AT THE SERVICE OF TIME - IN DEFENSE OF PEACE

NATO NCAGE No 9ATKH
NSN 6645-17-125631

NTS-5000 Rb ocxo

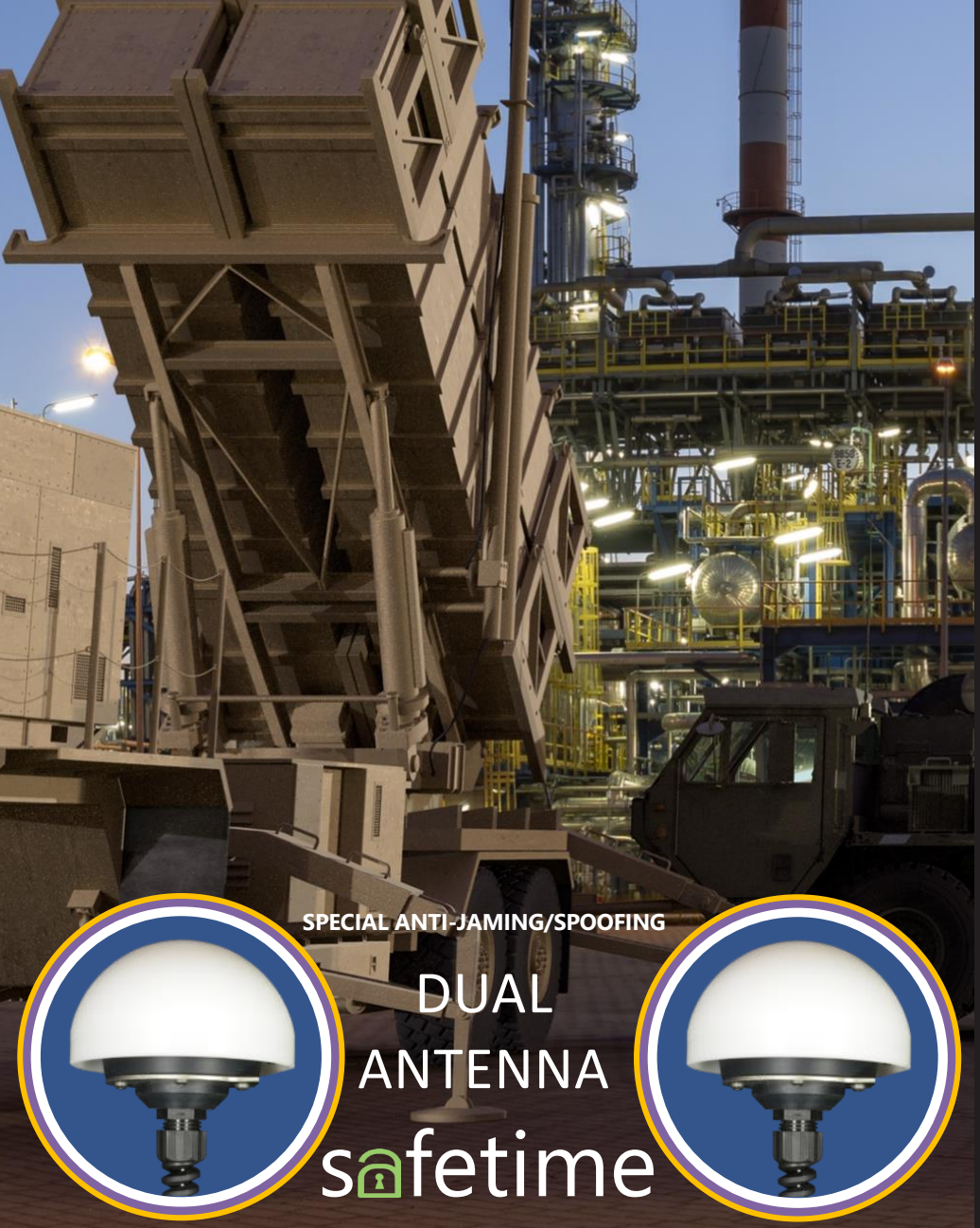
NTP/PTP IEEE1588 Modular Time Server

- IEEE1588 Grandmaster/Slave
- NTP STRATUM-1 Timeserver
- IRIG-B STANAG4430* NASA36*
- Redundant hardware
- Strong cybersecurity isolation
- UTC/ZULU time management

- GNSS anti-jamming*/spoofing*
- RF attack auto ON/OFF antenna
- GNSS 2x inputs (ANT1 ANT2)
- GPS/GALILEO/GLONASS/BEIDO

- Built-in OSC Rubidium & OCXO
- Extra long holdover w/o GNSS
- EURAMET audited & approved
- ITU-T G.8272 PRTC compliant
- Direct serial ToD from 5071A

- 10x LAN 10GbE/1GbE/100M
- PTP, SyncE, NTP, IRIG, DCF77
- 10,000 NTP msg/s @1GbE
- 128 PTP msg/s @1GbE
- 1000 IEEE1588 clients
- SNMP v2/v3 MIB-2 RADIUS
- I/O 1PPS 10MHz 2.048Mbps



SPECIAL ANTI-JAMING/SPOOFING

DUAL ANTENNA

safetime

ELPROMA

* extra feature requiring additional hardware and firmware upgrade

Technical specification

GNSS Input Options

- Dual redundant GNSS input (ANT1/ANT2)
- GPS, GLONASS, Galileo, Beidou support

Inputs

- 2 × 1PPS — standard
- 2 × ToD — standard
- 1 × IRIG-B AM — standard
- 1 × DCLS FO — option
- 1 × Direct Cs atomic 5071A time-scale UTC interface — option

Outputs

- 2× 1GbE output SFP /Expander slots 1-4/ — option
  HW/stamps supporting PTP, NTP, and SyncE
- 10× 1GbE output SFP /Expansion board 1/ — option
  SW/stamps supporting PTP, NTP
- 2 × 10GbE SFP — option
- 2 × 100/10Mbps RJ4 — standard
  HW/stamps supporting PTP, NTP, and SyncE
- 1 × E1 (2.048 Mbps /2.048 MHz) unframed — option
- 1 × 1PPS — standard
- 1 × 10MHz — standard
- 1 × IRIG-B AM — standard
- 1 × ToD (rs232) — standard
- 2 × IRIG AM or TTL (selectable) — option
- 2 × IRIG DCLS FO — option
- 4 × IRIG DCLS (rs422) — option
- 2 × GNSS simulation (GPS L1 NMEA183) — option

Client Capacity

- PTP IEEE1588 up to 1000 clients/port
- PTP IEEE1588 up to 128 msg/s
- NTP up to 100,000 clients (default polling)
- NTP up to 10mln clients (1024s polling)
- NTP up to 10,000 clients/s (port)

NTP Server

- Stratum 1 server through GNSS and/or atomic clocks
- Stratum 2 server when synchronised to remote Stratum 1

PTP IEEE1588:2008

- Grandmaster, Sub-Master, Slave
- 25ns accuracy Grandmaster-2-Salve HW/stamping

PTP IEEE1588 Profiles via 2x LAN 1GbE Expanders 1-4

- Default
- Telecom ITU-T G.8275.1 G.8275.2 G.8265.1
- Power & Utility IEEE C.37.238 v1 v2
- gPTP*, TSN* 802.1AS*,
- Broadcast* AES67*, SMPTE 2059.2*

