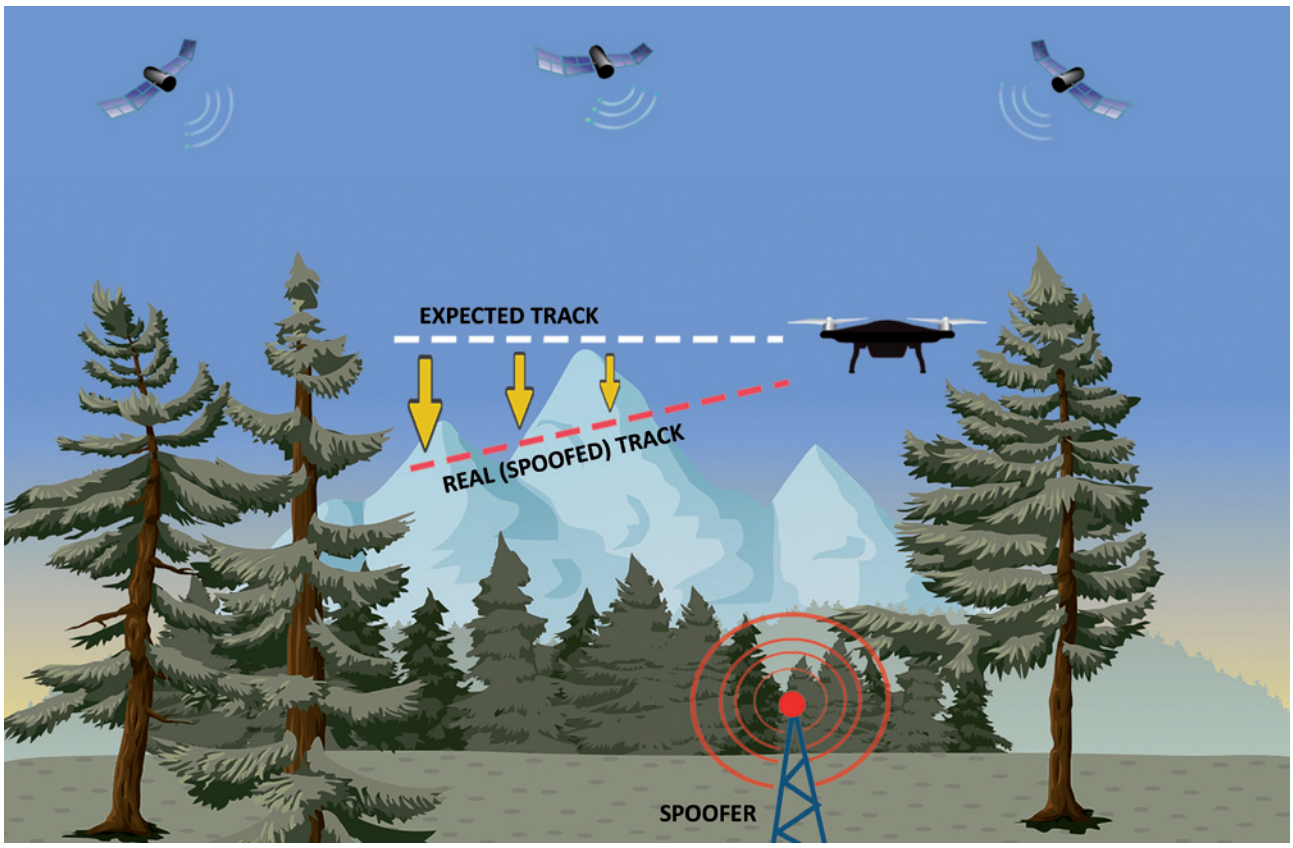
NavTD M23

Navigation Warfare Testing

Space technologies have become a strategic field of operations, in times of peace and crisis, besides land, air, sea, and cyber. Safety-critical applications in the area of national defense and internal security depend on these technologies. The greater the dependence, the greater the risk of jamming + spoofing.

OHB Digital Solutions has developed the navigation testing device **NavTD M23** that is able to assess the vulnerability of existing GNSS equipment and the performance of its countermeasures in a protected environment.

