WHITEPAPER

Robust GNSS Systems for Automated Mobility

Dr. Paulo Mendes
Dr. Martin Margreiter

www.iabg.de

Analysis and Test Methodology for Protection Against Jamming and Spoofing

Executive Summary

Automated mobility increasingly relies on Global Navigation Satellite Systems (GNSS) to provide accurate positioning and precise time synchronisation. At the same time, GNSS signals are inherently vulnerable to radio-frequency interference and deliberate manipulation. Jamming and spoofing therefore pose a growing safety and security risk for automated driving functions, particularly where navigation data are used directly for vehicle control and decision-making.

IABG addresses this challenge with an integrated test methodology that systematically evaluates the robustness and resilience of GNSS-based systems under realistic conditions. The approach combines controlled laboratory simulations with authorised outdoor interference tests at the Mobility Innovation Campus (MIC) in Ottobrunn. Reproducible jamming and spoofing scenarios are executed under regulatory approval and analysed using independent ground-truth data obtained from high-precision LiDAR measurements.

A key element of the methodology is the use of an “Experimental Twin”, which digitally mirrors real test scenarios and enables repeatable evaluation, parameter variation and efficient development of countermeasures. Test results show that even low-power interference can significantly degrade GNSS performance, while spoofing attacks may introduce undetected position drifts with potentially critical consequences.

The findings underline the necessity of holistic, system-level testing, including multi-frequency GNSS, sensor fusion and integrity monitoring. IABG’s methodology supports industry and public-sector stakeholders in validating secure, standards-compliant navigation solutions and contributes to the ongoing development of European GNSS robustness standards.

1. Introduction and Motivation

Automated driving is based on the tight integration of multiple sensor systems, data fusion and decision-support algorithms. Cameras, LiDAR, radar, inertial measurement units (IMUs) and GNSS receivers continuously provide data that are fused in real time within the vehicle. Together, these sensors form what is commonly referred to as the perception and localisation stack, which constitutes a core element of automated vehicle control.

Within this stack, GNSS fulfils a dual function. On the one hand, it provides absolute positioning in a global reference frame. On the other hand, it delivers highly accurate timing information that is essential for synchronising heterogeneous sensor data. Even small deviations – on the order of a few metres or microseconds – can result in safety-critical situations when automated driving functions are active, for example during lane changes, intersection manoeuvres or emergency braking.

GNSS signals reach the Earth’s surface with extremely low power levels, typically around −160 dBW. As a consequence, even commercially available jamming devices with comparatively low transmission power are capable of severely degrading or completely blocking signal reception. Within the European STRIKE-3 project, more than 450,000 interference events were recorded, most of them caused by so-called privacy protection devices [1]. These devices are often used by heavy-goods vehicle drivers to avoid monitoring of vehicle movements. However, their emissions extend far beyond the originating vehicle and can compromise the positioning performance of surrounding road users.

2. Threat Landscape and Technical Background

2.1. Jamming

Jamming refers to the deliberate transmission of interference signals within GNSS frequency bands, most notably L1 (1575.42 MHz) and L5/E5 (1176.45 MHz). Depending on their modulation characteristics, such interference signals may be broadband – often spanning several tens of megahertz, as is typical for noise-like jammers – or narrowband, for example continuous-wave or sinusoidal signals.

From a robustness perspective, the impact of jamming is determined not only by the characteristics of the GNSS signal itself, but also by the mitigation and hardening measures implemented on the receiver side. Experimental investigations at IABG have shown that transmission powers in the microwatt range can already lead to a complete loss of signal tracking within distances of approximately 100 m. In controlled test campaigns, interference at a power level of 1 µW resulted in position errors of 6–8 m and an increase in phase noise power of up to 15 dB.

2.2. Spoofing

Spoofing attacks aim at deceiving GNSS receivers by transmitting counterfeit satellite signals that closely resemble authentic GNSS signals in terms of frequency, phase and data structure. Modern software-defined radios (SDRs) make it possible to generate and radiate such signals in a highly controlled manner, enabling attackers to gradually manipulate the position solution computed by the receiver.