SyncE (Expander 1-4 only)

- SyncE ITU-ITG.8261

Other SW/HW License Options

- Direct Cs atomic clock 5071 synchronisation to UTC/TAI
- Expander 1-4 PTP-slave licence (32, 64, 128, 256 users)
- Expander 3-5 IRIG*, AFNAR*, STANAG4430*, NASA36*
  (contact ELPROMA for more Time Codes)

Power Requirements

- 110–230VAC/20-70VDC/120-370VDC (dual redundant)
- 2A(DC) / 1A(AC) max. 80W (typical 60W)

Hardware Modules

- Expander 1-4 (2 × LAN, 4x IRIG I/O ports) — option
- Expansion (10 × LAN, 4x IRIG I/O ports) — option
- OCXO module NTS-5000LITE & NTS-5000 — standard
- Rubidium module (only NTS-5000) — standard

Time Stamp Precision

- <5 ns RMS typical — standard

Frequency Accuracy

- Tracking to GPS: PRS/PRC/PRTC compliant. — standard
- Rubidium (G.812 type II) <1 × 10^{-11}/day — standard
- OCXO (G.812 type I) <1 × 10^{-10}/day — standard

Time Accuracy

- Tracking to GPS (1PPS): <20 ns

Holdover Performance

- Accuracy <200ns for 15 hours (Rubidium)
- Accuracy <200ns for 4 hours (OCXO)

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

Management

- IPv4 or IPv6 (MIB-2 compatible to any OSS/BSS)
- SNMP v2c, v3 with large database of MIB-2 traps
- Elproma NMS STAS (purchased separately)

Industry Standards/Requirements

- ITU G.811, G.812, G.823, G.8261, G.8272 G.703, G.704

Protocols

- IEEE 1588-2008 (PTP Precision Time Protocol))
- NTPv4, NTPv3
- IPv4 / IPv6 optional
- DHCP
- SFTP,
- VLAN (1x PTP-slave, 9x PTP-master, 10x NTP)
- TELNET
- SYSLOG
- RADIUS
- SSH

Certifications

- NATO NCAGE (9ATKH)
- NATO system registered product NSN 6645-17-1256311
- CE
- ISO 9001
- EMC
- Safety Directive

Physical Specifications

- Dimensions: 88,8 mm (H) × 484 mm (W) × 300 mm (D)
- Weight: 6.1 kg

Environmental Specifications

- Operating temperature: –5°C to +60°C
- Storage temperature: –55°C to +80°C
- Humidity: 5% to100% with condensation
- MTBF 391000 hours

safetime
#1 in ANTI-JAMMING/SPOOFING

The NTS-5000 is a carrier-grade Grandmaster clock with additional capabilities of cyber-security that provide a flexible technology suite to match the synchronization needs of evolving IPv4 and IPv6 networks. The server enables communications service providers to build a robust, stable and reliable distributed network infrastructure ensured by multi-protocol use: IEEE1588, NTP, SyncE, IRIG-B, 1PPS, 10MHz... etc.

Redundancy built-in from scratch

The hardware redundancy is built-in from scratch to each level of the architecture of the NTS-5000 time server. Dual GNSS receivers (ANT1, ANT2), dual holdover oscillators (Rubidium, OCXO), and multiport LAN network interface expansion modules - all ensure no impact on client synchronisation performance when failover occurs. Separating clients provides the best cyber-security protection, far superior to network redundancy models where random traffic pushes to reacquire synchronisation from a different grandmaster somewhere else in the network.

PTP/NTP/SyncE* simultaneous support per each LAN

#1 performance, stability, security, Private FPGA & IP-stack per NIC

When locked to a GNSS input, the NTS-5000 meets the applicable performance requirements of the ITU-T G.8272 standard for a primary reference time clock PRTC. Optionally equipped with a special 2x 10MHz input module it meets ePRTC class 5G and 6G telecom. With hardware-based PHY timestamping (Expanders 1-4) and special PDV packet processing, the NTS-5000 delivers high client capacity at total rates of up to 128 messages per second with performance that does not degrade as the number of clients increases. The NTS-5000 supports IEEE1588, SyncE and NTP operating simultaneously. The NTP capacity at 10GbE is up to 120,000 transactions/s, and the PTP capacity remains at up to 1000 clients. As the initial unit in a "rack and stack" configuration, the server arrives with 2x LAN 100Mbps, possibly extending up to 10x 1GbE/10GbE* or with various other synchronisation interfaces, incl. IRIG-B DCLS.

Protection of the input clock source has become increasingly important, The NTS-5000 has three independent LEVELS of GNSS cyber-protection

LEVEL-1 GNSS anti-jamming (Free)

The first (LEVEL-1) protection is standard for NTS-5000. It supports auto antenna ON/OFF switching when RF interference, including GNSS jamming attack. The LEVEL-1 protection lets NTS-5000 refuse GNSS signals and change early enough to Rubidium/OCXO holdover operation. The NTS-5000 will still ensure the accuracy of 200 ns for another 15 hours of GNSS-less operation (the ANT1/ANT2 antenna is OFF in STAND-BY power mode) when equipped with a Rubidium oscillator and 4 hours only when provided with OCXO. Longer holdovers increase the oscillator drift, ensuring less accuracy of synchronisation output on the following days (below data presents max. time error officially confirmed by independent EURAMET auditor measurements).

Best accuracy at very long holdover

Rubidium (Rb) 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

LEVEL-2 active jamming filters LEVEL-3 simulator isolates from GPS

The NTS-5000 may also respond at LEVEL-1 to random interferences. Therefore, Elproma offers LEVEL-2 active jamming filtering protection and LEVEL-3 - the GNSS signal simulation for NTS-5000. Using all three levels of protection simultaneously ensures no risk for Time Synchronisation Attacks incl. GNSS jamming and spoofing. Once the RF jamming/spoofing attack ends, the NTS-5000 switches back to regular operation synchronizing from GNSS.

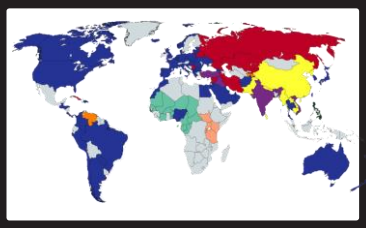
ELPROMA
www.elpromatime.com

safetime
#1 in ANTI-JAMMING/SPOOFING

US President Directive EO13905 protecting time at critical infrastructures

Centralised UTC Time Systems replaces old distributed antennas

GPS, GLONASS, BEIDOU are military
GALILEO is the only civil sub-system



The vulnerability of GNSS, especially of the GPS, to various signal incidents, is well documented today (for more information, please type in the Google search phrase "Time Synchronisation Attack"). The rapid proliferation of GNSS systems has embedded these vulnerabilities into critical national infrastructures that rely on GNSS for daily operations. This widespread deployment of GNSS receivers makes it impractical to replace all fielded GNSS systems in a timely or cost-effective manner. The new approach, much easier to maintain, use centralized UTC systems that protect against all synchronization vulnerabilities. Time systems consist of many grouped NTS-5000 servers creating an autonomous, corporate UTC timescale (GNSS-independent). The comparative source of time is still GNSS, but the essence of ensuring cybersecurity is the certainty to which of the individual GPS, GALILEO, GLONASS or BEIDO systems it synchronizes. Time is not universal, and all GNSS sub-systems use their different UTC(k). Ensuring what satellites you use is the essence of a new cyber-security paradigm.

