MOBATIME
GNSS Security

Guideline and Description

Scope:	DTS 4210.timecenter
	DTS 4150/60.grandmaster
	GNSS 4500 -> All Master clocks and time servers

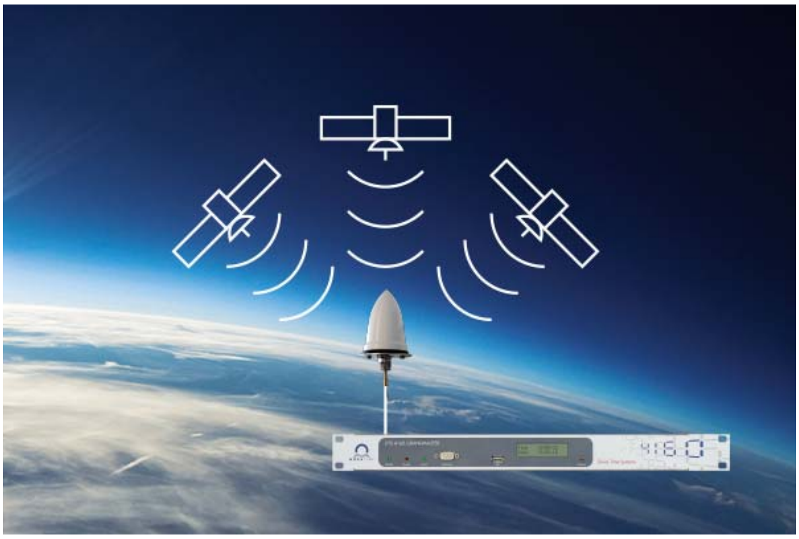


Table of contents

1 Scope 3

2 Introduction GNSS security 3

2.1 Jamming 3

2.2 Spoofing 4

2.3 Why is GNSS security important 4

2.4 What are the standards for GNSS security 5

3 High precision time server with integrated GNSS module 6

3.1 Security Features 6

3.2 GNSS Security Level according to PNT frame work [1] 6

3.3 Recommendation to increase the GNSS security level 6

4 Time server with GNSS 4500 7

4.1 Security Features 7

4.2 GNSS Security Level according to PNT frame work [1] 7

4.3 Recommendation to increase the GNSS security level 7

5 Masterclocks with GNSS 4500 8

5.1 Security Features 8

5.2 GNSS Security Level according to PNT frame work [1] 8

5.3 Recommendation to increase the GNSS security level 8

6 Abbreviations 9

7 References 10

8 Document revision 11

1 Scope

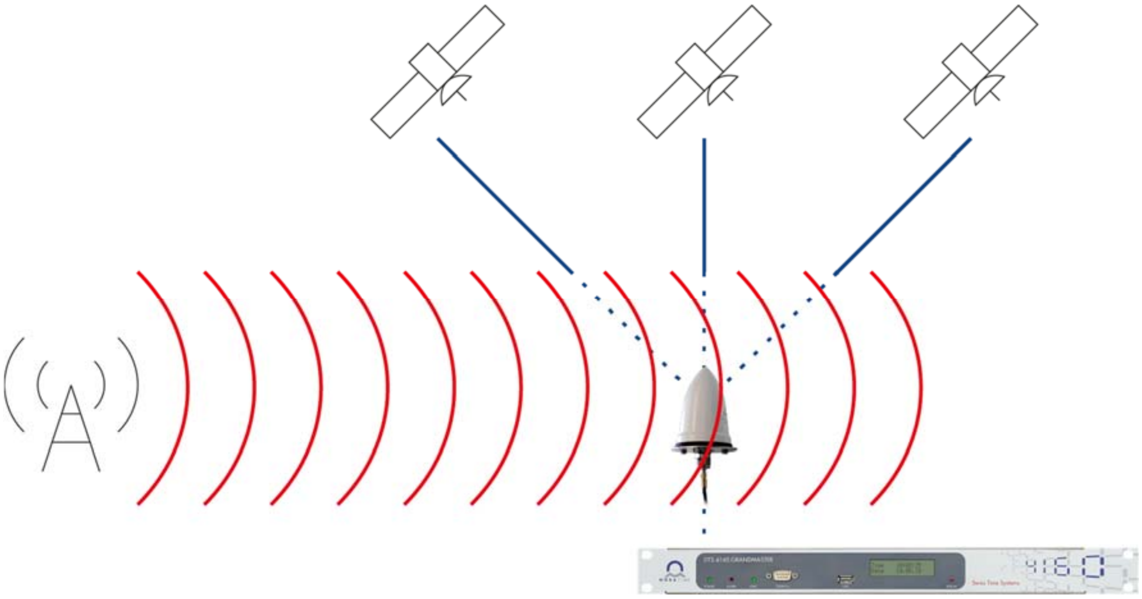
Mobatime is aware of the GNSS Security issues, which we and our customers are facing. We are continuously working on our devices to improve the security level and providing the most stable time source. With this document we are sharing our know-how and explaining the GNSS Security topic and the current threats.

