LEVEL-3 CYBER-PROTECTION

GNSS Guard

Anti-jamming/spoofing - isolates NTS-5000 from physical GNSS

- Identifies and protects GNSS spoofing & jamming
- GNSS multipath mitigation and anti-RF-meaconing*
- Isolates IT infrastructure from GNSS threats
- Identifies and protects GNSS Time Sync Attack
- Active Filter LEVEL-2* for GPS L1 anti-jamming
- GNSS simulation output to NTS-5000 ANT inputs
- Ref. Time Backup from:
  >Qualified Time via cloud
  >1PPS/10MHz local clocks
- Long distance distributed 2x ANT for ”geographical” anti-jamming/spoofing
- Constant position tracing to prevent manipulations
- 1U holdover OCXO (std.)
  2U holdover Rubidium*

ELPROMA

www.elpromatime.com

* extra feature requiring additional hardware

The “GNSS Guard”, similarly to a network firewall operation, solves the problem of protecting existing IT/OT systems by providing separation between physical GNSS and the NTP/IEEE1588 Time Server. It protects any class ELPROMA time server incl. NTS-5000 and NTS-4000. The “GNSS Guard” protects any critical infrastructure (incl. banks, stock exchange, air traffic control, railways, power stations, telecom, finance) from untrusted sky based physical GNSS satellite signals. It is a software engine that analyses timing from each selected GNSS subsystem: GPS, GALILEO, GLONASS, BEIDOU, IRNSS separately by providing simulated GNSS output that is level 100% information compatible to GPS L1. The GNSS Guard appliance is equipped with special timing analysis. It can optionally be equipped with GPS L1 anti-jamming active filter (null steering technology, protecting against amateur mobile GPS L1 jammers. Together with other algorithms it protects timeserver inputs from GNSS jamming and/or spoofing. Operation bases on checking several conditions, including disrupting criteria, such as: number of GNSS satellites, mismatching the GNSS antenna location, phase / time deviation, RF intensity / signal strength, SNR levels of GNSS signals. The LOG data can be optionally stored inside or exported to external SCADA/NMS/OSS class external software. GNSS Guard works via MIB-2 traps with all leading OSS class software. In addition, the ref. UTC time can be delivered to input LAN interface of SafeTime Guard from remote time backup center. Product accepts cryptographically authenticated NTP and/or PTP IEEE15) protocols. This is right approach to get your backup ref. time via Internet or cloud from National Institutes Of Metrology (NMI), such as: US NIST, UK NPL, Polish GUM, Italian INRIM etc. In case of network failures /links(-)/or during cyber-attacks (DDoS attacks, TDA -Time Delay Attack) device switches automatically to OCXO/Rubidium* holdover mode. The device sync accuracy is better than 1us.

Technical Specification

Synchronization Inputs

- GNSS (GPS, GLONASS, Galileo, Beidou support)
- 2x LAN (authenticated remote time backup)
- IRIG-B (local clock)

Synchronization Outputs

- Simulated GNSS (equivalent for real-time GPS L1)
- NTP / PTP IEEE1588 time to remote backup centre)

Synchronization Holdover

- OCXO (1U)
- Rubidium (2U)

Rubidium holdover accuracy degradation on each next day

Days	1d	2d	3d	4d	5d	6d	7d	14d
ERROR µs	0,5	1,2	1,8	2,4	2,9	3,3	3,7	3,9

OCXO holdover time accuracy degradation on each next day

Days	1d	2d	3d	4d	5d	6d	7d	14d
ERROR µs	0,6	2,8	7,2	13,7	22,1	32,9	45,9	184

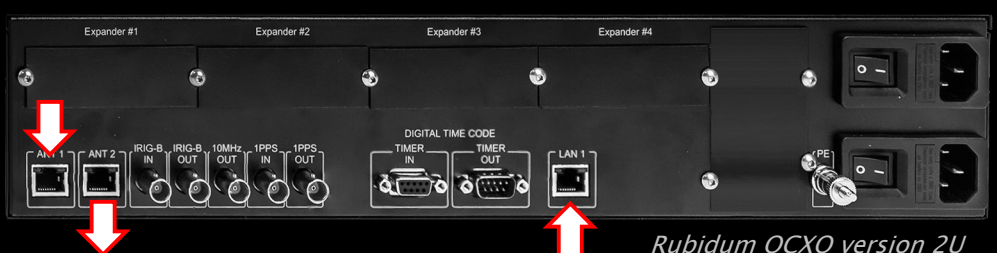
GNSS or LEVEL-2 Security

GNSS simulated output

LAN

OCXO version 1U

Remote Time Backup



Rubidum OCXO version 2U

I/O

- 3x rs232 (PPS/ToD)
- 5x BNC (50 Ohm: PPS, IRIG, 10MHz)
- 2x USB 2.0 (for firmware upload)

Mechanical/Env.

