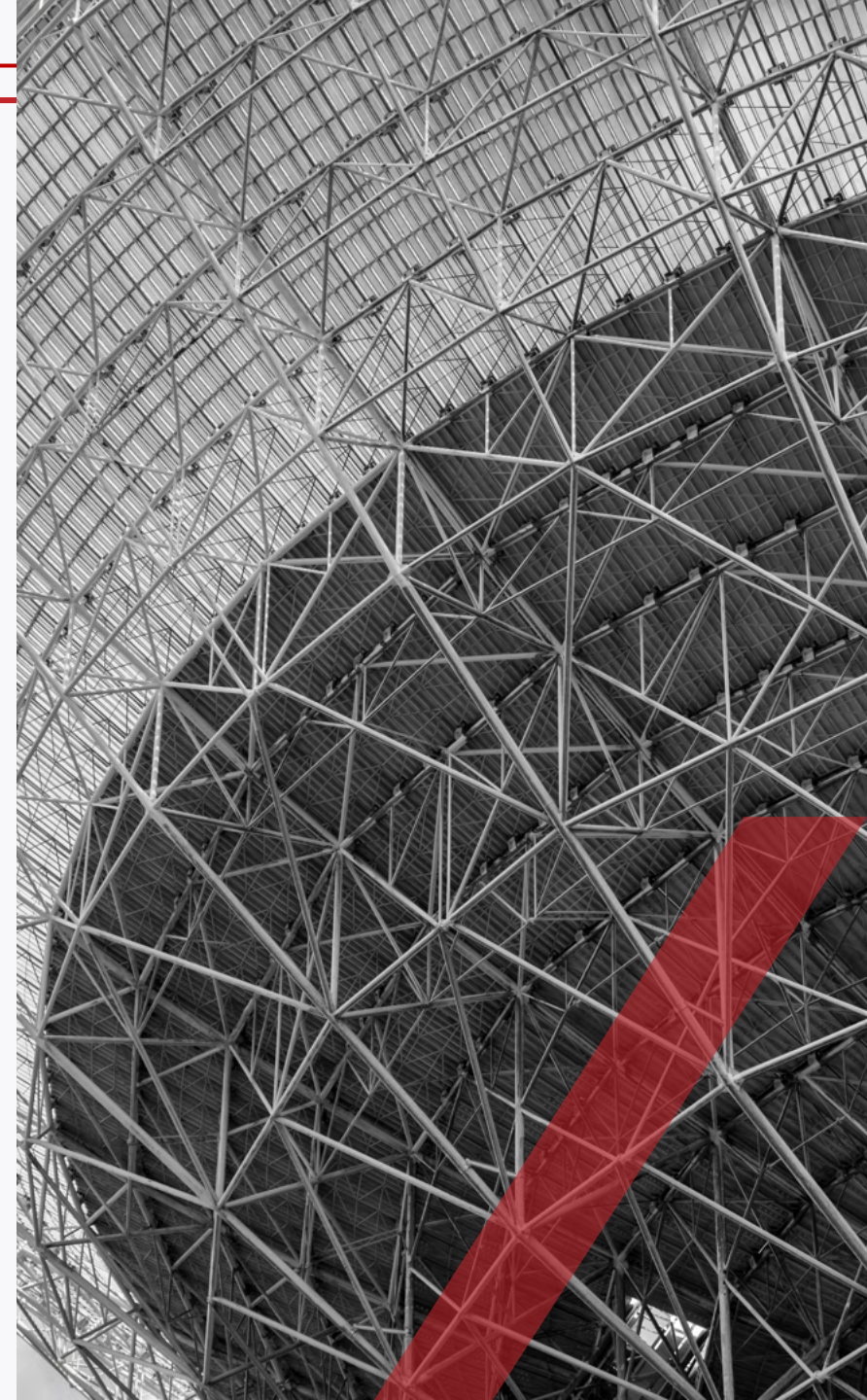


From IoT To Industry4.0 Elproma says “Better Safe Than Sorry”

Supporting Robust Network Time Synchronization for Critical Infrastructures:

- *Telecom 5G*
- *Traffic Control*
- *Space & Scientific*
- *Broadcasting*
- *TSN/Industry 4.0*
- *Military*
- *Smart-grids*
- *Cypher & Crypto*
- *Datacenters & Cloud*
- *Financial & HFT*
- *ISO27001 Security*
- *Autonomous cars*



