



Jamming and spoofing of safety-critical infrastructure

Global navigation satellite systems (GNSS) are ubiquitous and the backbone of many modern applications and services. It is not only positioning but also precise timing solutions which heavily rely on GNSS and its nominal performance. GNSS satellites orbit the Earth at an altitude of approximately 20.000 km, transmitting signals with a transmission power in the order of magnitude of approximately 100 Watts. This results in the signals received at the Earth's surface being very weak and susceptible to signal interference. This white paper shows the results of permanent GNSS quality monitoring near a European city and airport and demonstrates, that GNSS signal interference is more than a theoretical threat on an daily basis. Especially for safety-critical applications and infrastructure, close monitoring of the GNSS signals' health and quality is crucial!

Author: Manuel Kadletz, Product Manager – GNSS Quality Assurance
Date: January 2023

GNSS signal interference is not only a theoretical or military threat

OHB Digital Solutions researches and develops in the field of GNSS for more than two decades. In all of our activities since, a deep understanding of the GNSS signal design, its strengths but also weaknesses has been an integral part of what we do. One of the main focuses is and has always been the monitoring of the quality of the GNSS signals and services. Early on, we conducted field measurement campaigns to observe and analyze the received GNSS signals and evaluate their quality and possible disturbance by surrounding factors.

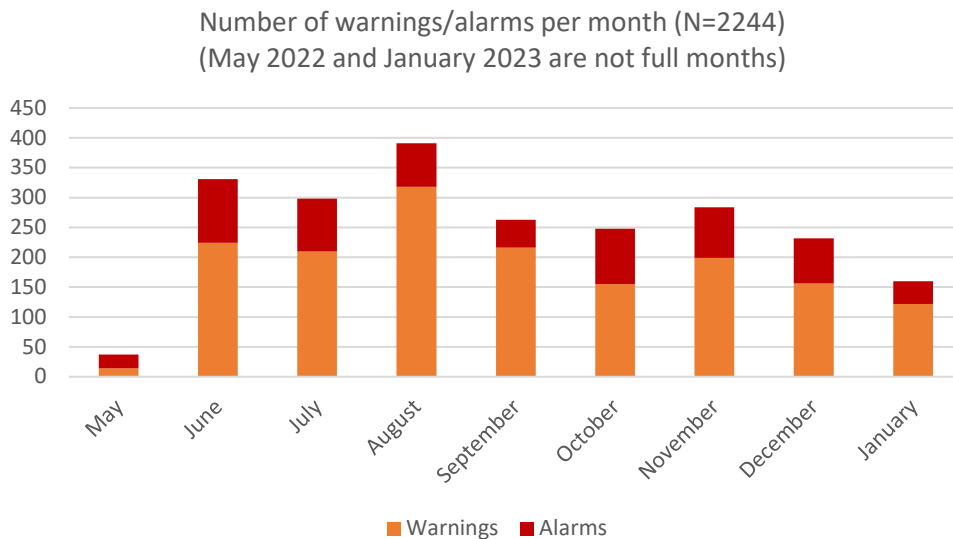


Analyzing the recorded data revealed that aside from natural interference, such as e.g., multipath, also intentional interference, such as signals from jammers appear on a frequent basis. A measurement campaign alongside the A9 motorway in Styria, Austria back in 2014 showed a first correlation of interference signals in the GNSS frequency band with bypassing trucks. These worrisome results lead to the development of permanent monitoring solutions which are the basis of today's GNSS quality assurance solutions of OHB. Since late 2021 and 2022, we operate three permanent GNSS interference detection and analysis systems (GIDAS) in Estonia, the Czech Republic and Austria, which detect GNSS jamming nearly on a daily basis. This white paper presents the jamming detection results of one of those installations during the last months and highlights the go-to strategy to get ahold of GNSS jamming and spoofing by use of a 24/7 monitoring solution.

Our recommendation is: The first vital step for GNSS-dependent applications is to be aware in real-time as soon as the GNSS performance is not nominal. By learning from recorded interference event data over time, a solid mitigation strategy can be designed to improve the robustness of safety-critical applications and systems!

