be connected directly to the receiver, so such testing does not violate spectrum regulations.

The clear disadvantage of such in-lab testing is that it is “open-book.” Developers write their own test cases. Since they know the questions, they should pass 100%. This type of testing is useful for software development, but there are no surprises, so this testing does not challenge product developers.

Organized Testing Events

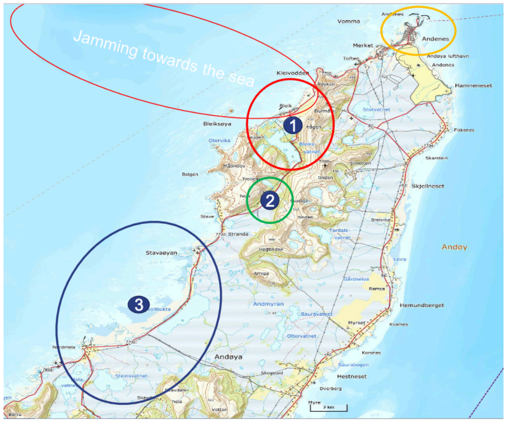
Generally, put on by governmental agencies, organized testing events have the advantage that developers do not know the test cases. Some of these events are conducted in a lab with signals distributed over a cable but others are “live-sky” meaning that they are conducted in open areas and participants must receive signals by antenna. Such “live-sky” events must be conducted in remote areas to prevent interference with normal use of GNSS and the radio spectrum.

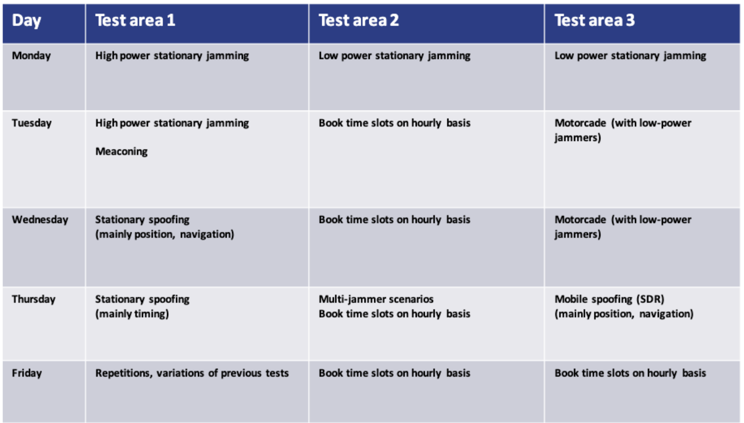
Two such events are:

- **GET-CI** (GPS Equipment Testing for Critical Infrastructure) [14] sponsored by US DoHS.
- **Jammertest** [15] conducted by Norwegian governmental organizations, held each September in Andøya, Norway, a remote place north of the arctic circle.

These events attract participants from many industries – satellite operators, GNSS chipset & module manufacturers, equipment makers, telecom service providers, and government organizations, including security and defense.

Such events combine the collective experience of a large community to present the most challenging test cases known, expose weaknesses of commercial receivers, and contribute to the advancement of anti-jamming and anti-spoofing technology. Figure 10 below shows an example overview of a Like-Sky test plan from Jammertest.





Day	Test area 1	Test area 2	Test area 3
Monday	High power stationary jamming	Low power stationary jamming	Low power stationary jamming
Tuesday	High power stationary jamming Meaconing	Book time slots on hourly basis	Motorcade (with low-power jammers)
Wednesday	Stationary spoofing (mainly position, navigation)	Book time slots on hourly basis	Motorcade (with low-power jammers)
Thursday	Stationary spoofing (mainly timing)	Multi-jammer scenarios Book time slots on hourly basis	Mobile spoofing (SDR) (mainly position, navigation)
Friday	Repetitions, variations of previous tests	Book time slots on hourly basis	Book time slots on hourly basis

Figure 10. Example Live-Sky Test Plan, source: Jammertest

Alternative PNT Sources

The fact that so many services rely on GPS and GPS is under threat has motivated the industry to propose alternative methods to obtain PNT (position, navigation, and time). Various technologies and supporting infrastructure are in development, but all face the same challenge. Deploying infrastructure, whether satellite or terrestrial, is expensive, and few customers are willing to pay to back up a free and historically reliable service. As a result, many of these technologies and services appear to be technically sound but cannot get the investment to build constellations or networks to the point where they can offer a wide coverage area.

One of the proposed technologies is low-earth orbit (LEO) satellite constellations. Because LEO satellites are much closer to earth (780 km vs. 20,200 km), they can provide a stronger signal and some immunity to jamming and spoofing. Some claim that the stronger signal also allows indoor operation, eliminating the need to put an antenna on the roof, but commercial implementations have not demonstrated dependable indoor operation. The fact that the satellites are much closer to earth means they move more quickly overhead, and the receiver has more jitter than GPS.

Another possible technology is eLORAN, which is a modernization of a low-frequency radio navigation system established during World War II. eLORAN was demonstrated in the late 1990s, but after GPS was proven effective, the U.S. Coast Guard terminated LORAN-C transmissions in 2010. Today, with concerns about GPS jamming and spoofing, there is increasing interest in eLORAN but commercial service is not possible without government investment, which is not yet committed.