The guideline is showing the current status of our devices and informs about the most secure configuration regarding GNSS time reception. Additionally it gives some guidance how to improve the overall system security.

2 Introduction GNSS security

2.1 Jamming

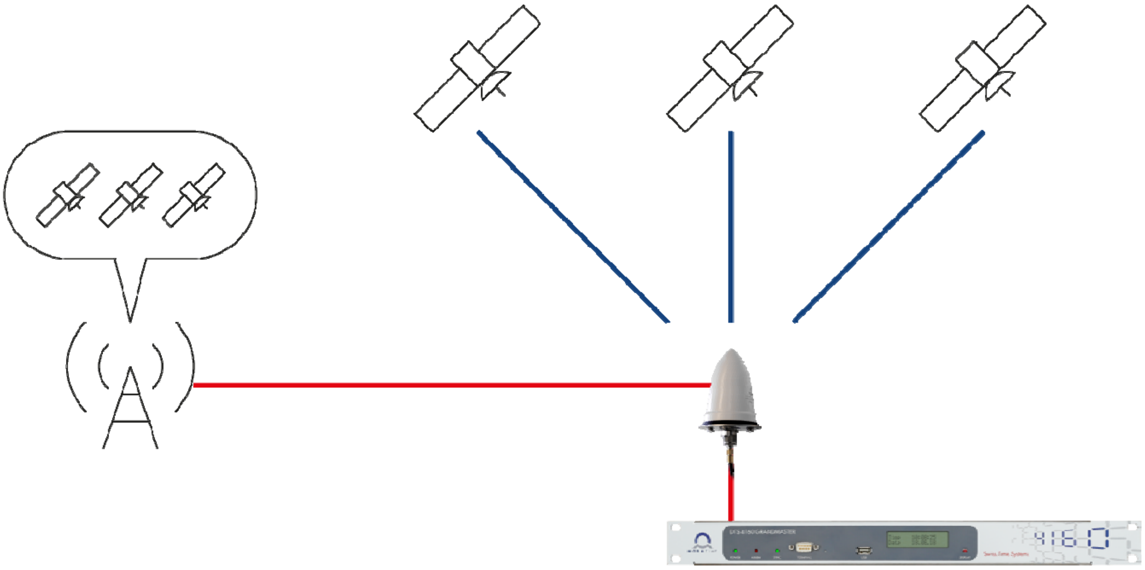
Jamming is the act of emitting strong electronic “noise” in the same frequency band as the GNSS signals, which prevents the receiver from getting the wanted GNSS signals. The jamming signal is saturating the low noise amplifier in the antenna and as a result no signal is passed to the receiver.



GNSS jamming is illegal in most countries, but the equipment is simple and readily available for a low budget. Almost no knowledge is needed and due to the low signal level of GNSS a jamming attack can disable reception over a large area.

2.2 Spoofing

Spoofing is a malicious attempt to manipulate the GNSS based time or position of a receiver by generating and transmitting fake GNSS signals. With these forged signals the spoofer tries to lead the receiver to a false position or time.



There is not only one type of spoofing attack. There are many different levels of attacks to consider. With modern and cheap SDR device (Software defined Radio) and an antenna a simple spoofing attack can be introduced. Such devices are available on a low budget and the tutorials are on YouTube. Such simple spoofing attacks are detected by the GNSS module, because there is a time jump or the signal level is unrealistically high. This kind of attack can be detected and do not lead to an issue.

A sophisticated spoofing attack requires professional equipment and a deep knowledge of the GNSS system to recreate the GNSS signal without noticing by the receiver module. These kind of attempts are hard to detect and the best solution is to have more than one source to compare, if one drift away.

2.3 Why is GNSS security important

If the GNSS receiver of a time server or a master clock is successfully spoofed, the time of this device can drift away from the correct UTC time. If the spoofing is not detected, the time server is distributing this invalid time to all its connected clients over different interfaces such as PTP, NTP or MOBALine.

The consequences of such an event are dependent on the customer's application. The customer needs to analyze the risk, which his system is facing, if the time source is manipulated.

Simple synchronized Clock system (e.g. School)
If the system is a master clock with some connected analogue and digital clocks, the consequences of a time deviation are quite low. If the deviation is bigger than seconds, the lessons will start too early or too late, but mostly nobody will even see the difference. In this case GNSS security Level 1 according the Conformance Framework from Homeland Security [1] is sufficient

Precise Reference for technical applications (e.g. automation industries)
Where the time server is used as a precise reference for a technical application, even a small deviation can lead to a system shutdown or even worse to a collision or some other damage or malfunction of the system.