GNSS interference occurs on a daily basis – especially along motorways

Since May 2022 we operate a permanent **GIDAS** installation at a European airport, together with the local air navigation service provider. The goal of the commonly operated GNSS quality assurance system is to gather data-based evidence for future decision-making and strategy definition on how to handle GNSS interference, inflicting air traffic surrounding the airport premises. The first eight months of operation show, that especially along motorways and construction sites, the quantity of interference signals in the restricted GNSS bands is even higher than expected. Between the 17th of May 2022 and the 18th of January 2023 (246 days of operation), the system detected 630 interference events with a severity classified as an alarm (which means that there was an actual degradation of the GNSS measurement quality). During this period an additional number of 1614 interference events with a severity classified as a warning has been captured.

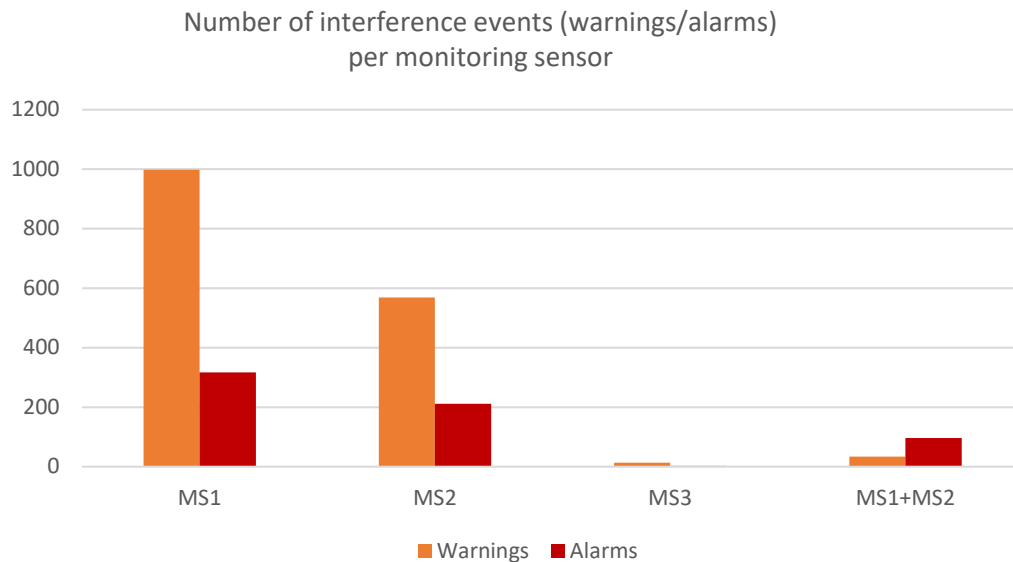


The **GIDAS** installation recording the presented data is composed of three distinct monitoring sensors, placed at strategic positions on the airport premises. The monitoring sensors cover both approach directions on the north and south end of the runway and host one additional monitoring sensor at the airport tower.

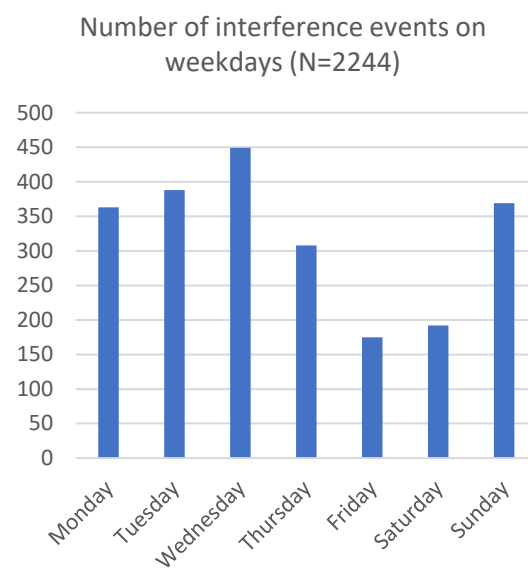
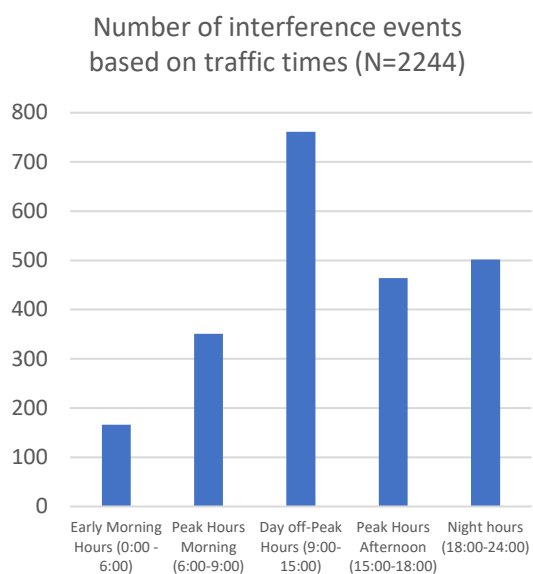