The most promising solution to amend GPS and mitigate jamming and spoofing appears to be the Broadcast Positioning System (BPS), proposed by NAB, and part of ATSC 3.0. Low-jitter time transfer has already been demonstrated [16] and deployment is in progress. Using high-power (1 MW) TV transmitters, BPS promises to provide both improved resistance to jamming and spoofing and dependable indoor operation. With a target of 1600 TV stations in the US, it would provide nearly nationwide coverage. If broadcasters can retain their spectrum and invest in Cæsium oscillators or terrestrial time transport, BPS would be a worthy alternative to GPS.

Conclusions

Jamming & spoofing can be classified into three types, each with different characteristics, and the method to mitigate is specific to the type.

Civilian Jamming

Civilian jamming is quite a common problem, but easy to solve. The combination of receiver filters and holdover oscillators is generally sufficient. Horizon-nulling antennas, redundant receivers, and remote antennas may also be helpful.

Military Jamming

Military jamming is so far limited to conflict zones. Anti-jamming antennas, both CRPAs and horizon-nulling antennas, can be helpful but the real solution is terrestrial time transfer, which is expensive.

Spoofing

Spoofing is a sophisticated technique to fool a time receiver into transmitting incorrect data. Spoofing is generally conducted by nation states and is usually limited to conflict zones. Several technologies are available to mitigate spoofing:

- Multi-constellation and multi-band receivers make spoofing more difficult.
- Consistency checks are effective to identify spoofed signals. The most effective consistency checks are the simplest ones, power and time.
- Authentication of GNSS signals is a powerful toll to solve the most severe spoofing attacks.

Equipment Recommendations

The most critical decisions are to:

1. Choose a good receiver, preferably one that has been extensively tested at organized events. The receiver choice includes the use of filters and, more importantly, the algorithms to implement consistency checks.
2. Choose a holdover oscillator appropriate in cost and accuracy for the end application and production tested with worst-case specifications.
3. Make sure the receiver and time server have been tested for resilience at jamming & spoofing events.

After the core decisions of receiver and holdover oscillator, enhancements are possible depending on the risk concern, particularly for spoofing:

1. Horizon-nulling antennas are inexpensive and can be helpful.
2. Redundant receivers should be used for redundant (red and blue) networks. Remotely located antennas can help and it’s possible also to have redundant antennas per receiver.
3. Terrestrial time transfer is the most powerful protection against both jamming and spoofing, but is expensive.

About the Authors

Allan Armstrong is the CEO of Meinberg USA Inc., the US subsidiary of Meinberg Funkuhren GmbH & Co. KG. Meinberg is the leading provider of network time synchronization for many applications, notably broadcast, datacenter, finance, power grid, defense, civil aviation, and telecom. Allan began his career as an analog/RF/microwave integrated circuit designer working on test & measurement, optoelectronics, and timing. Later he had roles in applications engineering, marketing, and business management. Allan earned his BSEE from MIT in 1986.

Leigh Whitcomb is a 30+ year veteran of the Professional Broadcast Media industry. His career spans analog TV, through digital TV, HDTV and IP TV. He participates in SMPTE, Alliance for IP Media Solutions (AIMS), Institute of Electrical and Electronics Engineers (IEEE), and Video Services Forum (VSF) standards committees. He is actively involved in SMPTE ST 2110 and ST 2059. He became a SMPTE Fellow in 2017. He is the co-inventor of several patents in the areas of networking and timing and synchronization. Leigh earned his BASc from University of Waterloo and MEng from University of Toronto.

Dr. Douglas Arnold is Principal Technologist at Meinberg USA. His duties include standards development, technical marketing and pre-sales support. He is currently chair of the IEEE 1588 Working Group, Chair of the ISPCS PTP Plugfest Committee, Technical Editor of IEEE P1952, Technical Editor of IEEE P3335, Co-Author of the IETF draft Enterprise Profile for PTP, and author of the *Five-Minute Facts About Packet Timing* blog. He has over twenty years of experience designing and specifying precise timing technology. Doug holds a Ph.D. in Electrical Engineering from University of Illinois Urbana-Champaign.

Geshan Wrosinghert manages the applications engineering team at Meinberg USA, Inc, the US subsidiary of Meinberg Funkuhren GmbH & Co. KG. The applications engineering team at Meinberg helps end users find the right product within the Meinberg portfolio based on the industry they operate in as well as specific application requirements. Geshan has multidisciplinary experience in many industries including defense, power grid, automotive, pharmaceuticals, and civil engineering software. Geshan earned his BSME at Boston University in 2013.

Matt Silver is a technical support engineer at Meinberg USA Inc. He's been working in technology support and engineering roles for 25 years, spanning consumer/end user support, enterprise IT system administration, and hyperscale data center operations. He is also an avid rock drummer, and as an ongoing art project, has given out almost 4000 stickers of his face, to people traveling all over the globe. Matt earned his BA in Communication and Media Studies from California State University Sacramento.