- Size: 484x 300x 44,4 mm
- Storage temp: -55°C to +80°C
- Operating temp: 0°C to +60°C

Redundant Power Supply

- Power: 110-230 VAC (1A), 50-60Hz 120-370 VDC (1A)
- Telecom: 48VDC option* 20-70 VDC

Management

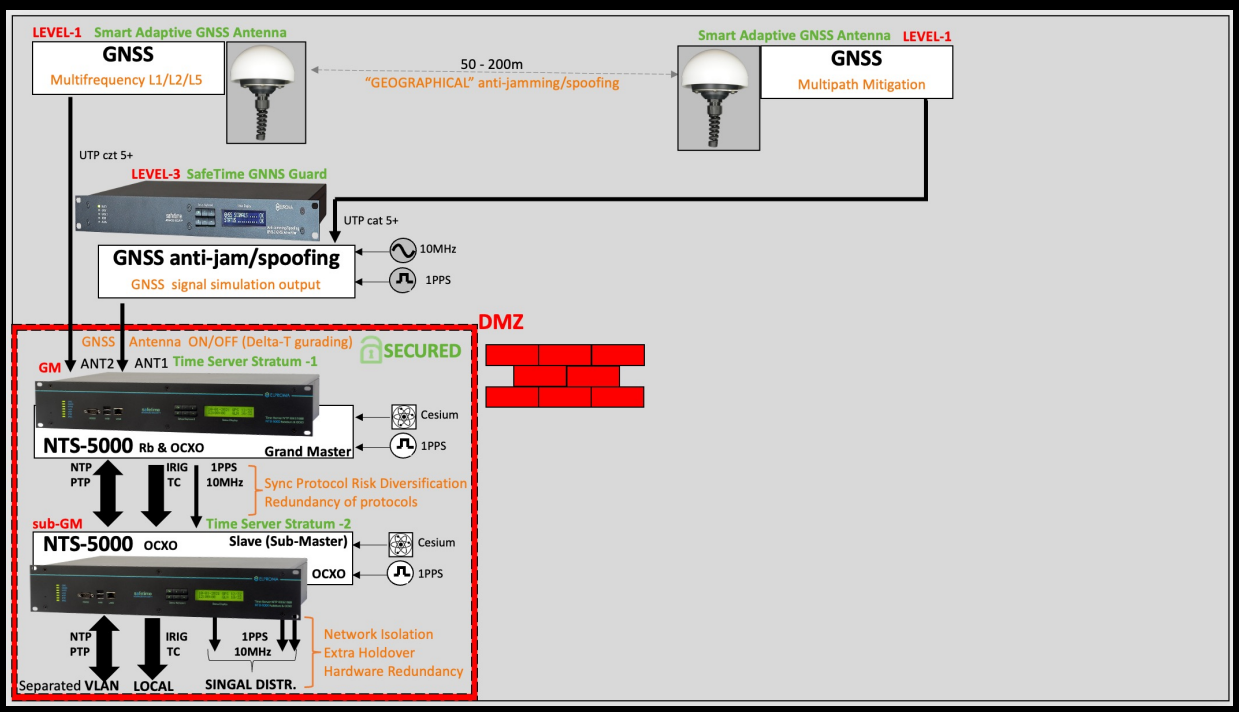
- SNMP v3/v2 MIB-2
- RADIUS
- HTTPS
- SSH
- Disabled HTTP, Telnet