Unlike jamming, spoofing is often not immediately apparent to the user. High-quality spoofing attacks may remain undetected while slowly introducing a position drift. A drift rate of only 0.5 m/s is sufficient to produce position deviations of more than 100 m within a few minutes, without triggering any alarms in conventional receivers.

Field experiments conducted by the University of Texas and the University of the Bundeswehr Munich have demonstrated that spoofing attacks against SAE Level 2 automated vehicles can lead to abrupt lane changes, unintended braking manoeuvres and even navigation failures [2][3].

2.3. Multisensory Protection

A key strategy for mitigating GNSS vulnerabilities is sensor redundancy. By cross-checking GNSS-derived position and motion data against inertial measurement units (IMU), optical sensors (cameras) and active sensors (LiDAR), inconsistencies can be identified and evaluated in real time. Such discrepancies may be detected using model-based integrity monitoring approaches, which assess the plausibility of sensor outputs within a dynamic vehicle context.

These concepts form the basis of current research initiatives such as **VorTNAF** (“Preparation of Testing and Certification of Robust Navigation for Automated Driving”), in which IABG is actively involved.

3. IABG Test Methodology

3.1. Laboratory Infrastructure

The GNSS laboratory at IABG enables precise reproduction of real satellite constellations and signal conditions. The GNSS simulator supports multi-constellation scenarios (GPS, Galileo, GLONASS) across several frequency bands (E1, E6) and can be extended to additional frequencies as required.

The laboratory environment allows:

- Simulation of authentic GNSS signals, including satellite dynamics, ionospheric delays and multipath effects,
- Superposition of synthetic jamming signals with configurable bandwidth, modulation schemes and power levels,
- Generation of spoofing scenarios involving manipulation of navigation messages at the level of navigation data, spreading codes and Doppler characteristics.

All signals can be recorded in operational environments and replayed under laboratory conditions, either unchanged or in combination with modified attack parameters. This capability enables fully reproducible test scenarios and supports reliable comparative evaluations of different receiver types or software versions.

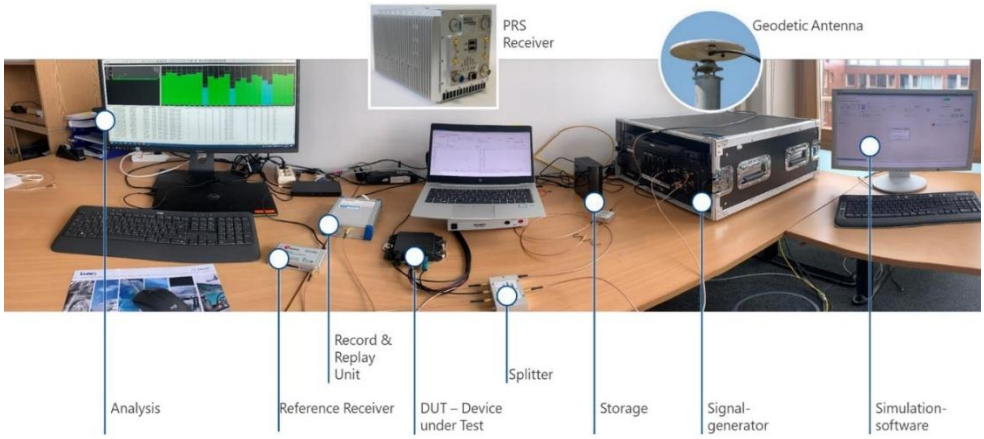

Fig. 1: GNSS- laboratory setup at IABG

3.2. Field Tests at the Mobility Innovation Campus (MIC)

To complement laboratory testing, IABG operates a dedicated test environment for automated mobility applications at the Mobility Innovation Campus (MIC) in Ottobrunn, Germany. Under authorisation by the German Federal Network Agency (BNetzA), controlled jamming and spoofing signals can be transmitted within the campus area [4].