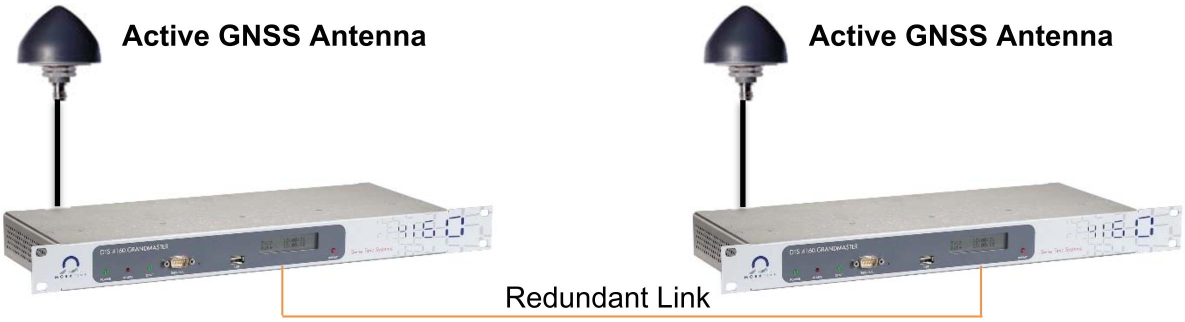
2.4 What are the standards for GNSS security

Until today there are no published standards about GNSS Security. The only publicly available description is from the US Department of Homeland Security. They have published a report “Resilient PNT Conformance Framework”, which describes different levels of GNSS security.

3 High precision time server with integrated GNSS module

Devices: DTS 4210, 4160/50

Configuration:



High Precision Time server
Synchronized by integrated GNSS receiver

High Precision Time server
Synchronized by integrated GNSS receiver

3.1 Security Features

- Multi-constellation GNSS capability
- State-of-the-art GNSS receiver module
- Redundant link and holdover capability
- Detection of the time deviation between the two devices of the redundant link configuration (alarm level configurable down to 100ns)
- Detection of time offsets (default 250ns)
- No time jumps after initial sync allowed by design

3.2 GNSS Security Level according to PNT frame work [1]

- Level 2-3 is fulfilled in redundant link configuration (Level estimated by MOBATIME)
- Jamming is covered by the holdover capability of the timeserver and the redundant link
- The spoofing detection is based on the used GNSS receiver module

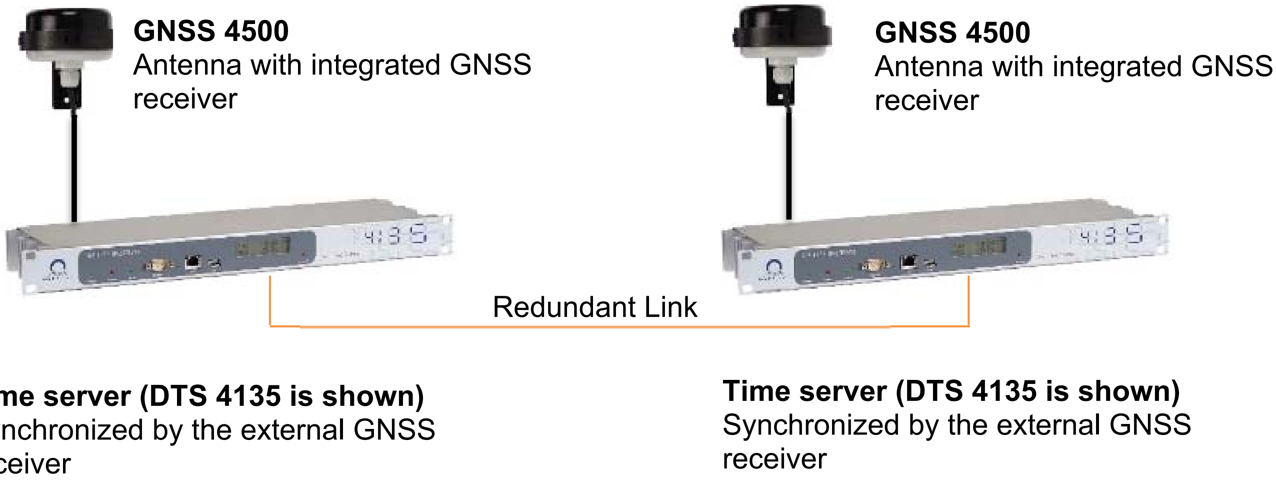
3.3 Recommendation to increase the GNSS security level