* extra feature requiring additional hardware

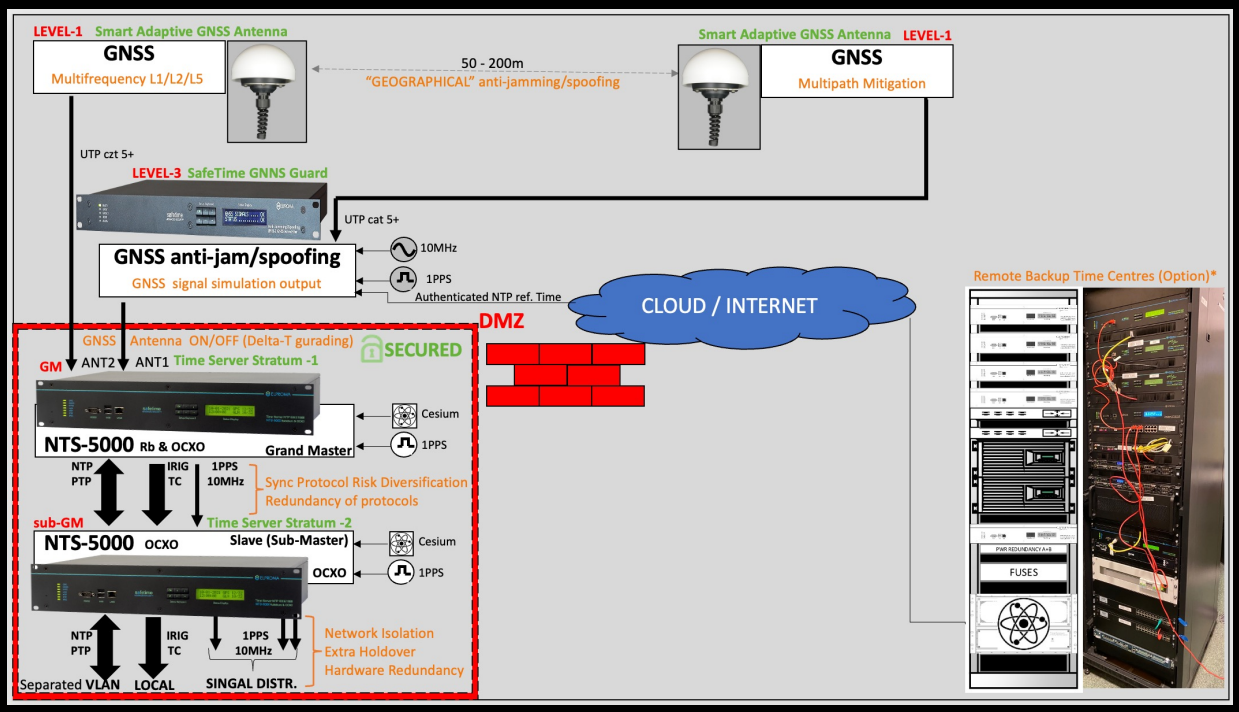
ELPROMA
www.elpromatime.com

Application Notes – Security for Anti-jamming/spoofing GNSS

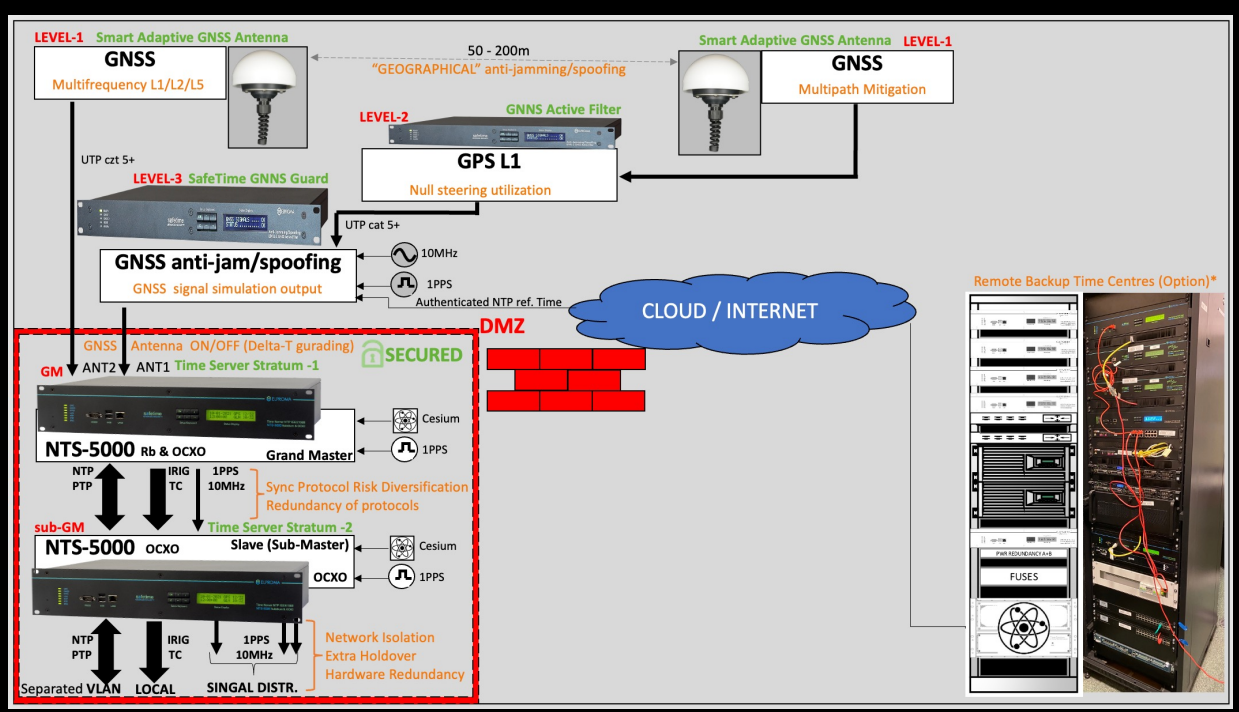
1) Basic Configuration. Use LEVEL-3 and independently 2x GNSS w/ min 200m distance between antenna



2) Mid Security. Use additional remote TIME BACKUP center and/or local holdover backup (atomic) clocks