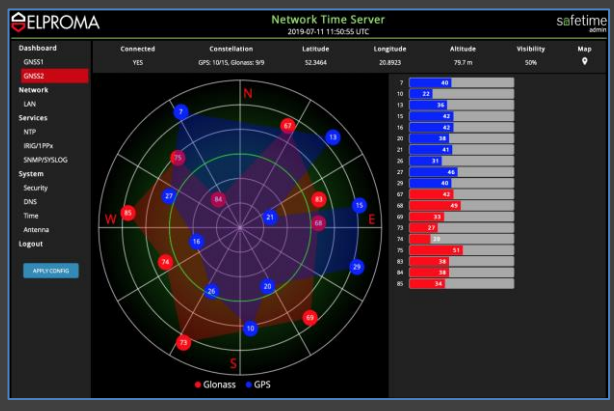
The US Presidential Directive no. EO13905 recommends ”zero trust” for any GNSS subsystem including GPS, GLONASS, GALILEO, BEIDOU, IRNSS when considering the synchronisation of US critical infrastructures

Instead, it recommends using many independent, trusted UTC references, including remote backup time systems from NIST - delivering ref. UTC independently on GNSS using authenticated time dissemination via Ethernet with IEEE1588 and NTP protocols.

It would be best to ensure what GNSS subsystem you are using.

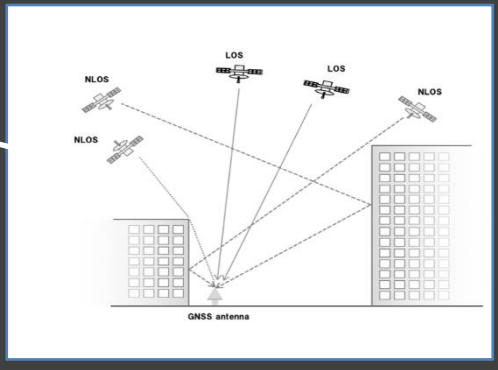
GNSS satellite traceability

NTS-5000 has built-in advanced GNSS satellite traceability SNMP external software supporting MIB-2. It is compatible with any OSS software. Our MIB-2 file defines one of the world's most significant event traps (alarms) databases, including GNSS jamming and spoofing recognition.



Link: Watch on Youtube

FURUNO advanced technology helps receive reflected SAT signals



Optionally, customers can request a particular GNSS cyber-security receiver version made by Furuno, who has developed a new unique technology to enhance the reception of GNSS signals. This unique functionality enables correct timing signals to be computed even when antennas are mounted in a lower part of the canyon, where GNSS signals are reflected, diffracted, jammed or spoofed.

safetime
#1 in ANTI-JAMING/SPOOFING

The GNSS smart-antenna with replaceable receivers

Elproma has developed special NTS-Smart-Antenna in which the replaceable GNSS receiver board is built into the Smart Antenna dome (instead of the usual approach of placing the receiver inside the server enclosure). Only 1pcs. Smart Antenna is included in NTS-5000 and the 2nd needs to be purchased separately.

Different replaceable GPS receivers improve IT stability & cyber-security

Link: LEVEL-1 smart-antenna

Link: Watch on Youtube

- single band L1 or L5
- dual (L1+L5 or L1+L2)
- triple L1 + L2 + L5

up to 700m to NTS-5000 (UTP cat. 5+)

Easy GNSS receiver replacement enables customized cybersecurity. It also ensures correct industry profile settings suitable for a region's current "geopolitical" situation. Protection of the input time from GNSS source has become increasingly important today, and therefore, it requires flexibility in changing to GNSS trusted receivers.

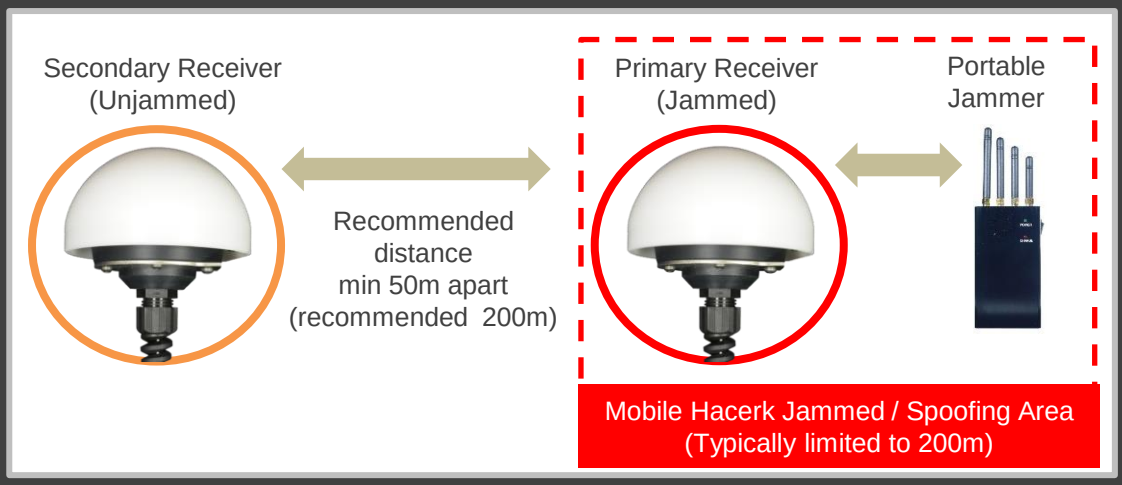
"Geographical" >50 m distance to protect from GPS jamming/spoofing

Check more GPS firewall products for GNSS anti-jamming/spoofing

Link: LEVEL-2 active anti-jamming filter

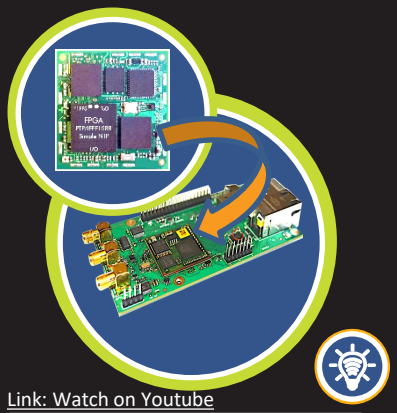
Link: LEVEL-3 SafeTime GNSS guard

The NTS-5000 comes with dual GNSS antenna physical ports ANT1 and ANT2. At the first (LEVEL-1) antenna protection, when 2 x Smart Antenna is at least 50 m apart, the physical distance deters the risk of mobile jammers, as the signal interference is typically limited to max. 200m. Therefore, if the primary antenna is jammed, the secondary antenna (which stays outside the jammed area) can take over to provide a 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 highest level of cybersecurity is always offered by those IT systems that use unique proprietary, irregularly changed (dynamic) security strategies. Optionally the NTS-5000 can use custom defined security pseudo-randomness algorithms. The operating concept assumes that once the server is readily synchronized initially to GNSS, it still mainly stays in GNSS-less holdover mode (as long as it can) and only periodically synchronizes its Rubidium + OCXO oscillators to GNSS. The server checks passive mode the condition of UTC offset between GNSS and OSC, and unless it detects UTC offset more than the predefined DELTA-T, it will periodically turn on the synchronization to GNSS for stabilizing Rubidium & OCXO oscillators. This option is available custom built.