The monitoring sensor 3 (MS3) has been relocated during the monitoring period, in January 2023, right before the data evaluation. Thus, the data recorded at this site cannot be considered.

The highest number of interference alarms and warnings has been recorded at the MS1 and MS2 site, both close to either a motorway or a busy country road. In total, a number of 98 interference events have been critical enough to be recorded at least at two sites in parallel. The distance between the sites MS1 and MS2 is 1,4 km. Again, the site MS3 cannot be considered for this analysis, as it was relocated during the monitoring period.

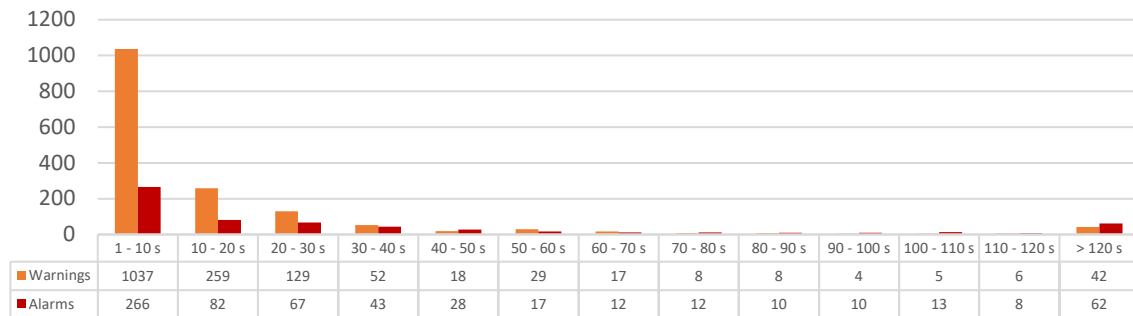


Analyzing the interference event data with respect to weekdays and time of day shows, that a significant number of interference events correlate with work-related traffic. This supports the thesis of company trucks operating jamming devices inside their truck cabin to shield their position against a fleet management system, with the side effect of jamming GNSS signals in a wider area and even affecting airport systems. The peak on Sunday is related to the weekend truck driving ban ending at 22:00 CET on Sunday. The work week of a truck driver in Austria typically starts at that time. Disguised by a jammer, it seems some trucks start a little earlier than the legal limit.