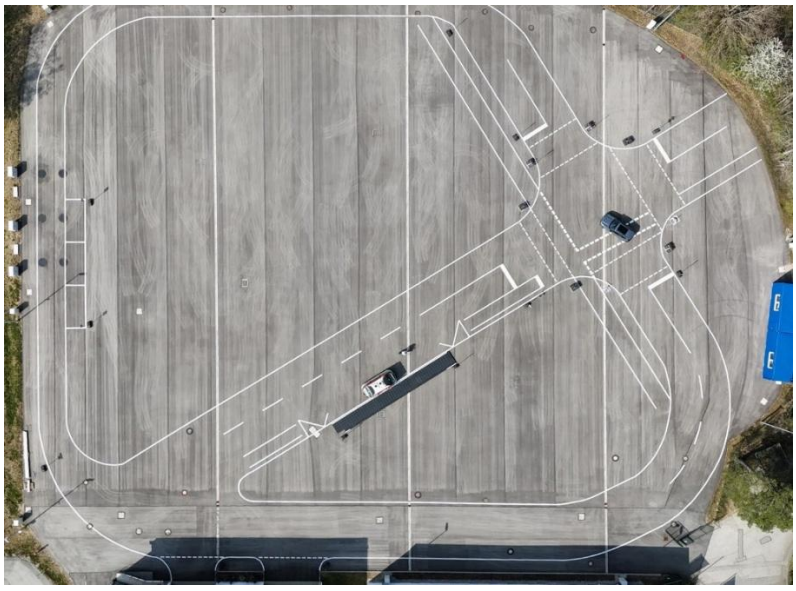

Fig. 2: Outdoor test area at the Mobility Innovation Campus (MIC)

Vehicle trajectories are captured using a distributed LiDAR network that provides ground-truth position data with an accuracy better than 2 cm. These independent reference measurements allow GNSS positioning errors to be quantified with high precision under real-world conditions.

3.3. The „Experimental Twin“

The Experimental Twin represents a digital counterpart of the physical test environment. All sensor data, vehicle states and interference parameters are stored in a synchronised database. This approach enables:

- Virtual repetition of real test scenarios with modified parameters,
- Extension of interference and attack patterns without additional field trials,
- Integration into simulation platforms for software-in-the-loop (SiL) testing.

4. Results and Analysis

4.1. Effects of Jamming

Analysis of recorded spectrograms shows that the automatic gain control (AGC) of GNSS receivers primarily reacts to the interference signal. As a result, the effective resolution of the analogue-to-digital conversion is reduced, leading to a degradation of the carrier-to-noise density ratio (C/N_0).

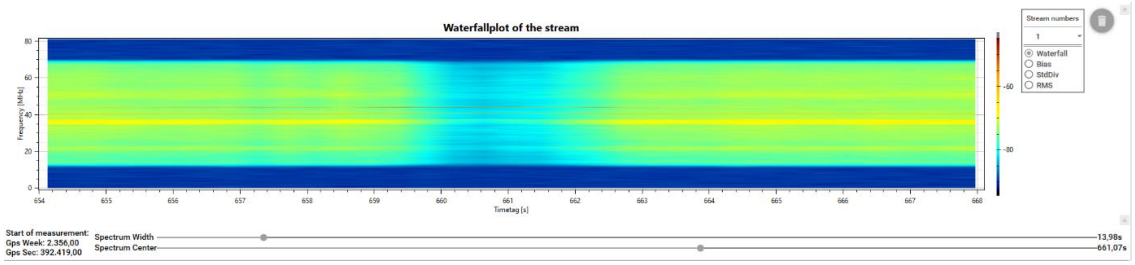

***Fig**. 3: Spectrogram of a recorded jamming event*

In the conducted tests, average C/N_0 reductions of 10–15 dB were measured. For receivers with limited robustness, this degradation was sufficient to cause loss of phase-lock-loop (PLL) tracking.