safetime
#1 in ANTI-JAMING/SPOOFING



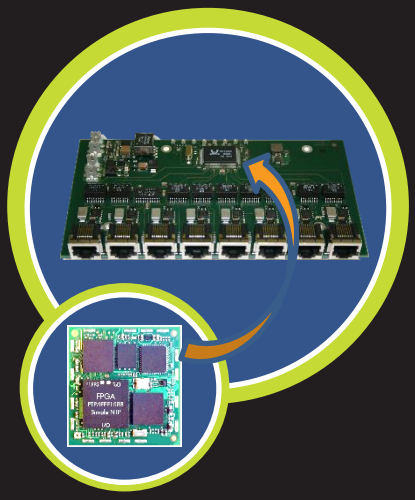
Link: Watch on Youtube

Private FPGA per each LAN
Best ever hardware isolation

4 modules X **2** LAN

Private FPGA per card
Best software VLAN isolation

1 modules X **8** LAN



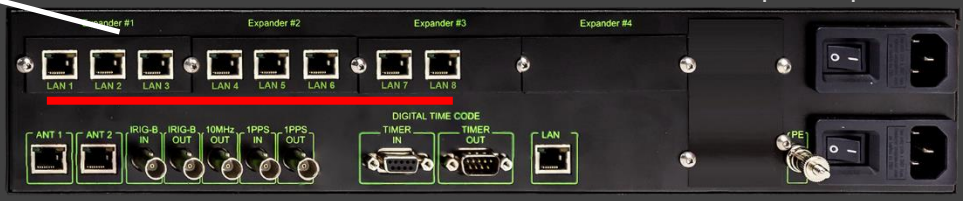
NTS-5000 provides strong security as each of the LAN module is 100% information isolated from another. It is so-called the “galvanic” isolation. To improve security NTS-5000 also isolate each network interface LAN on a software level. Any security compromise on one LAN module will be fully software isolated from another LAN module. Multiple independent networks and devices requiring separation can be connected to the same NTS-5000 without worry that security breach in one network will affect another network.

100% “Galvanic” isolation between LANs

On top of NTS-5000, GM server supports special expansion slots for additional network LAN interfaces. The available expansion modules are:

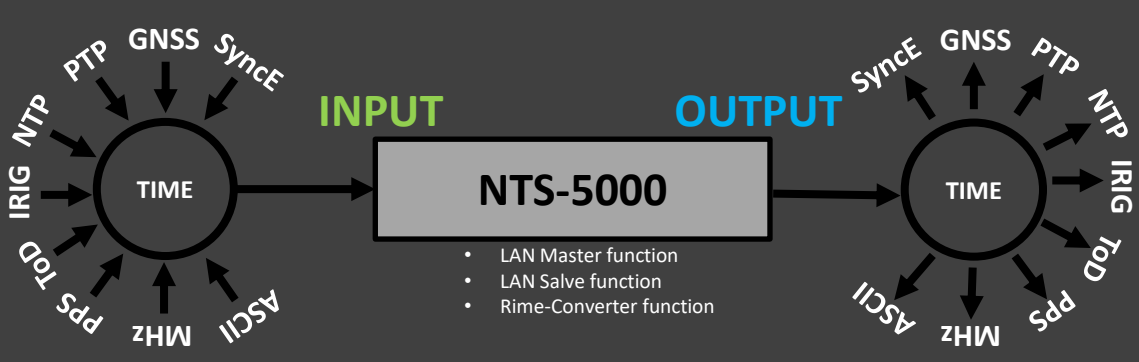
- 4x 2-port 1GbE Ethernet SFP/RJ45 (hardware high accuracy time-stamps)
  4x 2-port expanders

- 1x 8-port 1GbE Ethernet SFP/RJ45 (software std. accuracy time-stamps)
  1x 8-port expansion



Grandmaster – SubMaster/Slave – Converter

The value of the NTS-5000 is the functionality of a stable time distribution with a computer network offering very high synchronization accuracy as well as time coding conversion (NTP, PTP, IRIG-B, ToD/TC, 1PPS, 10MHz…).

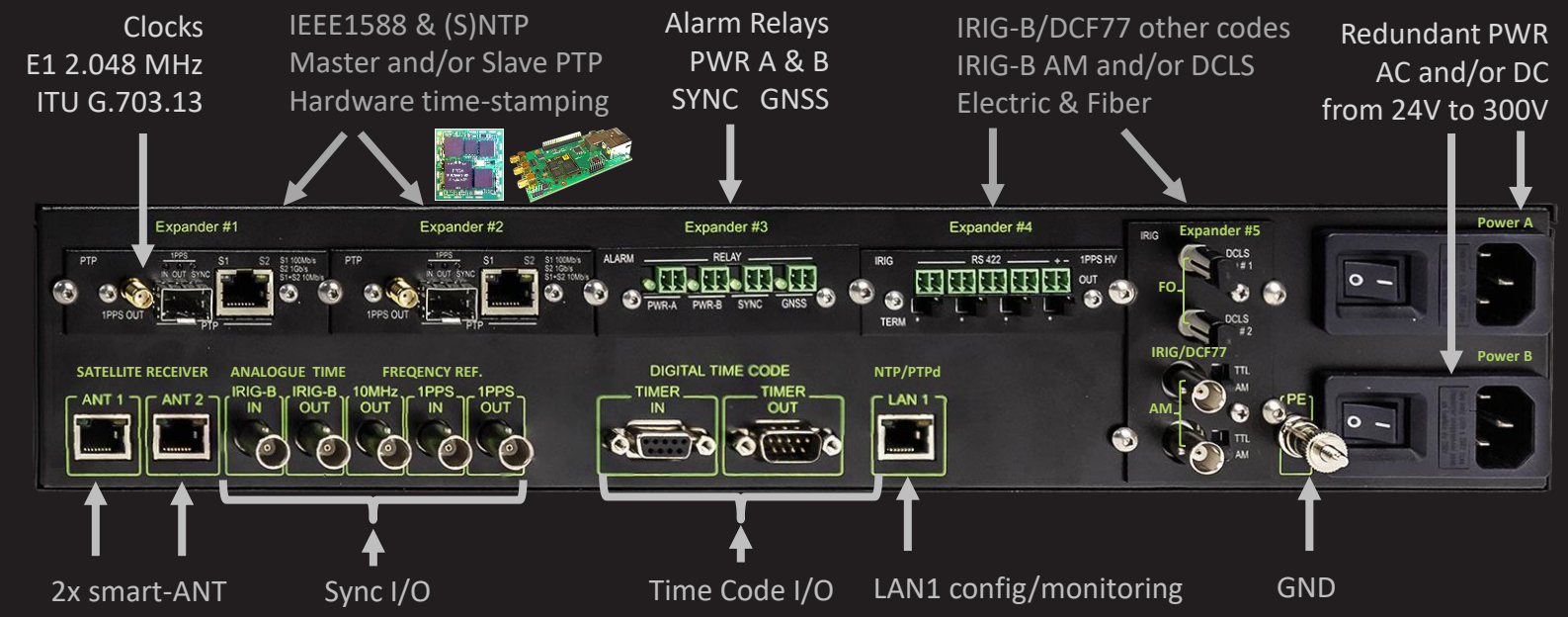


NTS-5000 offers world best class security network isolation ensuring high accuracy time & frequency domain operation.

