White paper

SAL Navigation SPU-100

"Battling GPS/GNSS jamming and spoofing"

The SPU-100 shows superior performance during exposure of real GNSS jamming and spoofing signals when tested along with traditional SOLAS class GPS/GNSS systems.

Background:

GPS/GNSS technology has revolutionized maritime navigation, providing accurate and reliable positioning information. However, the reliance on GNSS for ship navigation presents significant risks, particularly due to the potential for signal jamming and spoofing. These vulnerabilities can lead to serious navigational errors, with potentially damaging consequences.

The latest years, the threats posed by signal jamming and spoofing has dramatically increased in numbers and severity due to geopolitical tensions. GNSS signal disruption and manipulation is today playing a vital role as a warfare strategy in several conflicts around the world. Equipment to perform jamming and spoofing attacks is easily available. It is today equally easy for someone to carry out such attacks outside the known conflict areas.

Characteristics of GNSS disruption.

GNSS is a navigation satellite used two decades for military and commercial positioning and navigation. Today the following systems are available, providing signals for positioning and timing on a global basis

- GPS (USA)
- GLONASS (Russia)
- Galileo (Europe)
- BeiDou (China)

One-meter accuracy is routinely achievable, and downtime events are extremely rare. Through international cooperation, these GNSS systems share common frequency bands, and affordable, multi-constellation navigation can be accomplished with a single receiver. The various signals are spaced close enough together to make reception efficient, but not so close as to interfere with each other.

All these GNSS systems share a common vulnerability as their signals are weak. GNSS satellites operate from Mid-Earth Orbit (MEO), approximately 20,000-25,000 km above the earth, to provide the best coverage and geometry for triangulation. As such, the transmitted signal is extremely weak upon arrival at the surface of the earth and makes GNSS navigation very susceptible to interference.

There are four main bands dedicated to Radio Navigation Satellite Service (RNSS), in which the GNSS constellations operate:

1. L1/E1/G1 1559 – 1610 MHz
2. L2/G2 1215 – 1254 MHz
3. L5/E5/G3 1164 – 1214 MHz
4. E6 1260 – 1300 MHz

Jamming is the presence of a competing signal that prevents the GNSS receiver from decoding the authentic satellite signal. Jamming can be a result of an intentionally act (like warfare) or sourced un-intentionally (direct or harmonic interference waves from electronics)

Spoofing is the intentional transmission of fake GNSS signals to divert users from their true position. Spoofing requires more sophisticated equipment to recreate the satellite signals. This technique is for example used in modern warfare to “capture” drones.

Several real-world incidents highlight the dangers of GPS jamming and spoofing in maritime navigation:

- **Schelder River, The Netherlands (2021)**: Strong GNSS jammer was accidently turned on at the Damen Shipyard in Vlissingen for a period of 2 hours. Analysis showed that 75% of all ships in the exposed area lost position in the period, disrupting the entrance to the Antwerp port.
- **Black Sea Incident (2017)**: Over 20 ships reported GPS anomalies in the Black Sea, with GPS receivers showing locations miles away from their actual positions. This incident is believed to be a result of GPS spoofing.
- **Port of Shanghai (2019)**: GPS jamming affected shipping operations in the busy Port of Shanghai, causing navigational disruptions and operational delays.
- **Strait of Hormuz (2019)**: Several ships reported GPS interference in the Strait of Hormuz, a critical chokepoint for global oil transportation, raising concerns about maritime security.

Example

Below is also an example from the Suez canal in May 2024, showing erratic and potential damaging positioning of ship GNSS system while under exposure of signal disruption.

Testing in real-life jamming and spoofing conditions at Andøya, Norway.

For years, SAL Navigation has via its Norwegian partners been at the front line addressing the vulnerability related to GNSS signal disruption. The result of this work was leading to the obvious need for test of equipment in a controlled jamming environment. In 2022 the first test bed was organized by Norwegian authorities in collaboration with international partners, including defense agencies and research institutions.