Supported GNSS signals	GPS: L1 C/A, L2C, L5 Galileo: E1 B/C, E5a-I/Q, E5b-I/Q GLONASS: G1 C/A, G2 C/A BeiDou: B1, B2 SBAS: L1 C/A
Bandwidth	up to 120 MHz per RF output
Constellation update rate	up to 250 Hz
Resolution	up to 2 x 16 bit (complex I/Q)
Operating system	Linux
Spoofing signal generation	Satellite orbit generation based on actual assistance data input Satellite clock modelling for synchronized spoofing Consideration of atmospheric delays from actual input data Tropospheric delay models: Saastamoinen, Hopfield, GPT2w Consideration of antenna gain pattern Movement simulation (input through GUI, user file or API) for spoofer, target and simulated receiver position
Frequency range	2 x RF Tuner, 9kHz – 3 GHz (0.001 Hz resolution)
Accuracy between RF1, RF2	Lower than 100µs
Reference accuracy	OCXO ±5 x 10-8 ageing per year < ±1 x 10-8 temperature stability 10 min warm-up time
Power level	Maximum power output: +20 dBm typical (before optional power amplifier) Resolution: 0.1 dB Uncertainty: ±0.5 dB: +10 dBm – -50 dBm Range: ±1.0 dB: below -50 dBm Dynamic range: -134 dBm – +20 dBm (peak); ‹75 dB typical
Spectral purity	Harmonics f >30 MHz: <-30 dBc at +10 dBm Harmonics f <30 MHz: <-40 dBc at +10 dBm Non harmonics >30 MHz: <-75 dBc typical Non harmonics <30 MHz: <-80 dBc typical
Continuous operation	Supported
Simulation iteration rate	250Hz, 100Hz, 50Hz, 10Hz
Simulation update rate of trajectory	250Hz, 100Hz, 50Hz, 10Hz, 1Hz
Simulation of hardware in the loop HIL	250Hz, 100Hz, 50Hz, 10Hz, Latency to RF output < 2ms
Simulation of receiver antenna	Gain
Logging capabilities	Time related parameters Simulated vehicle trajectory parameters Receiver antenna parameters Satellite trajectory parameters Satellite transmit antenna parameters Received signal parameters
Power supply	230 VAC
Portable Case	Customizable Standard: 978 x 625 x 467 mm, 23.1 kg, IP54
Usability	Designed for GNSS equipment testing in a realistic navigation warfare scenario



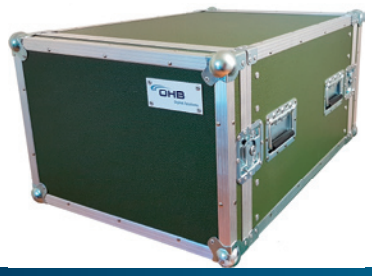
Navigation Warfare

While jamming deliberately blocks the signal reception of GNSS receivers, spoofing aims to manipulate the position and time information of the attacked receiver. This is of course enormously dangerous because the user is deceived with false time information or position and thinks he is somewhere else or at a different time than he actually is.
Since the use of GNSS will continue to increase in the future, it can be assumed that jamming and spoofing will also continue to increase. Armed forces therefore must get the possibility to test their equipment in a protected and realistic environment to assess vulnerabilities and improve equipment in order to better tackle GNSS jamming and spoofing. They have to be prepared for navigation warfare scenarios by working on jamming and spoofing as well as defending against that interference.

NavTD M23 is able to generate and transmit jamming and spoofing signals to test the effect of navigation warfare and the capabilities of countermeasures in a real environment.

NavTD M23 is a mobile and sturdy 19" rack box, including

- a user control unit (monitor, keyboard, and intuitive graphical user interface),
- a performant industrial-grade PC,
- a signal generator with dual-channel high-fidelity RF output,
- an integrated GNSS receiver for time synchronization and assistance data, and
- a broadcast antenna.




NavTD M23

With **NavTD M23** GNSS equipment can be tested under the influence of jamming and spoofing signals in a protected and realistic environment.

- Mobile, compact, and weatherproof advanced jamming and spoofing system
- Easy to use system to test military GNSS-based equipment against jamming and spoofing
- Covers a wide range of jamming and spoofing scenarios
- Supports synchronized attacks via built-in GNSS receiver
- Satellite data via built-in GNSS receiver or OHB's assistance data

NavTD M23 is able to generate and transmit jamming and spoofing signals. It allows the vulnerabilities of existing military GNSS equipment and the performance of its counter-measures to be assessed in a protected environment.

Get in touch with us to learn how to harden your GNSS-based infrastructure!

2024/02, V 3_0 - This material may contain errors or omissions, and is subject to change without prior notice. OHB Digital Solutions GmbH shall not be made liable for any specific, indirect, incidental or consequential damages because of its use. Copying of this document or giving it to others or the use or communication of the contents thereof are forbidden without express authority.

OHB DIGITAL SOLUTIONS GMBH

Kärntner Straße 7b/1
A-8020 Graz
Austria

+43-316-890971-0
www.ohb-digital.at
info@ohb-digital.at