Hardware Timestamping – a gateway to single nanoseconds

The ground floor of 2U of NTS-5000 timeserver is the compatibility floor for easy upgrade migration from NTS-3000/NTS-4000 to NTS-5000, the upper floor of 2U of NTS-5000 offers values-add functionalities.

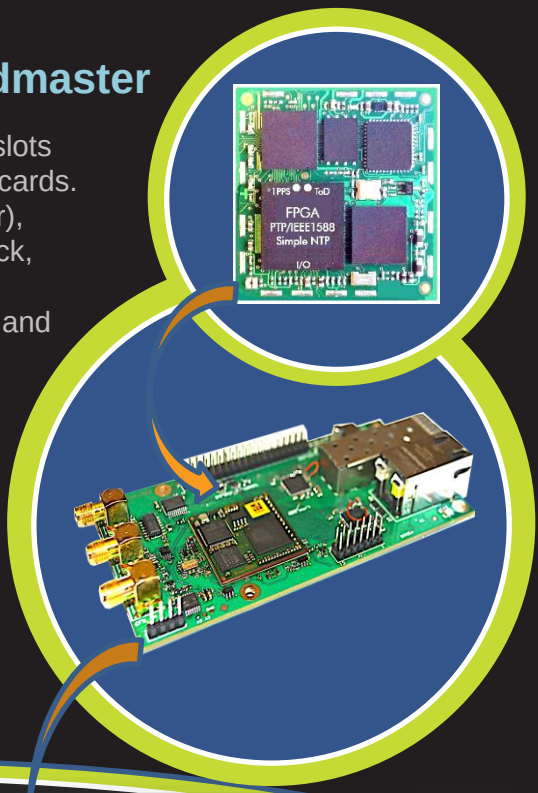
There are 2 kind of extensions boards for upper 2nd floor of 2U of NTS-5000:
(1) 4x 2-LAN miniatured expansion boards located in special Expander 1-4 slots (hardware timestamping)
(2) a single 1x expansion board supporting 8x 1-LAN (software timestamping)

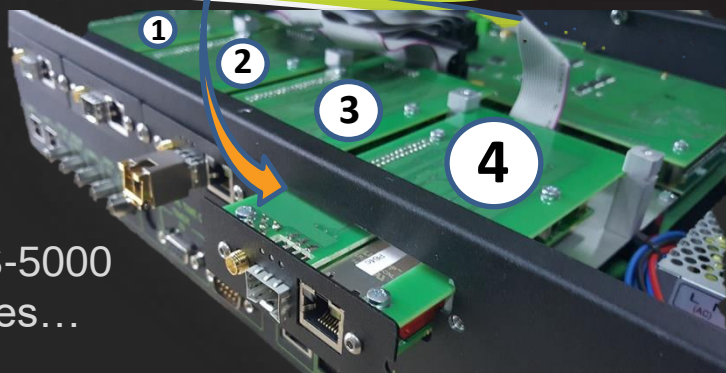


Autonomous NTP/ PTP servers inside one Grandmaster

On top of NTS-5000 Grandmaster (timeserver), there are 4 expansion slots for special autonomous (private FPGA) NTP/ PTP/IRIG-B (AM, DCLS) cards. Each Expander1-4 NTP/ PTP module has its own FPGA (the processor), private PTP-stack, private NTS-stack, private SyncE and private IP-stack, allowing each module to perform as autonomous master/grandmaster. Such architecture is like a hardware Master inside bigger GrandMaster and it ensures:

- highly accurate time domain for isolated critical networks
- best physical isolation of networks (handled by a single time server)
- Enables one NTS-5000 support of different PTP profiles:
  Example:
  =>Expander #1 set to PTP Telcom ITU-I G.8275.1
  =>Expander #2 set to PTP Power IEEE C37.238 v2
  =>Main LAN1 is dedicated to MIB-2 SNMP monitoring





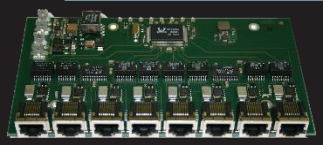
From private FPGA (via isolated NIC Network Interface Cards) to many independent 4x NICs inside one NTS-5000 handling national critical infrastructures…

Software Time-Stamping – increasing a volume of simultaneous

The ground floor of 2U of NTS-5000 timeserver is the compatibility floor for easy upgrade migration from NTS-3000/NTS-4000 to NTS-5000, the upper floor of 2U of NTS-5000 offers values-add functionalities.

There are 2 kind of extensions boards for upper 2nd floor of 2U of NTS-5000:
(1) 4x 2-LAN miniatured expansion boards located in special Expander 1-4 slots (hardware timestamping)
(2) a single 1x expansion board supporting 8x 1-LAN (software timestamping)

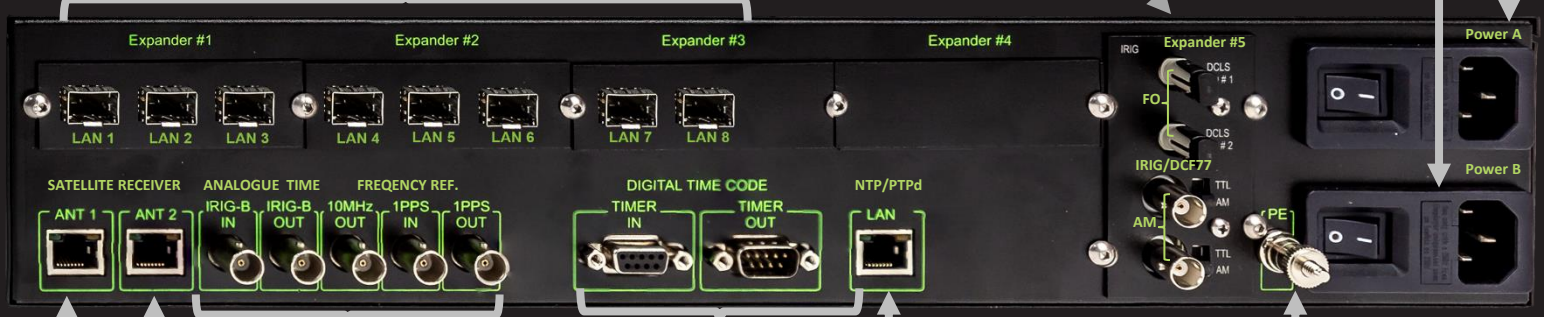
(2)



