ELPROMA

safetime

“Better Safe Than Sorry”

Advanced Sync Security

NTP/ PTP/ IRIG-B
IEEE1588 ePRTC
GNSS
Time Servers

- Smart Antenna Technology
- Jamming/ Spoofing Protection
- Enhanced Time Server Security
- Clock Accuracy
- SafeTime Audit Management Software (NMS-STAS)

Introduction Overview

1. Smart Antenna Technology

Current technology

Traditionally, to receive a GNSS signal, you will need a signal receiver board and an antenna to obtain RF timing signal for the NTP/ PTP time server. Most time server has the signal receiver board built-in the NTP/ PTP time server, while the antenna is a passive device that obtain signal from satellites through its line-of-sight.

Advanced technology

Elproma NTP/ PTP time server has developed a Smart Antenna where the GNSS receiver board is built into their Smart Antenna instead of the usual approach in time servers. The advantages of moving the GNSS signal receiver component to the Smart Antenna includes:

- Built-in jamming/ spoofing detection in GNSS receiver at the Smart Antenna before corrupted signal reaches the NTP/ PTP time server
- Easy replacement of faulty GNSS receiver or different GNSS satellite constellation receivers without downtime in NTP/ PTP time server, due to its modular design in the Smart Antenna
- Ease of updating to latest technology including Furuno's multi-path mitigation advanced technology, which enables antennas to be mounted in a low ground and accept reflected GNSS signal
- Elproma NTP/ PTP time server supports dual GNSS antenna ports to allow physical segregation of GNSS Antenna to receive different GNSS signals from different or same satellite systems
- Smart Antenna uses UTP/STP cat 5+ cable, which reduce expensive coaxial cable cost and enable connection to NTP/ PTP time server over a distance of up to 700m with any line amplifier

2. Jamming/ Spoofing Protection

Advanced technology

Elproma NTP/ PTP time server provides enhanced cybersecurity protection against jamming/ spoofing attacks. Elproma has developed a comprehensive jamming/ spoofing protection, which consists 3 levels of cybersecurity protection:

- Level 1: "Geographical" distance risk diversification
- Level 2: Anti-jamming/ spoofing filter (RF 1.5 GHz)
- Level 3: Time firewall with GNSS Emulation output

Introduction Overview

3. Enhanced Time Server Security

Current technology

Time server uses Network Time Protocol (NTP) and Precision Time Protocol (PTP) to distribute timing to other devices within a network. Most of them are single processor computer (FPGA) running over a single software stack dedicated to receive and distribute time via all available network LAN interfaces.

Advanced technology

- Elproma NTP/ PTP time servers supports expansion by adding special server autonomous NIC modules on top of the standard main network appliance. Each time server module has its own FPGA processor, private NTP/ PTP-Stack and IP-Stack, enabling each NIC module to perform as an individual autonomous grandmaster clock
- 100% isolation from other LAN cards
- Private PTP-Stack, IP-Stack and FPGA process

4. Clock Accuracy

Current technology

NTP/ PTP time server supports different internal oscillators to allow different holdover period of accurate time should the GNSS signal is not received. There are 3 common types of internal oscillators: TCXO, OCXO & Rubidium. Typically, these oscillators will provide holdover time from the internal quartz oscillator which receive time from GNSS.

Advanced technology

Instead of using TCXO as holdover clock like others, Elproma uses TCXO internal low-noise chip clocking capability to all its hardware in replacement of standard QUARTZ clock, commonly used by most time servers in the market. Using TCXO low-noise and OCXO simultaneously will further boosts the standard OCXO HOLDOVER. This approach helps to improve clocking input signal before output to OCXO or Rubidium for holdover or for time distribution.

5. SafeTime Audit Management Software (NMS-STAS)

Advanced technology

NMS-STAS is a powerful synchronization management and reporting tool which support multiple NTP/ PTP time servers according geographical regions. Using the application, you are able to manage hundreds of Elproma time severs and audit them with the data collected, to better understand the timing synchronization infrastructure.

1. Smart Antenna Technology

Traditionally, to receive a GNSS signal, you will need a signal receiver board and an antenna to obtain timing signal for the NTP/ PTP time server. Most time server have the signal receiver board built-in the time server, while the Antenna is a passive device that obtain signal from satellites through its line-of-sight.

Elproma NTP/ PTP time server has developed a Smart Antenna where the GNSS receiver board is built into their Smart Antenna instead of the usual approach in servers chassis. The advantages of moving the GNSS signal receiver component to the Smart Antenna includes:

Modular replaceable GNSS receiver inside smart NTS-antenna

Most GPS/ GNSS receivers are built-in to the NTP time server. Elproma has uniquely decoupled the GNSS receiver to their smart NTS-antenna to enable flexibility.