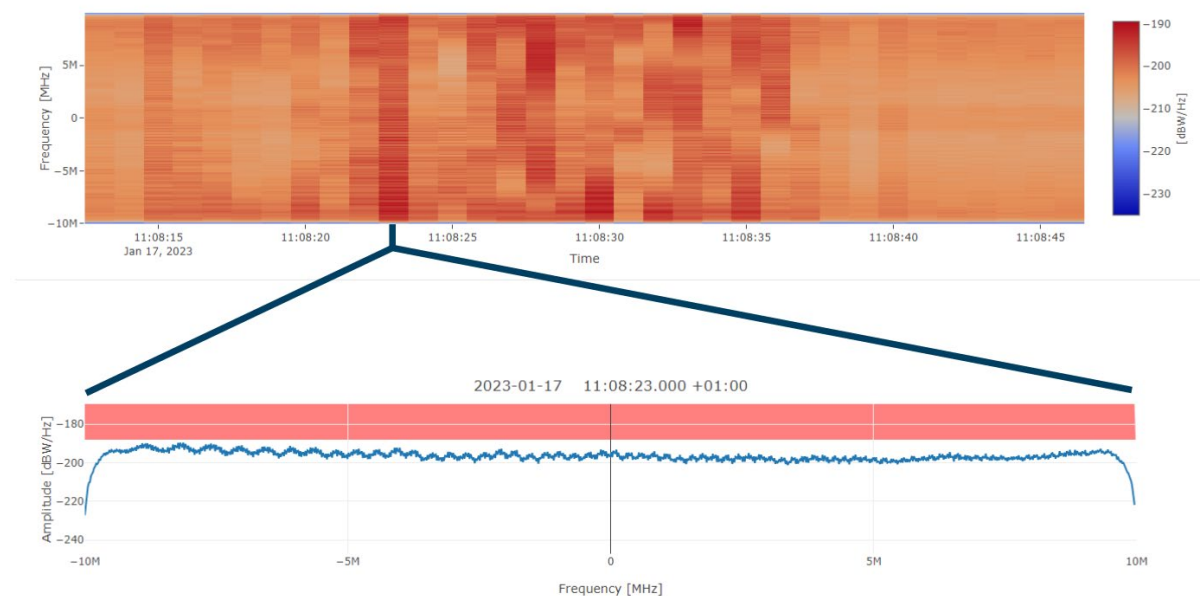


More than 80% of the recorded interference events, both warning and alarm, have a duration of 30 seconds or less, which is expected for bypassing vehicles. But at least two recorded events, classified as alarm, have continuously lasted for more than 30 minutes. (these events are included in the “> 120 s” group)

Number of interference events, grouped based on the duration (N=2244)

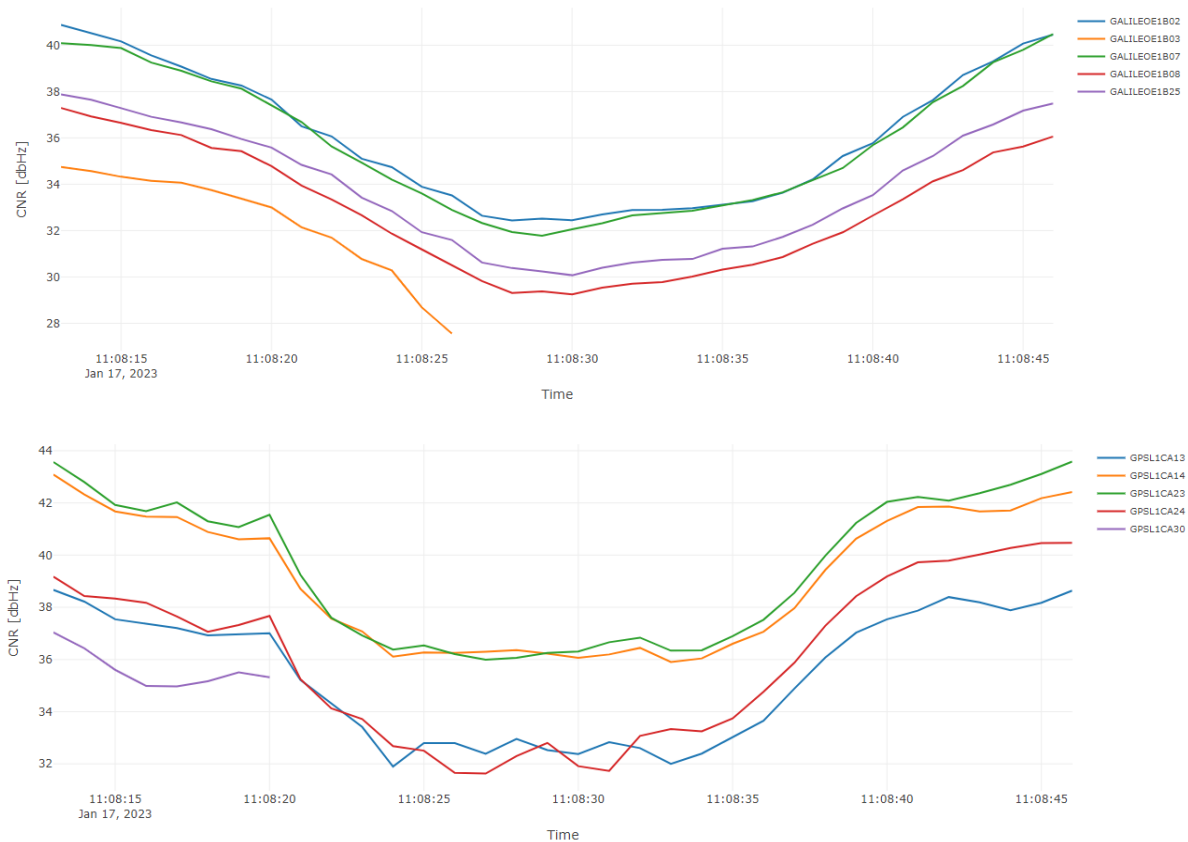


As an example of a typically recorded interference, a swept continuous wave (SCW) jammer is displayed. The graphic below shows the power spectral density (PSD) of the recorded baseband signal in the L1 frequency band (1575.42 MHz).