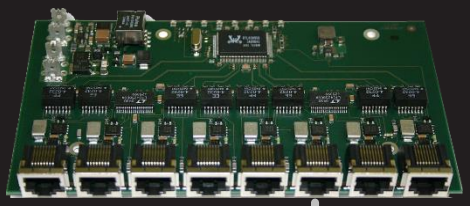
8x 1GbE SFP Ethernet NTP & IPTP EEE1588

IRIG-B/DCF77
IRIG-B AM or DCLS
Electric & Fiber

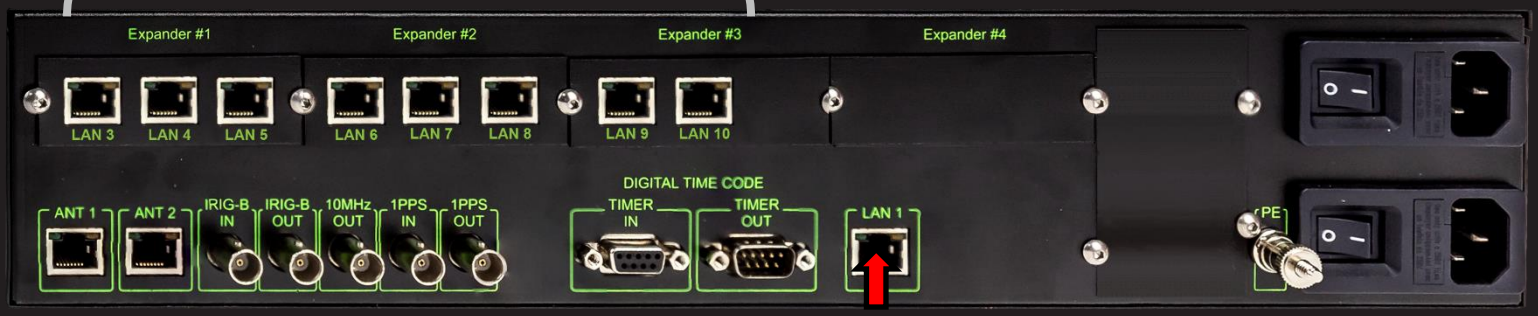
Redundant PWR
AC and/or DC
from 24V to 300V



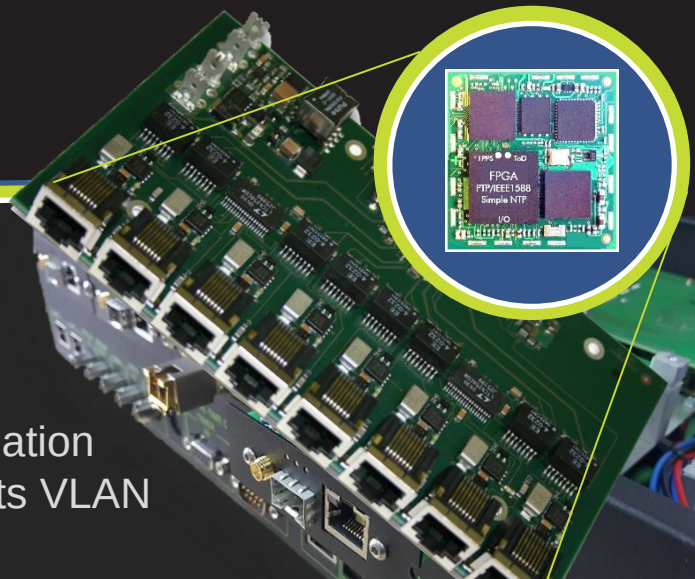
2x smart-ANT | Sync I/O | Time Code I/O | LAN config/monitoring | GND



8x 1GbE RJ-45 Ethernet NTP & IPTP EEE1588 (software timestamping)



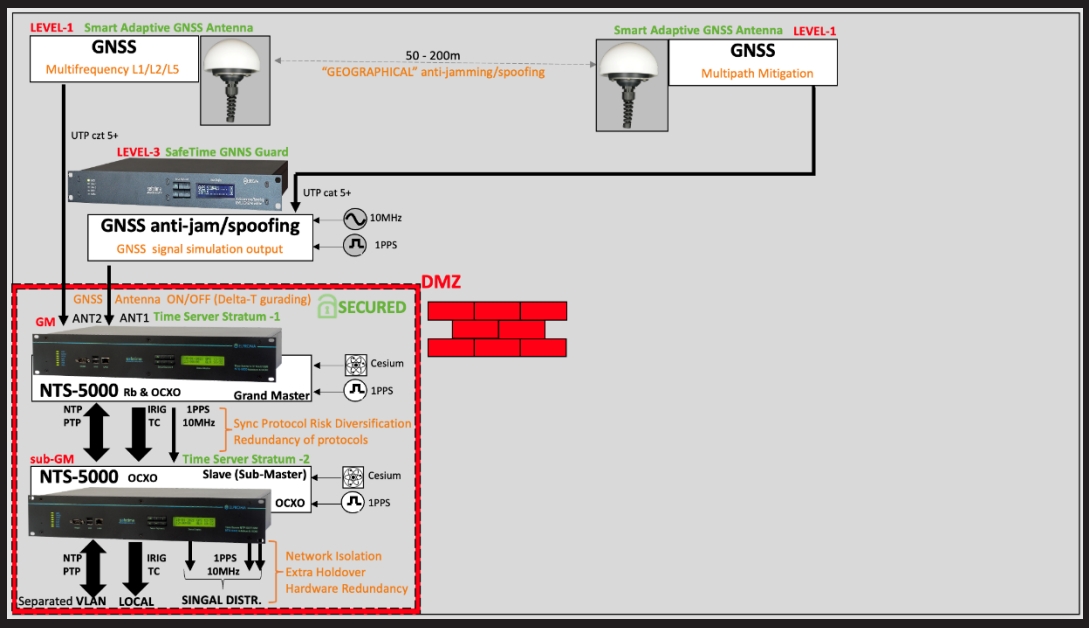
LAN interfaces can be numbered 1-10 or in 2 groups numbering 1-2 (compatibility mode) 1-8 extension floor



Single FPGA supports one expansion board (all 8x LAN interfaces). The isolation is software. This configuration supports VLAN

Application Notes – The three security LEVELS for GNSS anti-jamming/spoofing

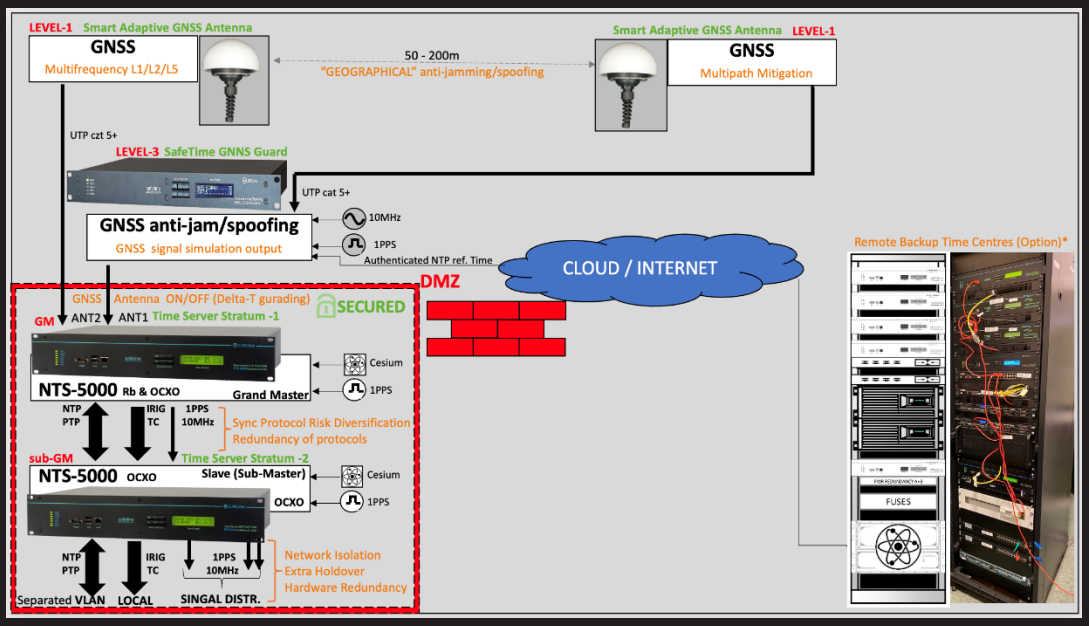
1) Basic Configuration. Use LEVEL-3 and independently 2x GNSS w/ min 200m distance between antenna