- Flexible to switch between GNSS receiver manufacturers. (supported CHIPS vendors include: Furuno, u-Blox, Trimble, NVS and others)
- Help to diverge risks of security & firmware gaps in using different CHIPS or receiver boards
- Ease of migration to new future GNSS constellations eg IRNSS or IRIDIUM
- Ease of migration from single (L1) to dual band (L1+L5 or L1+L2)

Dual GNSS antenna ports

Elproma NTS-3000/ 4000/ 5000 NTP/ PTP time servers comes ready with dual GNSS antenna ports. This allows:

- Greater coverage of GNSS services (each antenna can be receiving GNSS signal from different satellite constellations)
- Improves high availability (HA) of GNSS to each server
- Improves robustness of leap-second support
- Improves efficiency of bugs firmware risk diversification (when each antenna is equipped with a different GNSS brand receiver)

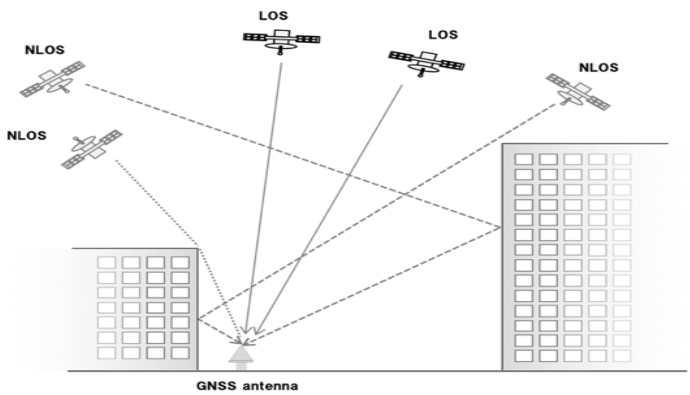
Built-in anti-jamming/ spoofing detection

Elproma has added anti-jamming/ spoofing detection to its smart antenna. When the NTS-Antenna deducts jamming and spoofing attacks, it sends special alarm signal directly to the NTP/ PTP time server to switch early to internal oscillator holdover clock (Rubidium or OCXO), and reject the false GNSS signals. This provides the first layer jamming/ spoofing protection to the antenna before reaching the time server.

1. Smart Antenna Technology

Ease of updating to latest antenna technology e.g. multi-path mitigation advanced technology from Furuno

Furuno manufacturer has developed a new technology to enhance the reception of GNSS signal. This unique functionality enables correct timing signal to be computed even when antennas are mounted in a lower ground and accept reflected GNSS signal.



Ease of Installation (UTP CAT5+ cable)

Most NTP/ PTP time server uses expensive coaxial cables to connect to GNSS antenna. Elproma time severs uses standard CAT5+ cable to connect to Smart Antenna. This provides:

- Long distance reach of up to 700 meters without the need for line amplifier
- Reduces cost by eliminating the need of expensive coaxial cable and line amplifier and eases the maintenance of active component (e.g. line amplifier), which can become a single point of failure

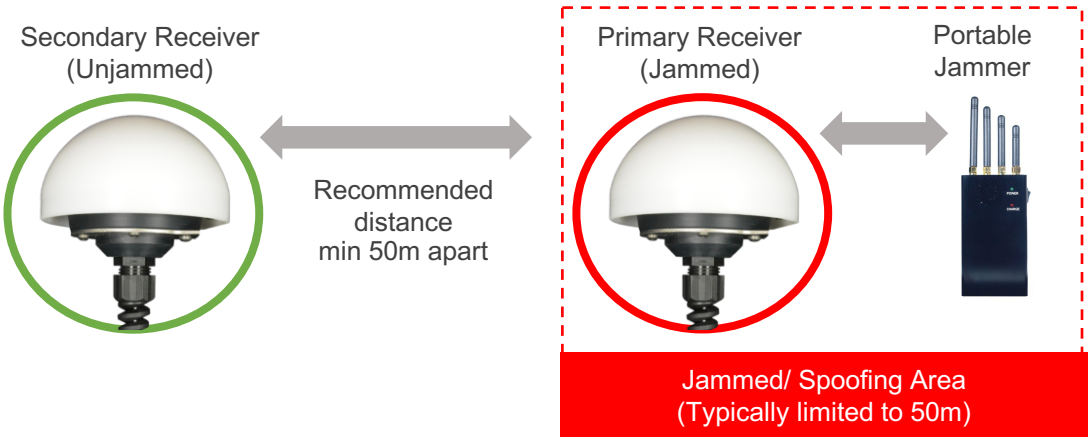
2. Jamming/ Spoofing Protection

Being a key global player in timing technologies, Elproma has invested many years of R&D into jamming/ spoofing protection. As jamming/ spoofing attacks come in different levels, Elproma has developed a comprehensive process of jamming/ spoofing protection which consists of 3 Levels.