The jammer tests conducted at Bleik, Andøya, Norway, are significant events aimed at assessing the impact of GPS jamming on various navigation and communication systems. Andøya, with its remote location up north of Norway and controlled environment, provides an ideal location for these tests.

Below is picture of the main test area at the village of Bleik along with a close-up of one of the jamming antenna arrays purposely provided by the armed forces.

Below is picture of participants of first tests that took place in 2022. It is the first time a civilian jamming test of this scale has been carried out world-wide. The number of participants doubled for the 2023 campaign.

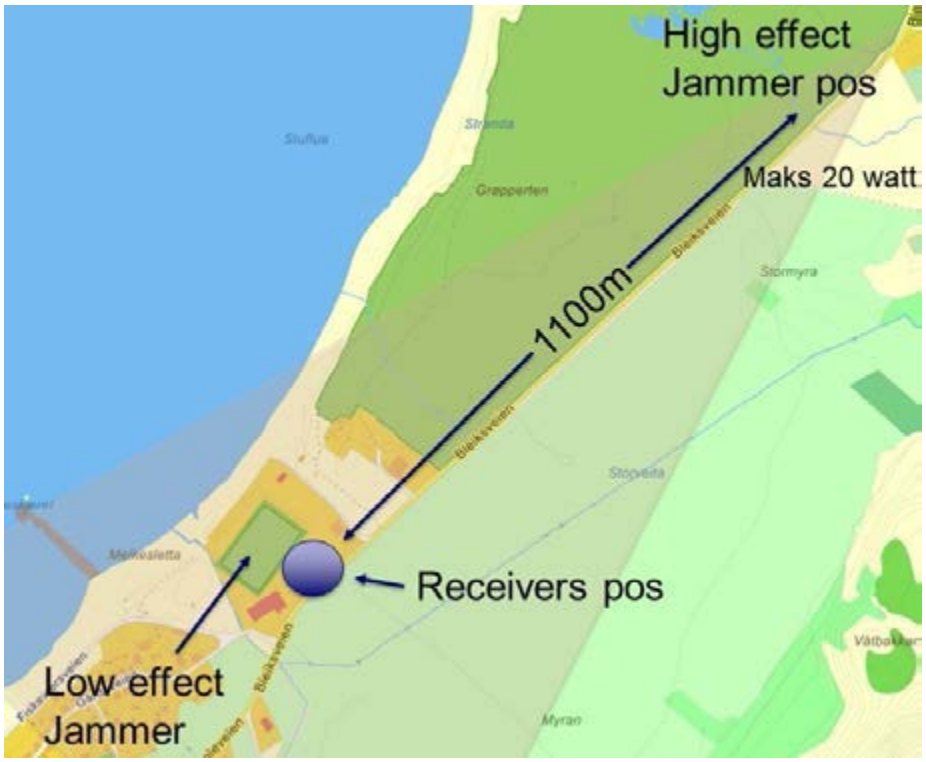
Jammer test program:

The tests at Bleik are carried out over a period of five days, covering a vast variety of jamming/spoofing scenarios. Overall, the tests are containing the following sequences:

- During the tests, three different types of interference generators were used: low-power jammers of the type commercially available from the Internet, a high-power military-caliber jammer that could vary transmit power, frequency band and modulation, and signal generators with jamming and spoofing options.
- The low-power jammers were a mix of several different L1-only jammers, L1&L2 and L1&L2&L5/E6, all with relatively wide frequency bands and typical sweep modulations, except for one that used frequency hopping.
- For the high-power jammer, two modulations were used, an unmodulated CW signal (the carrier of GPS L1) and a PRN signal (modulated carrier with C/A code from GPS satellite # 1, but without navigation message). During the tests, it was jammed in different combinations of modulations and frequency bands, whereupon the frequency bands used were L1, G1, B1l, L2, G2, L5 and E5b.
- The spoofing attacks simulated GPS L1 C/A and Galileo E1 signals, running both incoherent and coherent attacks (ie, where the signals are not synchronized or are synchronized with real-time satellite data for the test position, respectively). Otherwise, the spoofing attacks were run in combinations with jamming, both initial jamming attacks and jamming that was active while the spoofing was taking place (eg spoofing L1/E1 with jamming on G1, L2, L5).
- All these attack possibilities were then used in different test setups, and for static and dynamic combinations of jammers and attack targets (participants). An example is motorcade tests with a jammer in one of the cars in the motorcade, or with a jammer stationary on the side of the road while the motorcade drove past.