Applicable:

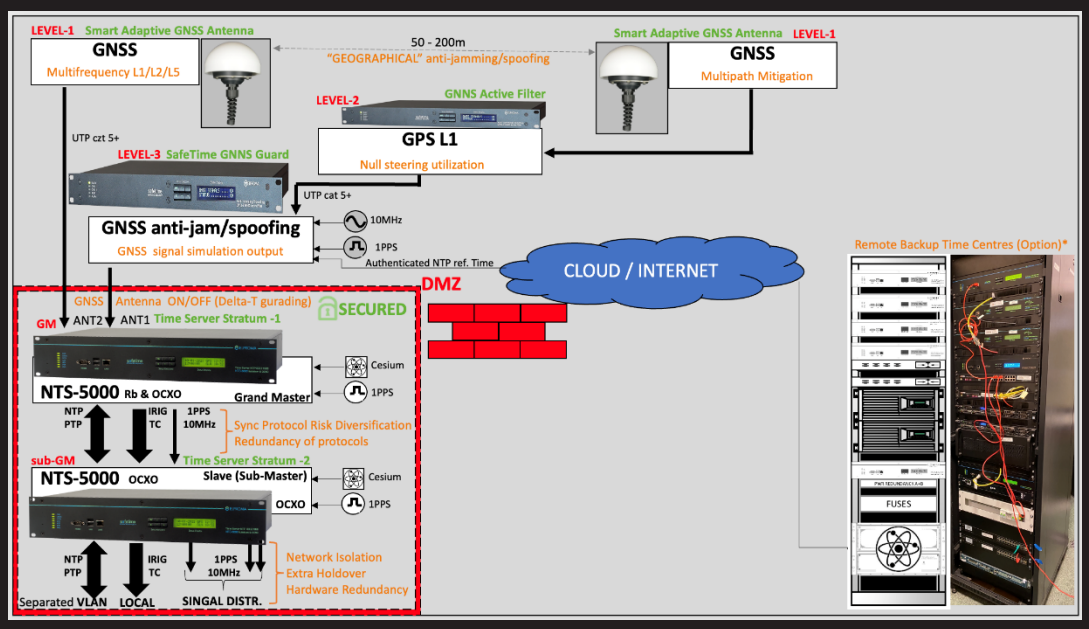
NTS-5000
NTS-4000
NTS-4000
NTS-Smart-antenna
SafeTime GNSS guard

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



NTS-5000
NTS-4000
NTS-Smart-antenna
SafeTime GNSS guard

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



NTS-5000
NTS-Smart-antenna
SafeTime GNSS guard
GPS L1 active filter

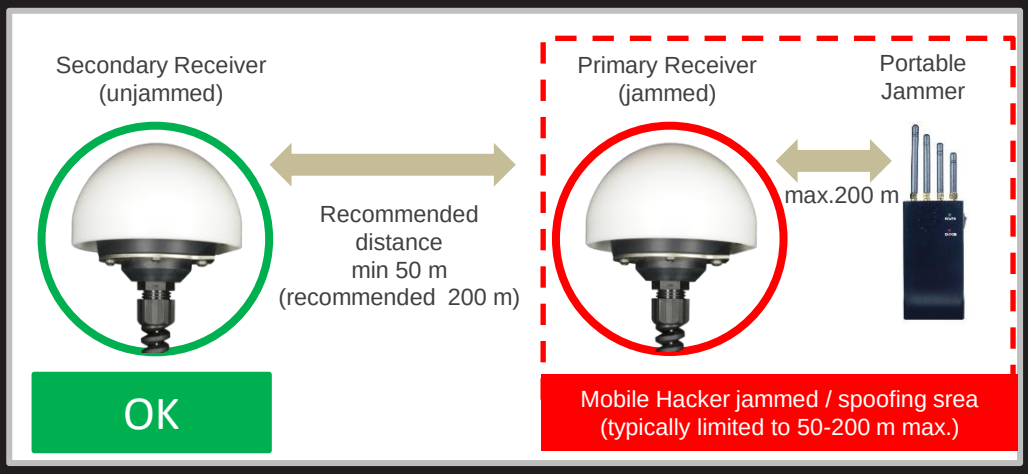
Application Notes – The three security LEVELS for GNSS anti-jamming/spoofing

Protection of the input clock source has become increasingly important. Elproma offers 3 LEVELS of cyber-security protection:.

- **LEVEL-1** 2x Smart-Antenna w/ GNSS receiver supporting RF-attack alarms down to NTS-5000
- **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 other levels.

The LEVEL-1 protection is built-in to standard NTS-5000/NTS-4000/NTS3000 network appliance. It has support for each GNSS receiver (ANT1, ANT2 inputs on NTS-5000) with auto-antenna ON/OFF switching when RF jamming or GNSS spoofing is recognised. It lets server switch early enough to operate 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 is special STAND-BY mode) when server is equipped with Rubidium & OCXO oscillators, and 4 hours only when NTS-5000 is equipped with OCXO oscillator alone (no Rubidium). Longer time holdovers increases the oscillator drift ensuring less accuracy of synchronisation for next days. Once the RF jamming/spoofing attack ends the NTS-5000 switches back to normal operation synchronizing from GNSS. The LEVEL-1 protection can be extra amplified by using simultaneously 2x GNSS receivers located min. 50 m (optimally >200 m) from each other. This is "Geographical" anti-jamming/spoofing approach perhaps the most effective to prevent against mobile amateur GNSS jammers and Hack-RF GPS spoofers. If the primary antenna is jammed (distance less than 200 m from jammer), the secondary antenna reminds outside the jammed area, and it still can take over to provide GNSS signal to NTS-5000. Independently NTS-5000 senses for RF-interferences and it is switching-OFF jammed antenna and continuing with 2nd antenna or algorithm can choose to switch to GNSS-less holdover mode. The LEVEL-2 protection is so-called GPS L1 Active Filtering, and it is boosting LEVEL-1 antenna operation by additional null steering GPS L1 filtering. It automatically recognizes and eliminates false GPS L1 signals send from ground, but not from space.