Level 1

"Geographical" distance risk diversification

Elproma NTP/ PTP time servers comes with dual GNSS antenna ports. At Level 1, when 2 x Smart Antenna are at least 50m apart, the physical distance deters the risk of mobile jammers as the signal interference is typically limited to 50m. Therefore, if the primary antenna is jammed, the secondary antenna (outside the jammed area) can take over to provide GNSS signal to the time server.



Level 2

Anti-jamming/ spoofing RF filter

The **Active Filter** ensures "clean" data by removing the jammed/ spoofed data. Elproma provide a separate Level 2 device which helps to filter jamming/ spoofing signal before it goes into the time server.

Level 3

Time firewall with GNSS Simulation output

Elproma also provide a separate device called the Time Firewall which **simulates** digital GNSS data NMEA It is time corelated to real-life GNSS.

NTP/ PTP time server

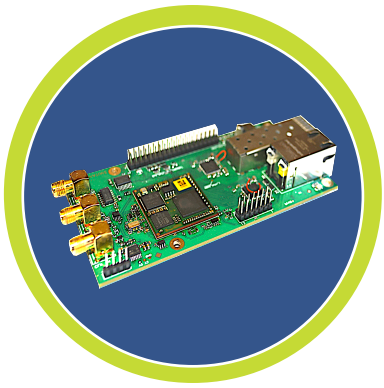
When an attack is detected at any level, time server NTS-5000 switches early to internal holdover clocks (Rubidium/ OCXO) refusing false signal. After the attack ended, NTS-5000 switches back to normal GNSS synchronization. This solution is also available for NTS-4000 and NTS-3000 too.

3. Time Server Security

NTP/ PTP time server uses Network Time Protocols (NTP) and Precision Time Protocol (PTP) to distribute timing to other devices within a network. Most of them are single processor server running over a software stack dedicated to receive and distribute time via all available LAN interfaces.

Autonomous NTP/ PTP time server

On top of Elproma NTP/ PTP time server, it also supports 4 expansion slots for the expansion of NTP/ PTP ports. Each NTP/ PTP module has its own FPGA processor, private PTP-Stack and IP-Stack, allowing each module to perform as an autonomous NTP/ PTP time server or Grandmaster clocks for PTP synchronization. Each module can also operate its own Private PTP IEEE1588 profile independent of another.

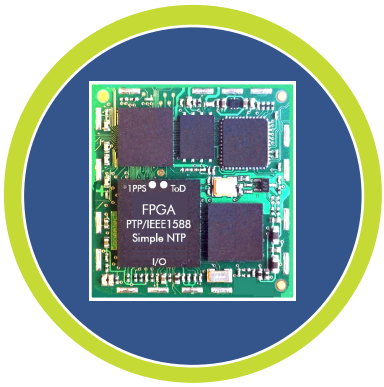


100% isolation from other LAN interfaces

Elproma NTP/ PTP time server provides strong security as each of the NTP/ PTP LAN module is 100% isolated from another NIC. Any security compromise on one LAN module will be fully isolated from another LAN module. Multiple autonomous networks can be connected to the same NTP/ PTP time server without worry that security breach in one network will affect another network.

Private PTP-Stack, IP-Stack and FPGA processor

Each module comes with private PTP-stack, IP-stack and FPGA chip onboard. This ensure SYNC stability resistance for random traffic (DDoS). Each module has its own operating firmware which help to minimize Time Peaks within each network. Any failure in a single module will have no impact on other modules.



NTS-4000 / 5000 NTP/ PTP time server has 4 expansion slots

Allow additional Gigabit COMBO ports LAN modules for NTP/ PTP expansion

4. Clock Accuracy

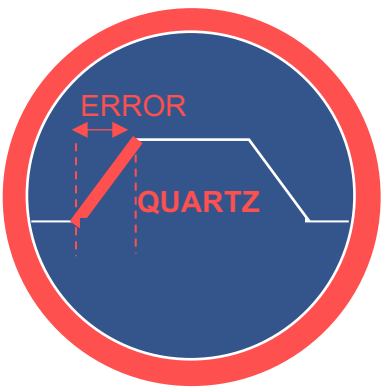
NTP/ PTP time server supports different internal oscillators to allow different holdover period of accurate time should the GNSS signal is not received. There are 3 common types of internal oscillators: TCXO, OCXO & Rubidium. Typically, these oscillators will provide holdover from the quartz oscillator received from GNSS.