3) Top Security. Use additional LEVEL-2 (Null Steering) GPS L1Active Filters with previous configuration



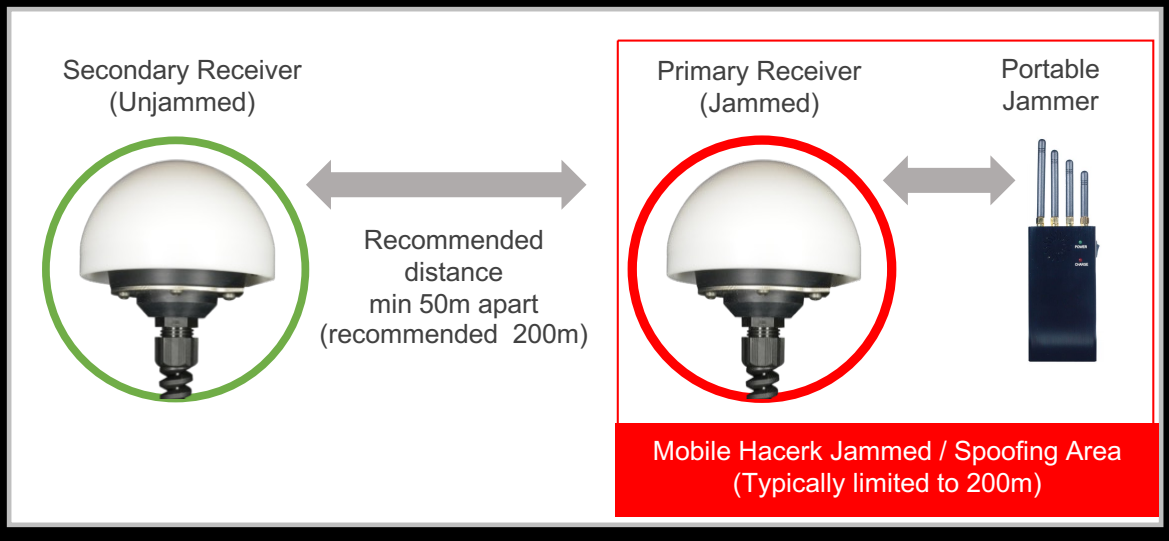
Application Notes – Security for Anti-jamming/spoofing GNSS

Protection of the input clock source has become increasingly important. Elproma offers 3 LEVELS of cyber-security protection to for NTS-5000, NTS-4000 and NTS-3000.

