



GNSS SECURITY FEATURE USER MANUAL

DTS 4160.grandmaster DTS 4210.timecenter



Important Note: This Manual is applicable for Firmware version **V1.26.x** (released March 2024) and newer.

References to the Instruction Manual

- 1. The information in this Instruction Manual can be changed at any time without notice. The current version is available for download on www.mobatime.com.
- 2. The device software is continuously being optimized and supplemented with new options. For this reason, the newest software version can be obtained from the Mobatime website.
- 3. This Instruction Manual has been composed with the utmost care, in order to explain all details in respect of the operation of the product. Should you, nevertheless, have questions or discover errors in this Manual, please contact us.
- 3. We do not answer for direct or indirect damages, which could occur, when using this Manual.
- 4. Please read the instructions carefully and only start setting-up the product, after you have correctly understood all the information for the installation and operation.
- 5. The installation must only be carried out by skilled staff.
- 6. It is prohibited to reproduce, to store in a computer system or to transfer this publication in a way or another, even part of it. The copyright remains with all the rights with BÜRK MOBATIME GmbH, D-78026 VS-Schwenningen and MOSER-BAER AG CH 3454 Sumiswald / SWITZERLAND.

Table of contents

1 General Information: Introduction	4
1.1 License model1.2 Requirements	4
1.2.1 Firmware 1.2.2 Hardware	4 4
1.2.3 MOBA-NMS 1.3 Introduction	4 5
1.3.1 Disturbance of GNSS signals - Fundamentals 1.3.2 Jamming 1.3.3 Spoofing	5 6 7
1.4 General Methodology 1.5 Mobatime Implementation	8
1.6 Supported device types for the GNSS security feature	9
 Configuration 2.1 Activation of GNSS Security system – Step by step 	10 10
2.2 Import license 2.3 GNSS Security system parameters in MOBA-NMS	11 12
2.4 Check GNSS security status	14
A lechnical data	15

1 General Information: Introduction

1.1 License model

The GNSS security system needs a license installed on the DTS Grandmaster.

Requirements / description:

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.

Please contact MOBATIME sales to order a license: export@mobatime.com

1.2 Requirements

1.2.1 Firmware

To be able to activate the GNSS security system, you need the DTS firmware version **V1.26.x** or higher.

1.2.2 Hardware

Min. required hardware revisions: DTS 4210: 121059.11 DTS 4160c: 122033.08 (with option E1) DTS 4160c: 137888.00 (standard)

1.2.3 MOBA-NMS

MOBA-NMS Version 2.12.x or higher.

1.3.1 Disturbance of GNSS signals - Fundamentals

GNSS are complex systems -> multiple error sources are possible.

Received signals are relatively week:

- Power is like a 100W light bulb in 20'000km distance
- GNSS frequency bands are dominated by white noise

GPS signal design dates to 70/80s

- Design of civil signals is publicly known
- At the time of design, intentional interference was not considered.

Common unintentional interference

Out-of-band-emissions (unwanted, uncertified):

- Wi-Fi Cameras
- Power supplies
- Cheap consumer electronics

Harmonics within the GNSS frequency bands:

- Mis-tuned RF equipment

Near-far effect and insufficient filtering:

- Any other RF components close to the GNSS antenna

In this document, the term interference is limited to jamming and spoofing.

1.3.2 Jamming

What is Jamming?

Jamming refers to the transmission of interfering signals with the aim of degrading the GNSS measurement quality or denying GNSS services.

This means, emitting of 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.



Who is able to perform Jamming?

- GNSS jamming is illegal in most countries
- The equipment is simple and available for a low budget.
- Almost no knowledge is needed
- Due to the low signal level of GNSS a jamming attack can disable reception over a large area.
- Jamming is also possible through unintentional installations, see chapter 1.3.1.

1.3.3 Spoofing

What is Spoofing?

Spoofing is the transmission of false GNSS signals with the aim of deliberately falsifying GNSS-based time measurement.