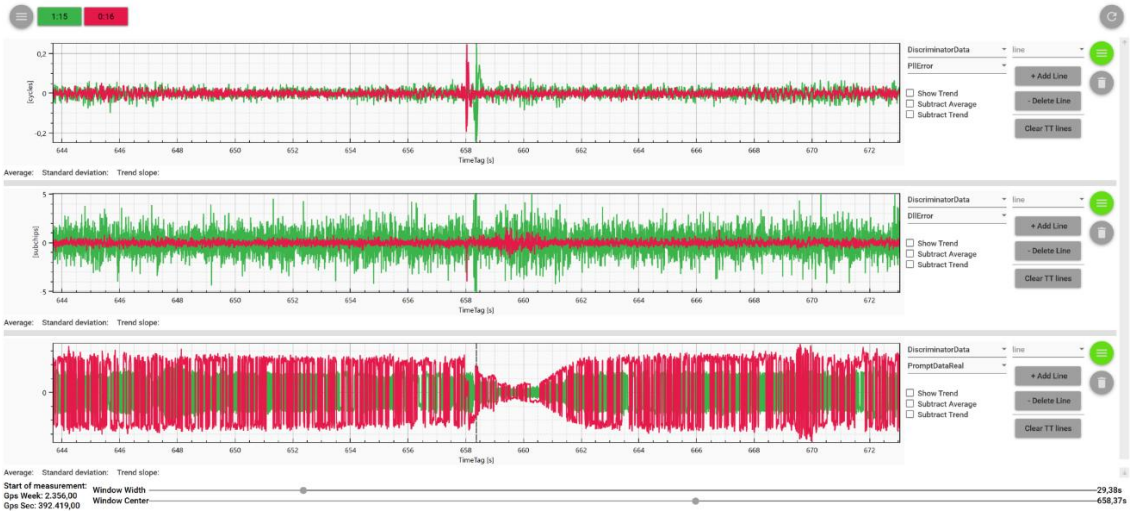

Fig. 4: Tracking error during a jamming event
Time history of PLL and DLL errors, as well as prompt correlator values, for two satellite channels (red = GPS, green = Galileo)

4.2. Effects of Spoofing

During SDR-based spoofing experiments, position drift rates between 0.2 and 0.6 m/s were measured, depending on the receiver architecture. Systems without real-time integrity monitoring mechanisms proved to be particularly vulnerable to such attacks.

4.3. Effectiveness of Countermeasures

The use of multi-frequency GNSS receivers in combination with sensor fusion approaches (GNSS + IMU + LiDAR) resulted in a significant increase in robustness. Across all test scenarios, the combined position error remained below 2 m, even during complete GNSS outages lasting up to 20 s.

Initial investigations into Galileo OSNMA (Open Service Navigation Message Authentication) confirm findings reported in international research. While authentication of navigation data substantially increases the effort required for successful spoofing, it does not yet fully eliminate the threat—particularly when authentication information is processed with latency at receiver level.

5. Conclusions and Outlook

The test results obtained by IABG demonstrate that even low-power interference can severely impair GNSS-based navigation. Evaluations limited to signal-level metrics are therefore insufficient. A holistic, system-level assessment is required.

The presented findings contribute to the ongoing development of the European EN 16803 standards series, which defines procedures for assessing accuracy, availability, continuity and integrity of GNSS-based positioning systems. In addition, IABG is able to integrate cyber-resilience aspects in accordance with ISO/IEC 27000 and TISAX into test and certification processes.

In the future, the developed methods will be transferred to other safety-critical application domains, including rail, maritime and unmanned systems, as well as agricultural GNSS applications. The overarching objective is to establish a scalable test framework that combines physical testing, simulation and standards-based evaluation.

References

[1] STRIKE-3-Projekt (2019): *European GNSS Interference Monitoring*, ARIC Aachen.

[2] Universität der Bundeswehr (2025): *MuSNAT – Multi-Sensor Analysis Tool for GNSS Evaluation*.

[3] Clements Z.; Yoder J. E.; Humphreys T. E. (2022): *Carrier-Phase and IMU Based GNSS Spoofing Detection for Ground Vehicles*, Institute of Navigation, Long Beach (CA).

[4] Margreiter M. (2025): Whitepaper IABG Mobility Innovation Campus.