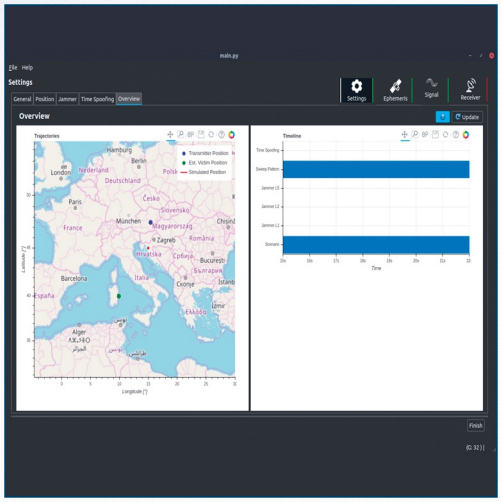
OHB DIGITAL

AJ+S
Advanced Jamming + Spoofing System



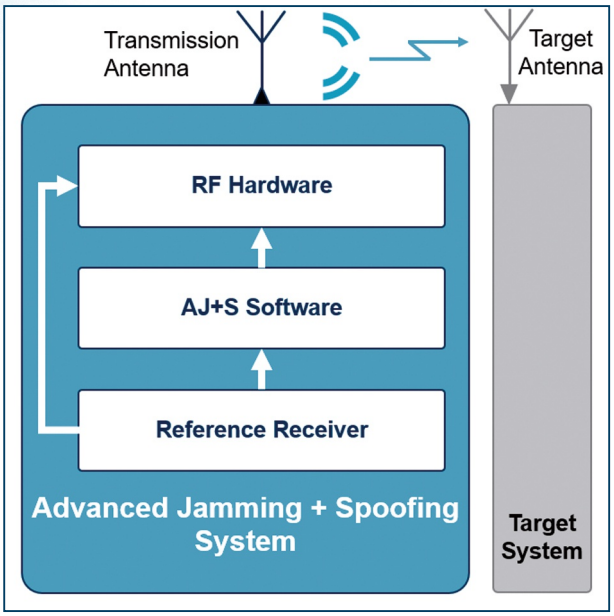
OHB Digital Solutions GmbH provides a mobile **Advanced Jamming + Spoofing (AJ+S) System** to test Global Navigation Satellite Systems (GNSS) applications against intentional interference, such as jamming or spoofing.

Most GNSS receivers rely on open service GNSS signals which can be easily affected by jamming or spoofing. The greater the dependency on GNSS services, the more serious the potential impacts of a GNSS attack. While GNSS jamming blocks deliberately the GNSS signal reception of GNSS receivers, the aim of spoofing is to manipulate the position and time information of the attacked receiver undetected.

OHB's **AJ+S** System is capable of successfully performing sophisticated jamming and spoofing attacks. Thus, it is possible to assess the vulnerability of existing GNSS solutions or the performance of countermeasures.

AJ+S

Advanced Jamming + Spoofing System



The **Advanced Jamming + Spoofing System** is used by governmental authorities and system integrators (be aware of possible export restrictions) with the aim to test and harden their GNSS-based infrastructure against possible jamming or spoofing attacks.
This mobile system, with its enhanced features, offers the most professional solution to attack GNSS equipment using interfering signals as well as the GNSS signals itself.
The **Advanced Jamming + Spoofing System** consists of Hard- and Software for generating jamming and spoofing attacks for GPS, Galileo and GLONASS signals in selected GNSS frequency bands.
Thus, it is possible to assess the vulnerability of existing GNSS solutions or the performance of countermeasures in a protected environment.
The hardware consists of:

- High-end signal generator supporting the generation of GNSS L-band signals with a bandwidth of up to 120 MHz. The following GNSS signals and systems are supported:
  - GPS L1, Galileo E1 (1575.42 MHz)
  - GPS L2 (1227.6 MHz)
  - GPS L5, Galileo E5a (1176.45 MHz)
  - GLONASS G1 (1602 MHz)
  - GLONASS G2 (1246 MHz)
- 19 inch computer with an integrated replay unit.
- Integrated reference receiver for performing synchronized spoofing attacks.
- A power amplifier with a powerful transmission antenna ensures the desired (adjustable) total transmission power.

The design of the **Advanced Jamming + Spoofing System** ensures mobility with its portable 19” box and can be put into operation within a few minutes at any place (230 VAC required). The jamming and spoofing SW is based on the GIPSIE signal simulator of OHB Digital Solutions GmbH. Further GNSS signals and systems are available on request.
An intuitive Graphical User Interface (GUI) provides predefined and configurable jamming and spoofing scenarios for the GNSS signal simulation and the time-synchronous playback of the signals. The GUI enables many further settings to generate individual and complex scenarios. The jamming and spoofing scenarios are freely configurable and, in addition to combined attacks, also enable the generation of sophisticated ones.

Spoofing Scenario

The system can obtain authentic GNSS navigation messages directly from the integrated reference receiver and generate a synchronous position- or time-spoofing. The starting point of the scenario can be defined as needed and is automatically synchronized with the “real” GNSS time. The distance-dependent runtime of the spoofing signal to the target receiver as well as the power of the signal are adjusted automatically.

Jamming Scenario

In addition to spoofing scenarios, also user-defined jamming signals can be generated and transmitted. The jamming signals are user definable (frequency, broadband, type of signal, performance) and can be generated and transmitted for up to 2 frequency bands simultaneously.

OHB Digital Solutions GmbH
www.ohb-digital.at
Rettenbacher Straße 22, 8044 Graz, Austria
T: +43-316-890971 M: info@ohb-digital.at