

**GIDAS EMBEDDED**

# GNSS SECURITY

**INTRODUCTION**

In this document, the term interference is limited to jamming and spoofing. Jamming refers to the transmission of interfering signals with the aim of degrading the GNSS measurement quality or denying GNSS services. Spoofing is the transmission of false GNSS signals with the aim of deliberately falsifying GNSS-based time measurement.

**GENERAL METHODOLOGY**

The general methodology within GIDAS Embedded relies on the usage of multiple individual detectors for jamming and spoofing. These detectors are independently evaluated and provide (within their respective capabilities and limits) a monitoring result, indicating jamming, spoofing or normal operations.

For the final interference detection decision, all individual detector results are combined within a weighted approach, accounting for the strengths and weaknesses of the individual detectors. This approach ensures that the strengths of certain detectors can overcome the weaknesses of others and vice versa. The threshold settings and combination weightings are chosen empirically optimized for detection sensitivity while at the same time maintaining a reasonable false alarm rate.

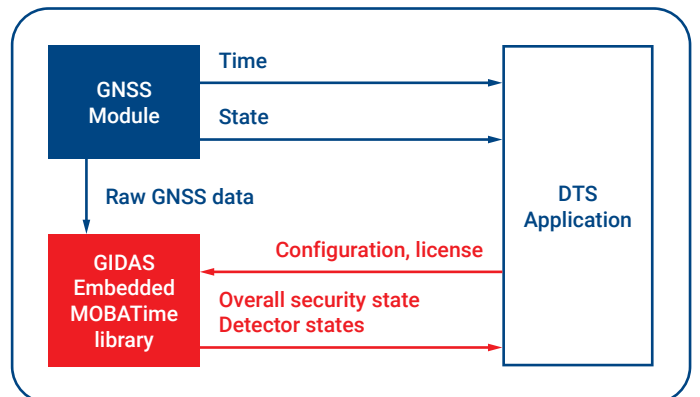
**MOBATIME IMPLEMENTATION**

The key components consist of the GNSS receiver module of the MOBATime application and the GIDAS library developed by OHB. Time and state are regularly sent to the application while the raw data from the GNSS receiver module is permanently transmitted to the GIDAS library.

The DTS application receives the overall security state as well as the different detector states as a return value. Using the severity levels (jamming & spoofing), the return values are classified as „GNSS security warning“ and „GNSS security error“.

A warning is forwarded to the Network Management System (NMS) and any third-party systems for information purposes only. Low risk of interference detected - No action for the time server in this scenario. If one or both severity levels exceed the threshold value of 20%, this leads to an error.

Similar to the warning, the error is forwarded to the NMS and any third-party systems, but the DTS application discards the GNSS source signal as a time source and goes into holdover as long as the error is present. Once the GNSS signal has been released by the GIDAS library, the time server switches back from holdover to normal operation.



**LICENSE MODEL**

One-time license per device. The license activates the GIDAS Embedded software features for a customer device and includes the usage of the GIDAS background IP. The license validity does not end. The license is bound to a specific device and cannot be transferred. The license does not include future upgrades. Future upgrades to the functionality of GIDAS Embedded are possible, but not automatically included.

**SUPPORTED DEVICES**

- DTS 4160.grandmaster
- DTS 4210.timecenter

*Do you have any questions?  
We are happy to help.*