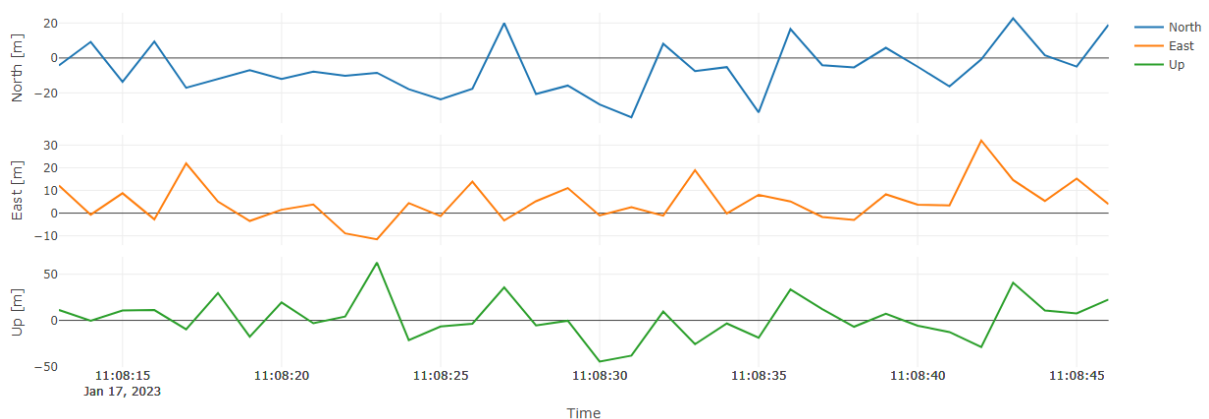


Since **GIDAS** automatically captures and stores raw baseband signal snapshots for every interference event, it is even possible to gather more detailed insights on the jamming signals by post processing analyses. As an example, the short time Fourier transform (STFT), which is also used to automatically classify the type of signal, is presented for the same interference event.

The recorded SCW jammer leads to a significant drop in the measured carrier-to-noise ratio (CNR) of the tracked GPS and Galileo satellite signals.



Even though the GNSS measurement quality is degraded significantly during the presence of a jamming signal, a typical GNSS receiver is still outputting a position solution, without any warning. This can lead to misleading PNT information without recognition of a of the jamming.



COTS GNSS receivers are typically designed to output a PNT solution to the extent possible, even during the presence of interference signals. Thus, it is very important to monitor the quality of GNSS with an independent system, designed to have quality monitoring as its first priority.

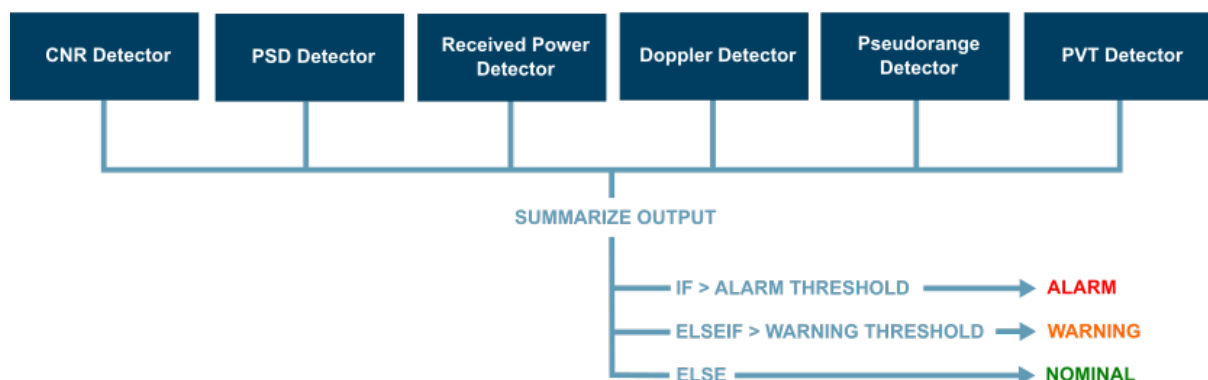
Tackle the issue - with the first step, real-time monitoring