- Geographically disperse the antennas of the two devices
    - Connect one antenna over fiber to place it in a different location
- Use Anti-Jamming/spoofing Antenna
- Use a Multi-constellation configuration (default setting: GPS and GLONASS)
- Configure lowest offset error (100ns)

4 Time server with GNSS 4500

Devices: DTS 4128, 413x, 4148

Configuration:


GNSS 4500
Antenna with integrated GNSS receiver
GNSS 4500
Antenna with integrated GNSS receiver
Redundant Link
Time server (DTS 4135 is shown)
Synchronized by the external GNSS receiver
Time server (DTS 4135 is shown)
Synchronized by the external GNSS receiver

4.1 Security Features

- External Receiver GNSS 4500 with Multi-constellation capability
  Configured during production → order option
- State-of-the-art GNSS receiver module for GNSS 4500
- Redundant link and holdover capability
- Detection of the time deviation between the time sources of both device in the redundant link configuration (configurable down to 1us)
- Sync Only offset feature (minimal 100 ms)
- Maximal adjust rate of time correction is configurable

4.2 GNSS Security Level according to PNT frame work [1]

- Level 2 is fulfilled in redundant link configuration (Level estimated by MOBATIME)
- Jamming is covered by the holdover capability of the timeserver and the redundant link
- The spoofing detection is based on the used GNSS receiver module

4.3 Recommendation to increase the GNSS security level

- Geographically disperse the GNSS 4500 antennas of the two devices
- Use a Multi-constellation GNSS 4500 receiver
- Configure lowest Sync only offset (100ms)
- Configure the maximal time adjust rate to a slow correction

5 Masterclocks with GNSS 4500

Devices: DTS 480x, ETC, NTS

Configuration:

GNSS 4500
Antenna with integrated GNSS receiver

Masterclock (DTS 4806 is shown)
Synchronized by the external GNSS receiver

5.1 Security Features

- External Receiver GNSS 4500 with Multi-constellation capability
  Configured during production → order option
- State-of-the-art GNSS receiver module for GNSS 4500
- Sync Only offset feature (minimal 100 ms)

5.2 GNSS Security Level according to PNT frame work [1]

- Level 1 is fulfilled (Level estimated by MOBATIME)
- Jamming is covered by the holdover capability of the masterclock
- The spoofing detection is based on the used GNSS receiver module

5.3 Recommendation to increase the GNSS security level

- Synchronize the masterclock over NTP by a redundant timeserver with a higher level of GNSS Security
- Use a Multi-constellation GNSS 4500 receiver
- Configure lowest Sync only offset (100ms)

6 Abbreviations

GNSS	Global Navigation Satellite System This is the generic name which includes all the different satellite systems (GPS, GLONASS, Galileo and BeiDou)
TCXO	Temperature Compensated Xtal Oscillator
OCXO	Oven Controlled Xtal Oscillator
SDR	Software defined Radio
PNT	Position, Navigation and Time

7 References

[1] Homeland Security - Science and Technology, „Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework - Version 1.0," 12 2020. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/2020_12_resilient_pnt_conformance_framework.pdf.

8 Document revision

Rev.	Date	Author	Change reference
00	28.06.2021	FeM	Initial document
01	04.03.2022	FeM, TF	Minor text clarifications

Headquarters/Production

MOSER-BAER AG | Spitalstrasse 7 | CH-3454 Sumiswald
Tel. +41 34 432 46 46 | Fax +41 34 432 46 99
moserbaer@mobatime.com | www.mobatime.com

Sales Worldwide

MOSER-BAER SA EXPORT DIVISION
19 ch. du Champ-des-Filles | CH-1228 Plan-les-Ouates
Tel. +41 22 884 96 11 | Fax + 41 22 884 96 90
export@mobatime.com | www.mobatime.com

Sales Switzerland

MOBATIME AG | Stettbachstrasse 5 | CH-8600 Dübendorf
Tel. +41 44 802 75 75 | Fax +41 44 802 75 65
info-d@mobatime.ch | www.mobatime.ch

MOBATIME SA | En Budron H 20 | CH-1052 Le Mont-sur-Lausanne
Tél. +41 21 654 33 50 | Fax +41 21 654 33 69
info-f@mobatime.ch | www.mobatime.ch

Sales Germany/Austria

BÜRK MOBATIME GmbH
Postfach 3760 | D-78026 VS-Schwenningen
Steinkirchring 46 | D-78056 VS-Schwenningen
Tel. +49 7720 8535 0 | Fax +49 7720 8535 11
buerk@buerk-mobatime.de | www.buerk-mobatime.de