This means, 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.



Who is able to perform Spoofing?

There are many different levels of attacks to consider:

- With modern and cheap devices and an antenna, a simple spoofing attack can be performed. Almost no knowledge is needed.
 But this kind of attack can be detected from the GNSS modules (time jump or too high signal level) 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, or using a special GNSS security system offered with this feature.

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.

1.5 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.



1.6 Supported device types for the GNSS security feature

	Model		Oscillator type	Holdover	Product no.
	DTS 4210.timed	center	Rubidium	G811	125600
Туре	Model	Oscillator type	Compatibility according to oscillator	Options	Product no.
С	DTS 4160c.	Rubidium	G811	Standard (without E1) With option E1	137888 122033

2 Configuration

2.1 Activation of GNSS Security system – Step by step

- Connect GNSS antenna to the grandmaster device. Time source GNSS must be configured. Select "Constellation Mode" e.g. GPS & Galileo & Beidou
- 2. Leave GNSS security mode to "off"
- Wait until the device is properly synchronized (no alarm and synch LED = on) (this takes approx.. 20 Min.)
- 4. Wait another 30 minutes until the GNSS module is showing stable position data from the antenna position.

Take a screenshot of the GNSS time source details in "Overview" Tab:

MMS	×
GNSS Details	
Receiver internal time state:	Time OK
Number of used satellites:	28
Dilution of precision of time:	0.42
Internal receiver time accuracy:	24 ns
Fix type:	3D-fix
Position latitude:	47.0291189 N
Position longitude:	7.7451095 E
Height above sea:	717.913 m
Height above ellipsoid:	765.179 m
Antenna cable delay:	0 ns
State of next leap second:	No leap second detected
Date of next leap second:	No info
Direction of next leap second:	No info
	Close

- 5. Go back to "Time handling" Tab and set GNSS Security values (steps 7 to 9)
- 6. Set GNSS Security Mode to "on" (do not press "Save" button until step 10)
- 7. Import GNSS security license file, see chapter 2.2.
- 8. Select "Antenna type"
- Set "Position Mode" to "Manually" and enter the antenna position data (values from screenshot or exact position data from a map). See chapter 2.3.
- 10. Press "Save" button to store the configuration.

Important: The GNSS module will now restart and this could release temporarily warnings or alarms.

11. Check GNSS security status, see chapter 2.4.

2.2 Import license

The licence file can be imported via MOBA-NMS only (Version 2.12.x or higher):

1) Open the device view and click on the Tab "Time handling".

iority 1: GNSS	Alarm delay for failure of source [min]: 1
iority 2: None	Stratum (0=auto, 1-15=fix): 0
iority 3: None	Stratum limit for synchalarm: 12
iority 4: None	Stratum timeout (1-16) source fail [h]: 999
iority 5: None	Stratum change when source fails: Default
arity for None	Max. offset for time ok [ns]: 250
None	Time adjustment settings
ority mode: Manually	Adjust mode: Follow (Adjust slowly)
ASS settings Red. link settings PTP settings GNSS-DCF setti	gs E1 settings NTP settings Max. catch-up speed [ns/s]: 5
General	Synch.only offset
Min. required satellites 5	PTC mode: Off
Min. required signal level (dBHz) 20	Alexe Bis Offset
Constellation Mode: GPS & Galileo & Beidou	V Alam big Onset: 355
Alarm max. Offset: 200	Leap second / Manual time adjustment
GNSS Security	Leap second mode: None
Security Mode: On	Leap second date:
Security suite licence:	Set time (UTC): 04.04.2024
Antenna type: PCTel GPSGL	Adjust time [ns]: 0
Source drop on Al. Sec. Warning: off	
Position Mode: Manually	
Latitude in degrees South: 47.020125	
Longitude in degrees -= Fast: 7.745125	
Height above ellipsoid in m: 771.0	
	▼.