OHb's **GIDAS** is the market-leading GNSS quality assurance system for permanent installations at safety-critical infrastructure, such as airports. The technology has been developed in more than two decades of research in GNSS signal processing and interference detection and performs robust, real-time interference detection and alerting. In the case of an airport being monitored, the air traffic management (ATM) can directly be interfaced with custom alert interfaces (software-based or hardware-based). With **GIDAS**, air traffic controllers have a live view at the on-site health and quality of GNSS, before navigation systems are negatively affected by GNSS interference.



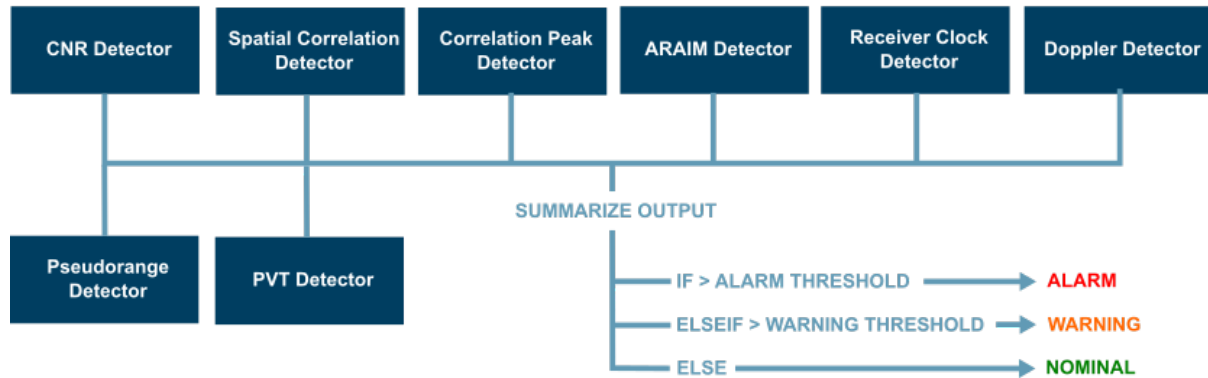
The go-to approach of **GIDAS** is to continuously monitor the GNSS signals and services. **GIDAS** supports all civilian GNSS constellations (GPS, Galileo, GLONASS, Beidou, QZSS) and all civilian GNSS signals. Based on 24/7 monitoring, **GIDAS** processes the digitized GNSS signals and performs a multitude of combined detection techniques to robustly and reliably detect interference signals. The jamming detection model combines detection techniques with individual strengths in different scenarios and different jammer types. Depending on specific combinations of the detection techniques indicating the presence of interference, the system either raises a warning or an alarm. This approach covers a wide range of different jammer types and minimizes the probability of false alarms.