Jammertest trials

The Jammertest are organized with a strict programme, incorporating several runs each day. Some of the runs were performed with a stable interference signal, and some were used dynamically, changing interference signals. The equipment ranged from low effect handheld jammers to high effect jamming in different combinations of the different frequency bands, including power-ramp tests.
The trials were conducted around Bleik, and there were several areas which were available for the participants to conduct different types of tests. The entire test area is shown marked in red. The village of Bleik and the surrounding area was the main testing area, marked in green. In addition, there was a "sandbox" for low effect jamming trials at Grundtvatn, marked in yellow.

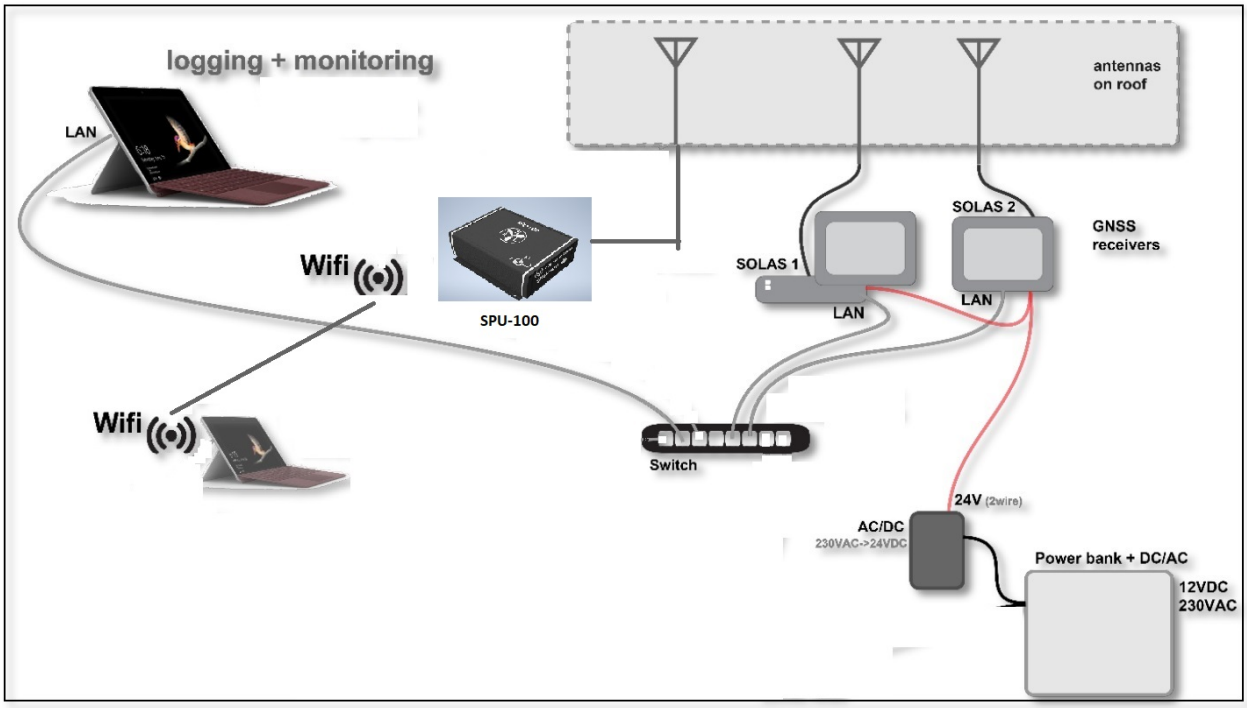


Below is the variety of “commercially available” handheld jammers tested

Test gear setup SPU-100 and SOLAS receivers

The test gear:

- One SPU-100 with high-end GNSS antennas
- Two SOLAS receivers of high-profiling brands along with GNSS antennas
- Laptops for logging raw GNSS, NMEA 0183 data and monitoring
- Power supply



Results from ramp tests

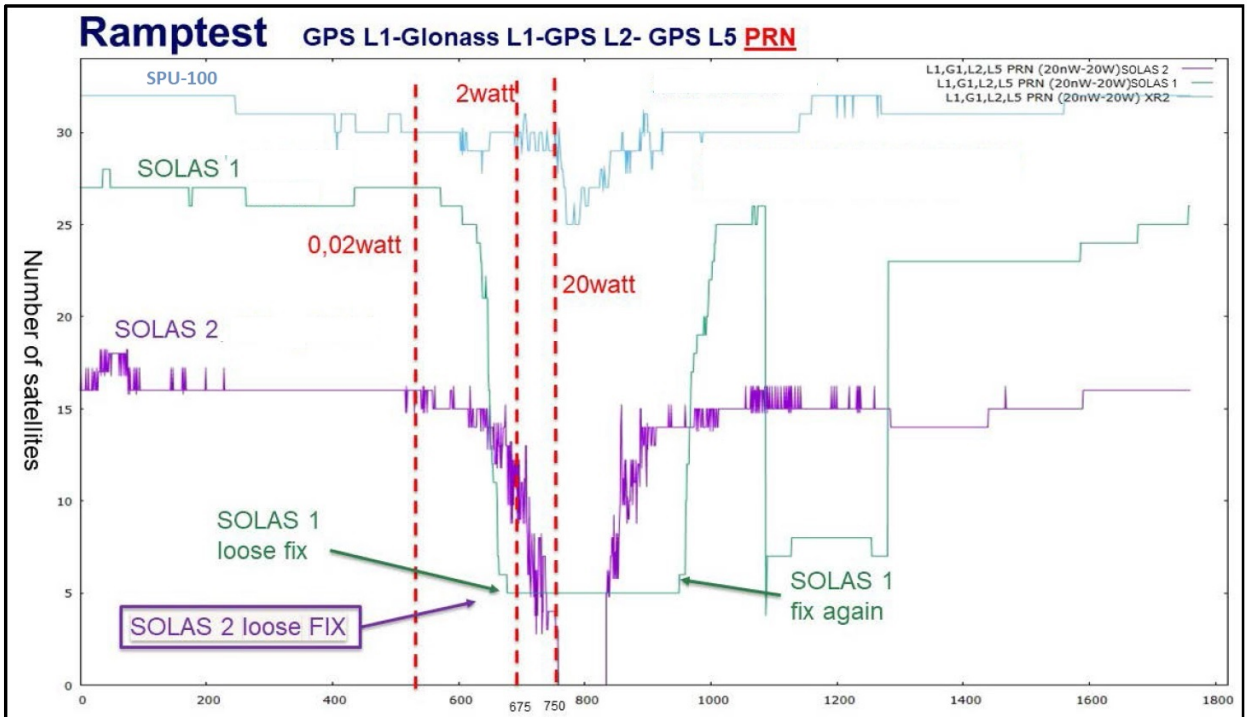
A variety of tests have been carried out. Probably the most interesting test is the Ramp test.

To investigate for a dependency on jamming power, ramp tests with increasing and decreasing jamming power were performed. In this, the receivers (and the car) are stationary and the distance to the jammer is constant at approximately 1100 m. The jammer used in this trial has a maximum power of 20 Watts, here shown for the L1, G1, L2 and L5 frequency bands.