2) Click on the blue "Import" link to select the license file from a folder on your PC:

NMS Öffnen					×
← → ~ ↑ 📙 « 09	Manual working folder > DTS 4160	> GNSS_License_mobil	atime_10458530003 v 🖱	GNSS_License_n	nobatime_104 🔎
Organisieren 👻 Neuer	Ordner				H • 🔳 🕐
- Cohnallauguiff	^ Name	^	Änderungsdatum	Тур	Größe
Desktop	* license.	ic	04.04.2024 09:17	LIC-Datei	1 KB
Downloads	*				
😫 Dokumente	*				

Once the license is successfully activated, the other parameters in the frame "GNSS Security" can be selected and configured.

2.3 GNSS Security system parameters in MOBA-NMS

The configuration parameters are located in the NMS Tab "Time Handling". The GNSS Security can be used only with time source "GNSS".

GNSS Security		
Security Mode:	On	~
Security suite licence:	Import	
Antenna type:	PCTel GPSGL	~
Source drop on Al. Sec. Warning:	off	~
Position Mode:	Manually	~
Latitude in degrees, -= South:	47.029125	•
Longitude in degrees, -=East:	7.745125	•
Height above ellipsoid in m:	771.0	•

Path: Time Handling – GNSS settings

The frame "GNSS Security" show the configuration parameter:

Switch on or off the GNSS security:

Security Mode:	on / off
Security suite license:	click on "Import" to select the license file
Antenna type:	default: PCTel PCTel GPSGL Tallysman 3742
Source drop on Al. Sec. W	 /arning: off (default, recommended) Security warnings are only reported in the Alarm History on: each warning releases an alarm in the device
Position Mode:	Manually (default) The position of the antenna needs to be entered manually. Auto (future option)

Important: After first commissioning of the device, wait until the GNSS synchronization is completed and the device is properly synchronized. This usually takes approx. 20 minutes. After this time, wait another approx. 30 minutes. Then select the "Overview" Tab and GNSS Source "Details", see next page. There you find the exact position data of the antenna. Enter this values in the position fields below. Find antenna position data:

GNSS Source GNSS OK, can be used as time source. Details	1
GNSS Security Suite enabled Details	
NTP state	
Show NTP status details	

Overview Network Overview Outputs Time handling Alarms PTP configu

NMS	×
GNSS Details	
Receiver internal time state:	Time OK
Number of used satellites:	28
Dilution of precision of time:	0.42
Internal receiver time accuracy:	24 ns
Fix type:	3D-fix
Position latitude:	47.0291189 N
Position longitude:	7.7451095 E
Height above sea:	717.913 m
Height above ellipsoid:	765.179 m
Antenna cable delay:	0 ns
State of next leap second:	No leap second detected
Date of next leap second:	No info
Direction of next leap second:	No info
	Close

Latitude in degrees:	Position latitude from antenna position + Value = N - Value = S
Longitude in degrees:	Position latitude from antenna position + Value = W - Value = E
Hight above ellipsoid in m:	Height above ellipsoid from antenna position

2.4 Check GNSS security status

MOBA-NMS: Tab: Time handling - Frame: GNSS Source

Click on GNSS Security Suite enables -> Details



Overview Network Overview Outputs Time handling Alarms PTP configu

GNSS security status:

MMS	×	
GNSS Security Suite Details		
Common		
Licence state:	valid	
Detect state:	HEALTHY	
Jamming severity:	0.00%	
Spoofing severity:	0.00%	
Detectors		
Carrier-to-Noise Density Ratio:	HEALTHY	
Clock	HEALTHY	
Doppler:	HEALTHY	
Pseudorange:	HEALTHY	
Position, Velocity and Time:	HEALTHY	
Power Spectral Density:	HEALTHY	
Geofence:	HEALTHY	
RF Monitor:	HEALTHY	
Spoofing state:	HEALTHY	
CI	ose	

A Technical data

Further technical specifications can be requested from MOBATIME.



Headquarters/Production Sales Worldwide	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 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	