GIDAS JAMMING DETECTION MODEL

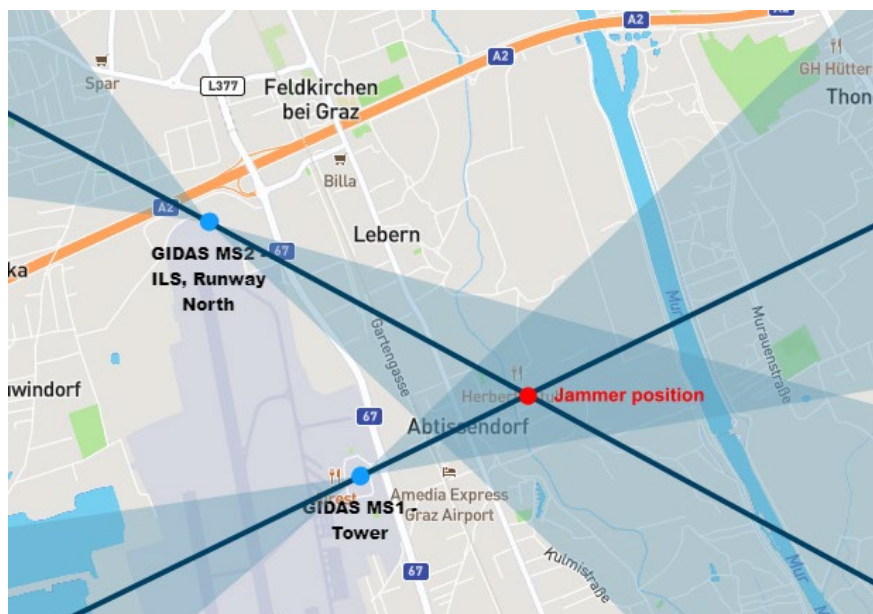


For spoofing detection the **GIDAS** system uses another set of carefully selected techniques. For the combined approach, the same mechanism applies as for the jamming detection model. Depending on specific combinations of the detection techniques indicating the presence of interference, the system either raises a warning or an alarm.

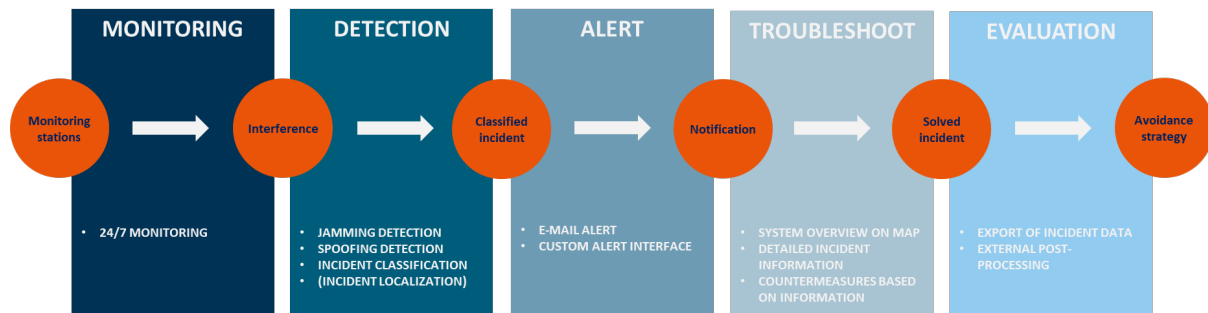
GIDAS SPOOFING DETECTION MODEL



After the detection, **GIDAS** performs additional steps and classifies the interference signal type as well as localize the signal source. The classification of jamming signals distinguishes between amplitude modulated (AM), frequency modulated (FM), continuous wave (CW), swept continuous wave (SCW) and pulsed jammer types. A **GIDAS** installation typically includes three or more monitoring sensors (MS), depending on the size of the area that needs to be monitored. Each monitoring sensor is built up by a distinct dual-module GNSS antenna combined with a local signal processing unit. Multiple monitoring sensors distributed over the to-be-monitored area can localize the interference signal source by triangulation.



The next step after detection, classification, and localization is the automatic alerting to an operator or higher-level system which is available within **GIDAS** via a customizable, automatic alerting interface. The typical time-to-alert (TTA) of the **GIDAS** system is well below six seconds. For troubleshooting, evaluation of countermeasures and long-term mitigation measures, the **GIDAS** system automatically records snapshots of the raw baseband signal as well as all intermediate detector results and jamming or spoofing alarm levels.



OHb’s GNSS interference detection and analysis system is a turn-key solution for safety-critical infrastructure, to automatically monitor the GNSS signals and services in real-time.

Since 2022 GIDAS is also available as a portable version. All features of GIDAS are integrated into a ruggedized form factor, designed for fully autonomous use.

In addition to the autonomous operation mode, GIDAS portable can also be connected to a stationary GIDAS installation as an easily relocatable monitoring sensor.



Summary

GNSS interference is more than a theoretical threat, especially to safety-critical, GNSS-dependent applications and services. Permanently installed GNSS quality assurance systems monitor the GNSS signals and services on a 24/7 basis and alert operators and higher-level systems before GNSS interference results in a safety risk. Multiple reports went public in the last months and years, highlighting the frequent occurrence of GNSS interference and the impact on safety-critical applications. Jamming being a daily observable phenomenon is confirmed by our monitoring systems too. This is also true far away from military conflict zones. Take a first step and increase your operational safety by getting in contact with us and asking for **GIDAS** consultation.

info@ohb-digital.at