The SPU-100 is generally performing better, never losing more than approximately 5 of its 32 satellites even during the highest intensity during this rather intensive jamming regimen. Generally, PNR jamming has a greater impact compared to CRW (continuous wave) jamming.

As displayed below, during the PRN-ramp test, at around 1-2 watt jamming from 1100 meters away, the jamming starts to affect both SOLAS receivers. More than 2 watts significantly reduce the performance, being all that is needed for the two SOLAS maritime receivers to lose position. The SPU-100 is doing very good, producing reliable positioning throughout the entire test.

Also observed during the high effect jamming trials, it seems obvious that the Signal to Noise Ratio (SNR) determined for individual satellites is a good variable for warning for jamming incidents.



Lessons learned

The tests done in 2022 has also been repeated in 2023. Further tests of SPU-100 will also commence in September 2024. The tests of SPU-100 along with the SOLAS receivers has been vetted by independent researchers from Norwegian Coastal Authorities.

The findings from 2022 and 2023 are clear. SOLAS receivers were more vulnerable to interference compared to the SPU-100.

Compared to each other, the SOLAS receivers performed to some extent more differently than was expected. At one time, one SOLAS receiver loses the position fix even though there are a lot of satellites in view and conditions seems OK, whereas other SOLAS receiver seemed stable.

The two receivers also disclosed a different time to recover after being jammed, where the one receiver came back at once after the influence was removed, and the other took a significant time to recover.

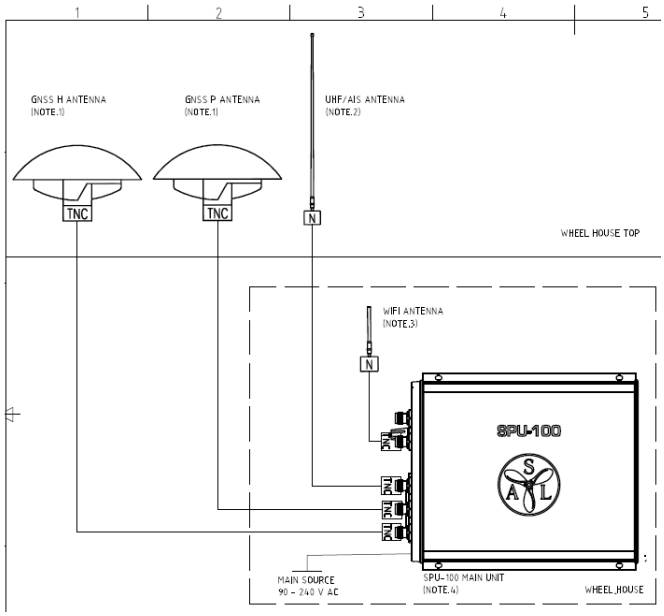
Interestingly, there seems to be different philosophies at hand on how to respond after loss of fix. One SOLAS receiver continued to send the last known position – with aging timestamp, while the other stopped sending positioning data.

Spoofing tests

Commonly, spoofing attack typically starts with a severe jamming attack to trig the GNSS receiver to lock onto the stronger spoofed signal.

The fully deployed SPU-100 is tracking signals from two high-precision antennas, with the main purpose to derive positioning as well as heading. When combining the information from the two antennas, the SPU-100 is capable to detect spoofing in a reliable way. This was thoroughly tested and proved during the Jammertest campaign in 2023.

Hence, the SPU-100 is the best tool to alert the ship crew that a spoofing attach is taking place, and that positioning derived by ship GNSS/ECDIS systems may be severely affected.



Further developments

The SPU-100 is prepared to receive signals from a third GNSS antenna. The plan for near future is to offer a specialized Anti Jamming antenna to operate as backup in case the ship is exposed to severe jamming attack in the scale and severity seen in warzones today.