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 SafeTime GNSS Guard (this brochure product).
  It is the equivalent of network firewall appliance, but dedicated for separation from physical GNSS signals.
  The SafeTime GNSS Guard is a satellite GPS L1 C/A code simulator operating on electric signal level.
- The SafeTime 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

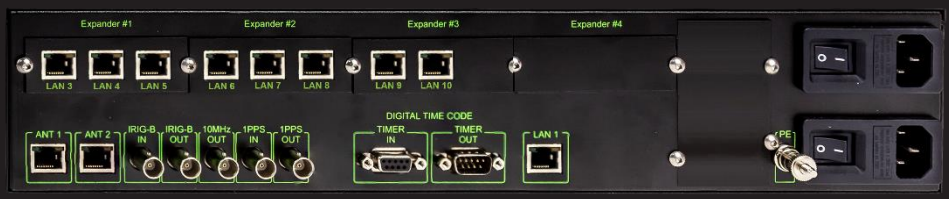
DATACOM & FINANCIAL Application Notes

DATACOM1: 2x100/10Mbps (Software Time-Stamping) LAN1&LAN2

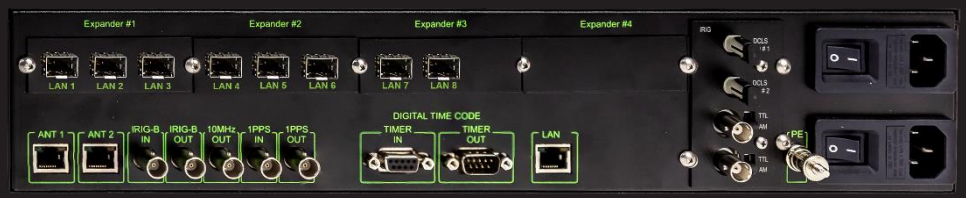
DATACOM2: 1x10GbE(LAN1) + 1x100/10Mbps LAN2 (Software Time-Stamping)

DATACOM4: 2x1GbE LAN3-4 (Hardware Time-Stamping) + DATACOM1 config

DATACOM5: 8x 1GbE LAN3-10 (Software Time-Stamping) + DATACOM1 config



DATACOM7: 8x 1GbE LAN3-10 (Software Time-Stamping) + DATACOM1 config

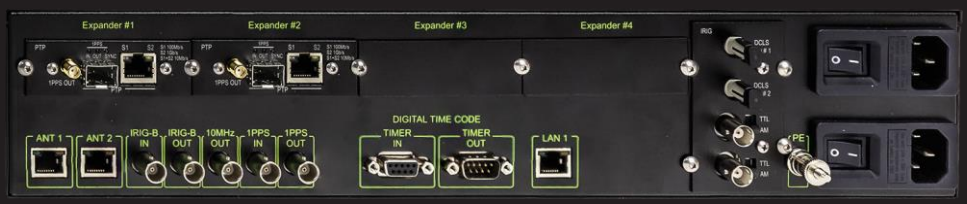


DATACOM9: 8x1GbE LAN3-LAN10 (Hardware Time-Stamping) + DATACOM1

SMART GRIDS – Application Notes

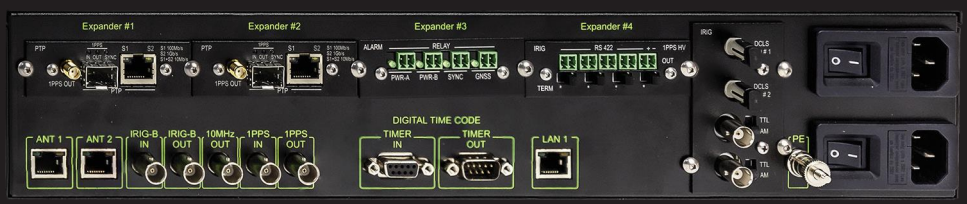
SMART-GRIDS1 4xIRIG-B DCLS rs422 (Expander #4) basis on DATACOM-5 conf.

SMART-GRIDS2 2xDCLS Fiber 2xDCLS TTL (Exp. #5) basis on DATACOM-5 conf.



SMART-GRIDS3 is a summary of 2x& 3 item above

SMART-GRIDS4 is like SMART-GRIDS3 with extra 4x ALARM RELAY



SMART- GRIDS CUSTOM1 - This is PTP SLAVE generating IRIG & DCF77 AM/DCLS

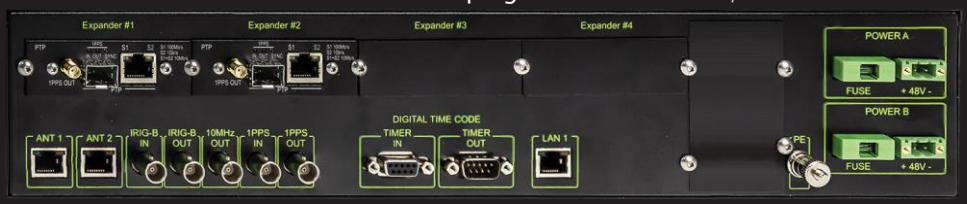
SMART-GRIDS CUSTOM2 - This is PTP SLAVE + CUSTOMS1 (above) + 10GbE out

TELECOM 5G/6G – Application Notes

TELECOM-1 PRTC-A 2x100/10Mbps, 48VDC NTP-Server w/ PTPd support

TELECOM-3 PRTC-A 2x10GbE,48VDC SW-stamping NTP-Server w/ PTPd support

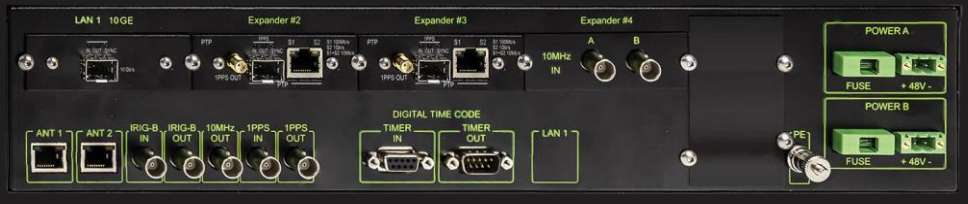
TELECOM-5 PRTC-A 4x1GbE HW-stamping Autonomous NTP/PTP GrandMasters



TELECOM-7 PRTC-A 8xGbE HW-stamping Autonomous NTP/PTP GrandMasters

TELECOM-8 PRTC-A 2x10GbE, 4xGbE HW-stamping Autonomous GrandMasters

TELECOM-9 ePRTC 1x10GbE, 4xGbE HW-stamping Autonomous GrandMasters



MIL/NATO Certification

WOJSKOWE CENTRUM NORMALIZACJI, JAKOŚCI I KODYFIKACJI
Military Centre for Standardization, Quality and Codification
43 KRAJOWE BIURO KODYFIKACYJNE
43 National Codification Bureau

ZAŚWIADCZENIE
CERTIFICATE

Zaświadcza się, że na podstawie złożonego wniosku podmiot o nazwie:
This is to certify that:

ELPROMA ELEKTRONIKA Sp. z o.o.

z siedzibą w:
located in:

05-152 CZOSNÓW UL. DUŃSKA 2A

otrzymał
was given

Kod NATO Podmiotu Gospodarczego:
NATO Commercial and Government Entity Code – NCAGE Code:

9ATKH

m.p.

DYREKTOR

dr inż. Mariusz SOCZYŃSKI

Warszawa, dnia 21 czerwca 2022 r.

Wojskowe Centrum Normalizacji, Jakości i Kodyfikacji – 43 Krajowe Biuro Kodyfikacyjne
00-909 Warszawa ♦ ul. Nowowiejska 28a ♦ tel. 261845708, fax 261845891 ♦ wcnjk@ron.mil.pl