- **LEVEL-1** 2x Smart-Antenna w/ GNSS receiver supporting RF-attack alarms
- **LEVEL-2** Active Filtering GPS L1 , the additional to LEVEL-1 null steering filtering
- **LEVEL-3** GNSS simulation, providing additional separation from physical GNSS signals

Each single level of protection can be used separately or together with others levels.

The LEVEL-1 protection is built-in to standard NTS-5000 (also NTS-4000) network appliance. It has support for each GNSS receiver (ANT1, ANT2 inputs) with auto antenna ON/OFF switching when RF jamming or GNSS spoofing is recognised. It lets server switch early enough to oscillator (Rubidium, OCXO) holdover mode refusing false signals. The NTS-5000 will then still ensure the accuracy of 200ns (nanoseconds) for another 15 hours of GNSS less operation (the ANT1/ANT2 antenna is OFF or STAND-BY mode) when equipped with Rubidium & OCXO oscillators, and 4 hours only when NTS-5000 is equipped with OCXO oscillator only (no Rubidium). Longer holdovers increases the oscillator drift ensuring less accuracy of synchronisation on next days. Once the RF jamming/spoofing attack ends the NTS-5000 time switches back to normal operation synchronizing from GNSS. The LEVEL-1 protection can be extra amplified by using simultaneously 2x GNSS receivers located min. 50m (optimally if more than 200m) from each other. This is "Geographical" anti-jamming/spoofing approach perhaps the most effective one to prevent against
mobile jammers and Hack-RF GPS spoofers. If the primary antenna is jammed, the secondary antenna (outside the jammed area) can take over to provide GNSS signal to NTS-5000. Independently NTS-5000 senses RF-interferences switching-OFF jammed antenna and continuing with 2nd antenna or switching to GNSS-less holdover. The LEVEL-2 protection is boosting LEVEL-1 by additional null steering GPS L1 active filtering. It automatically recognizes and eliminates false GPS L1 signals send from ground or air, but not



Tips and recommendations (what they do not teach you at school)

- If possible always use 2x GNSS Smart Antenna at least to ensure hardware redundancy;
- Use redundancy on smart way – ask your supplier to provide both Smart Antennas with a different vendor GNSS receivers inside. In other words - do not use the same type of GNSS receivers for both r Smart Antennas. In case of security threat both antenna will be automatically affected. Especially GNSS spoofing attack will easily affect both the same GNSS receivers. This is because GNSS spoofing requires a proper strategy to hack into the GNSS receiver and using different GNSS receivers you are much safer;
- Use natural "GEOGRAPHICAL" anti-jamming/spoofing by locating both Smart Antennas on a min. distance of 200m from each other. More of mobile GNSS jammers and RF-hacker spoofers have limited range of effective disruption distance do max. 200m. Locating 2x Smart Antennas in a distance of min 50m already reduces probability both will be affected by mobile jamming/spoofing.

Recommendation for USA/EU critical infrastructures:

- The GNSS receivers should be configured exclusively for GPS-alone, GALILEO-alone, GPS+GALILEO pair only…
- GNSS constellations like the Russian GLONASS or Chinas BEIDOU can be considered for time monitoring only …
- Follow the US President Directive EU13905 to stay synchronize to emanative remote time backup centres (NIST, EURAMET etc.)…

Recommendation for other regions:

- Always try to make your GNSS configuration suitable for current geopolitical situation in the region…
- Try to consider the GNSS receivers that supports multipath-mitigation, null steering anti-jamming GNSS techniques…

- Separate NTS-5000/NTS-4000 time server form physical GNSS signals using GNSS Guard (this brochure product). It is the equivalent of network firewall appliance, but dedicated for separation from physical GNSS signals.
  The GNSS Guard is a satellite GPS L1 C/A code simulator operating on electric signal level.
- The GNSS guard protection enables functionality to get ref. time from remote Time Backup Center or NMI using TCP/IP. Above is the only protection for strong (>150dB) military RF-jamming attack.

- Consider to order extra protection functions for NTS-5000 that switches OFF the antenna when RF- interference is recognised;
- The customised NTS-5000?NTS-4000 is able to work all the time in holdover mode of oscillator switching ON "from time to time" to get synchronised to GNSS