Mathias Kleinsorge is responsible for RF development at Meinberg in Germany, including antenna technology. Mathias acquired broad experience in RF IC building block design at Infineon, in RF system design including quadband transceiver IC development at Siemens Mobile, and in multiband antenna design and development of proprietary digital wireless transmitters and receivers for digital audio at Sennheiser. He holds several patents and received his Dipl. Ing. (FH) degree from the Lippe University of Applied Sciences.

Daniel Boldt, Managing Director, Meinberg, has over two decades of expertise in time synchronization technologies, including IEEE 1588 (PTP), NTP, and Synchronous Ethernet. As one of the key architects of the Modular Time Server Platform IMS, he combines extensive embedded software expertise with broad experience in broadcasting, finance, and telecom applications. Since 2014 he was leading the Software Development department before joining the management team in January 2025. Before joining Meinberg, Daniel worked on Software tools for the DVB playout and IP streaming projects at ZDF, German Television. He holds an M.Sc. in Media Technology from the Technical University of Ilmenau, Germany.

Heiko Gerstung, Managing Director, Meinberg has a background in business administration and Computer Science. Heiko joined Meinberg over 20 years ago as a software engineer, developing software for embedded systems and rebuilding the Linux-based LANTIME Operating System (LTOS). Alongside his technical work, Heiko took on leadership roles, managing marketing and distribution partners. In 2009, founders Werner and Günter Meinberg appointed Heiko as Managing Director alongside a colleague and gradually transferred responsibility to them. Despite his role, Heiko remains actively involved in software development and supporting customers. Additionally, Heiko actively contributes to the standardization of NTP and PTP.

Bibliography

[1] M. Z. H. Bhuiyan, N. G. Ferrara, S. Thombre, A. Hashemi, M. Pattinson, M. Dumville, M. Alexandersson, E. Axell, P. Eliardsson, M. Pölöskey, V. Manikundalam, S. Lee and J. Reyes Gonzalez, "H2020 STRIKE3: Standardization of Interference Threat Monitoring and Receiver Testing - Significant Achievements and Impact," in *European Microwave Conference in Central Europe*, Prague, Czech Republic, 2019.

[2] M. Thompson, "Synchronizing the Super Bowl: A Look into Large-Scale Live Broadcast Synchronization," in *Workshop on Synchronization and Timing Systems*, San Diego, CA, USA, 2024.

[3] O. Chambin, "Synchronizing in Broadcast: The Olympic Challenge," in *Workshop on Synchronization and Timing Systems*, San Diego, CA, 2024.

[4] S. &. V. EBU, "Joint Task Force on Networked Media (JT-NM) Phase 2 Report, Reference Architecture v1.0," 2015.

[5] D. Goward, "Lack of Attention to PNT & GPS Endangers America - Critical Issue for New Administration and Congress," in *https://rntfnd.org/wp-content/uploads/Critical-Issue-Lack-of-Attention-to-PNT-and-GPS-Endangers-America.pdf*, February 2025.

[6] J. Hautcoeur and G. Panther, "Anti-Jamming GNSS Antenna for Timing Applications," in *https://sites.calian.com/app/uploads/sites/8/2023/11/Anti-Jamming-GNSS-antenna-for-timing-applications.pdf*, Waterloo, ON, Canada, 2018.

[7] ITU, "Precision time protocol telecom profile for phase/time synchronization with full timing support from the network," in *file:///Users/allan/Downloads/T-REC-G.8275.1-202211-I!!PDF-E.pdf*, Geneva, Switzerland, 2022.

[8] ITU, "Precision time protocol telecom profile for phase/time synchronization with partial timing support from the network," in *file:///Users/allan/Downloads/T-REC-G.8275.2-202211-I!!PDF-E.pdf*, Geneva, Switzerland, 2022.

[9] P. Lindgren and M. Danielson, "PTN, Wide Area Synchronization," in *International Timing and Sync Forum*, Antwerp, Belgium, 2023.

[10] U. Keten and T. Turkdogan, "Simulation of a Nationwide GPS/GNSS Outage," in *International Timing and Sync Forum*, Antwerp, Belgium, 2023.

[11] EUSPA, "Galileo Open Service Navigation Message Authentication (OSNMA)," [Online]. Available: https://www.gsc-europa.eu/galileo/services/galileo-open-service-navigation-message-authentication-osnma.

[12] EUSPA, "Galileo OSNMA FOC," 22 July 2025. [Online]. Available: https://www.euspa.europa.eu/newsroom-events/news/galileo-open-service-navigation-message-authentication-adds-another-layer.

[13] R. de Vries, "Fugro Atomichron," [Online]. Available: https://www.fugro.com/expertise/satellite-positioning/atomichron.

[14] DHS, "GET-CI," [Online]. Available: https://www.dhs.gov/science-and-technology/publication/gps-equipment-testing-critical-infrastructure-fact-sheet.

[15] "Jammertest," [Online]. Available: https://jammertest.no/.

[16] Mondal, Tariq I., J. A. Sherman and D. A. Howe, "Time Transfer Performance of the Broadcast Positioning System™ (BPS™)," in *International Technical Meeting*, Long Beach, CA, USA, 2025.