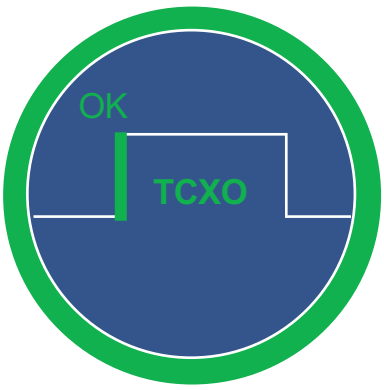
Elproma time server improves clock input signal accuracy by reducing its low noise error. Elproma NTP/ PTP time server supports holdover oscillators:

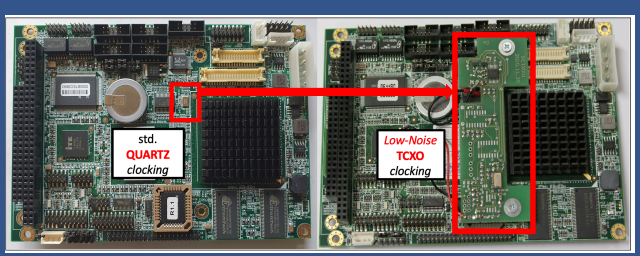
OCXO (HQ)

RUBIDIUM (Rb)

Instead of using TCXO as holdover clock like others, Elproma uses TCXO internal low-noise clocking capability to all its hardware in replacement of standard QUARTZ clock, commonly used by most NTP servers in the market. Using TCXO low-noise and OCXO simultaneously will further boosts the standard OCXO HOLDOVER. This approach helps to improve clocking input signal before output to OCXO or Rubidium for holdover or for time distribution.







2xGNSS | OCXO | Rb

Time server with QUARTZ ⟺ ~~TCXO~~

2xGNSS | OCXO | Rb

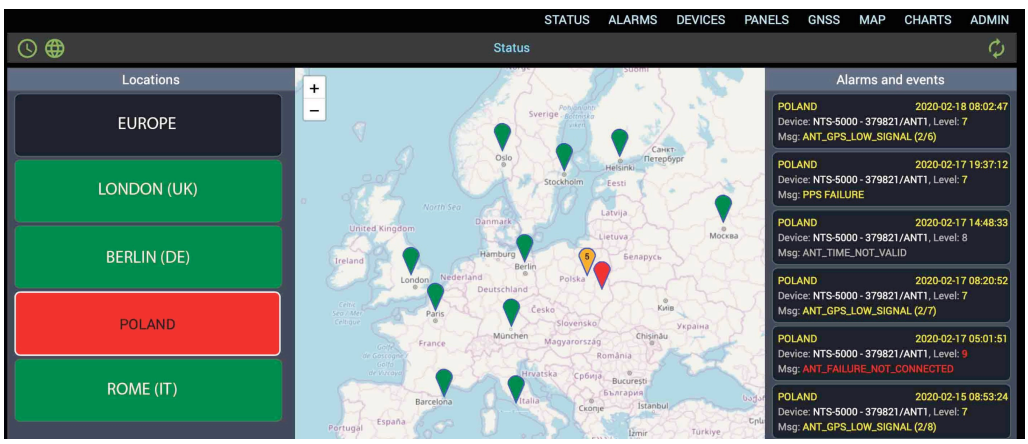
Time server with Low Noise TCXO

5. SafeTime Audit Management (NMS-STAS)

NMS-STAS is a powerful synchronization management software and reporting tool which support multiple Elproma NTP/ PTP time servers according geographical regions. Using the application, you are able to manage hundreds of NTP/ PTP time severs and audit them with the data collected, to better understand the timing synchronization infrastructure.

Real-time monitoring of multiple NTP/ PTP time servers and antennas

- Ease of monitoring as users can group their NTP/ PTP time servers based on their preference
- Quick visibility of multiple NTP/ PTP time servers' alarms and events log
- Multiple antennas can also be tracked as a group on a single console



Centralized graphical reporting

- Consolidation of data from multiple NTP/ PTP time servers data in central database. Data can be monitored simultaneously for all 3 parameters: OFFSET to UTC, Network DELAY, synchronization JITTER. Any time the UTC can be replaced by TAI time scale
- Centralized database provides the ability to produce a more comprehensive and graphical reporting. This functionality is important for critical infrastructures to prove the condition of synchronization system

Centralized audit logs and analysis

- These data will be stored in local database subsystem for several years (depends on legislation requirements) and can be used for time auditing purpose
- This also enhances analysis as it also provides the ability to recover the synchronization conditions at the defined date and time. Such functionality is useful for analysis like preventive for future blackout

ELPROMA

Your Trusted
Cyber Security &
Network Solutions Partner

Elproma Value-Added Distributor