Board of Management

Form the left:

Robert Bender (age 54)

Member of Supervisory Board

28 years experience in International Business Development

Sales Director of Elproma (1992-2014)

Monika Wardzyska (age 42)

Board of Directors (CEO) - President

20 years experience in International Business Development

Krzysztof Borgulski (age 44)

Board of Directors (V-ce President, CTO)

12 years experience in International Business Development

Tomasz Widomski (age 55)

co-funder, Member Of Supervisory Board (CINO, CMO)

30 years experience in International Business Development

Co-funder of Elproma Poland (1992) and CEO (1992-2014)



Company structure in hierarchy:

1. Shareholder Meetings (7 private investors)
2. Supervisory Board (Widomski/Bender)
3. Board of Directors (Wardzyska/Borgulski)
4. Directors (Wojciechowski/Grzywacz)



Elproma - a young well work motivated team located inside EU near Warsaw (Poland)

About



- ELPROMA global brand in telemetry & synchronization
- Engineering polish tech company since 1992,
- Subcontracted production,
- Product manufactured in Poland (EU),
- Poland => low fares & high quality,
- 50 employees, incl. 16 r&d engineers,
- Rapid prototyping,
- Flexibility & customizations,
- No project to small or to big,
- ISO 9001 certified
- IQ-Net auditing by Quality Austria
- Compliant to security ISO 27001



Company Value Management

Material assets:

- **portfolio of own product & systems**

Telemetry/M2M

www.teleorigin.com

Synchronization

www.elpromatime.com

Quantum sensors

www.fosrem.eu

- **end-customers, critical infrastructures, markets:**

NGCP (Philippines) => smart-grids IEC61850

T-Mobile (Poland) => 5G ITU-I G.8275.1 & 2

and many more ...

Immaterial assets

- **governmental relationships (immaterial asset)**

ITU => International Telecom Union

NMI => BIPM, NPL, NIST, GUM, SIQ, VSL, ROB ...

test & calibration to state primary ref. std.

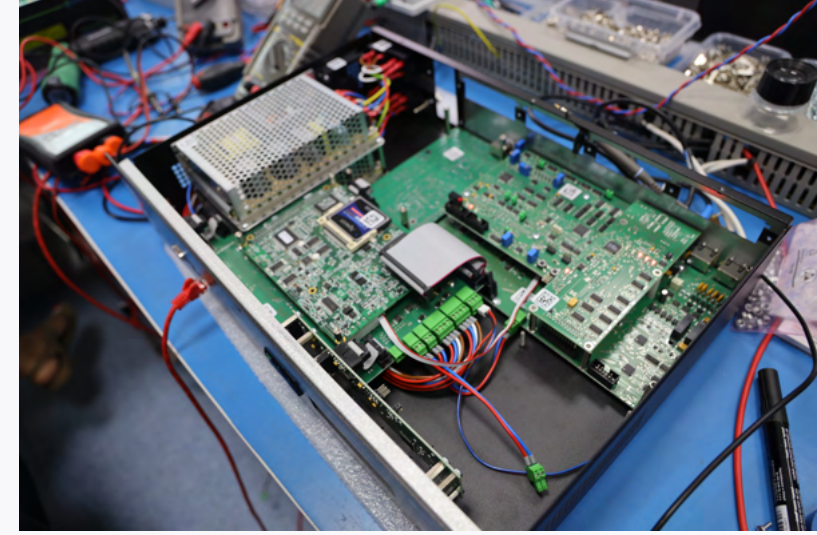
Generating Future Free Cash Flow:

- **Know-how** the picosecond clock synchronization,

- **Technology**, Signac effect quantum navigation,



SEIKO CEO
fascinated on NTS-pico
“CELSYDRA” brand



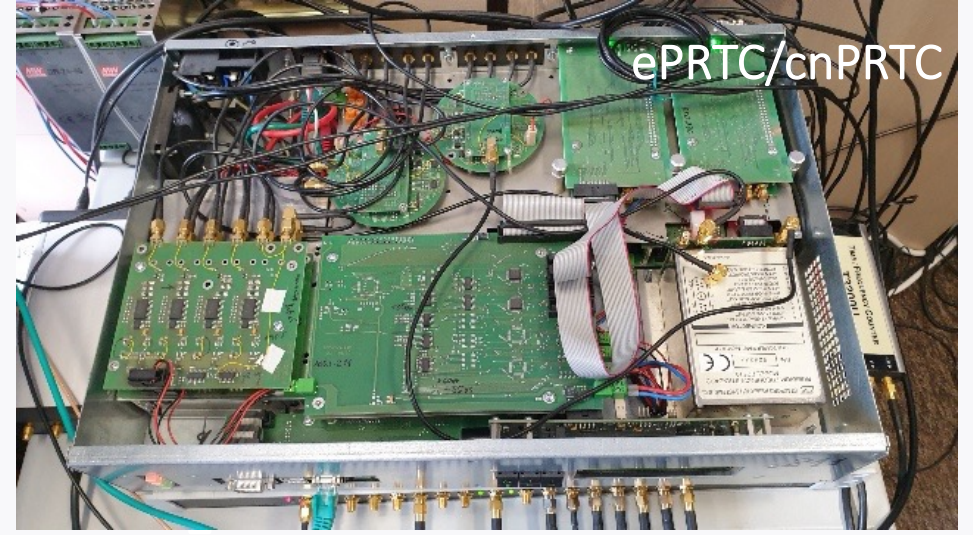
Production

- Qualified subcontracting
- Ultra fast std. 1 (max. 3) shift system
- Modern automatized SMD production
- X-rays & microwave quality control
- AI-cameras and human "eye" inspection
- Space industry clean room standards
- All above controlled under ISO9001



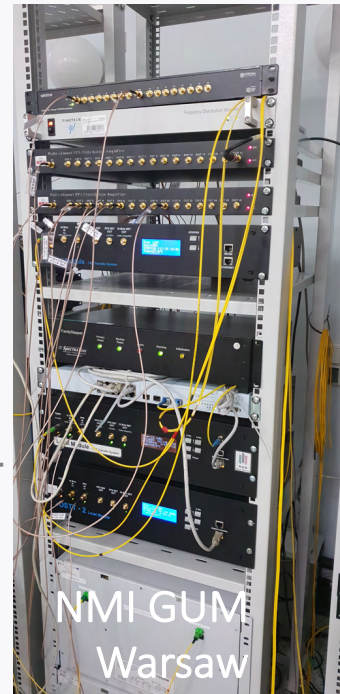


EUSPA (GSA/ESA)



Testing & Calibration

- Excellent references from EUSPA DEMETRA H2020
- Cesium Fountain & Clocks for ePRTC development
- Calibration to UTC(PL) at Polish Office of Measures
- GIANO calibration, the 1st GALILEO SAASM receiver
- UTC(NPL) at UK and UTC(IT) at INRIM validation
- White Rabbit



Our Contribution

- **ITU (International Telecom Union)** removing UTC leap-second [link](#) (doc #15)
 - ITFS2020 importance of time for Industry 4.0 (You Tube [link](#))
 - G2 Forum Geo-political TV discussion with 3M, Elproma (You Tube [link](#))

- **TAP Project (OCP)** – replaceable GNSS modules GM PCIe from Facebook/NVIDIA
 - Elproma contribution to Facebook & NVIDIA video (You Tube [link](#))
 - OCP Project Page listing ELPROMA as participant (7th Oct 2020 [link](#))

- **GIANO Project** (Thales Alenia Space) – the 1st professional GALILEO Timing Rcv with Anti-Spoofing Authentication Facility (together with PIK-Time)

- **DEMETRA Project H2020** TSI#2 “Trusted Time Distr. w/ Audit & Verif. Facility”
 - Horizon2020 Demetra GSA web page ([link](#))
 - PTTI/ION 2016 Demetra TSI#2 PDF paper ([link](#))
 - Success Story in Asia Smart-Grids ([link](#))

- **CERN White Rabbit** co-developer (today’s High Accuracy IEEE1588:2019 stack)
 - PTTI/ION 2011 very first introduction PDF paper ([link](#))
 - CERN original team list 2009-2014 ([link](#))

2021-2022



Radiocommunication Study Groups WP-7A

2020-2021



OPEN
Compute Project®

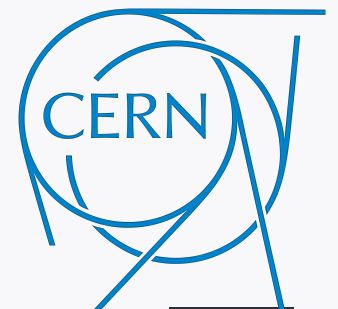
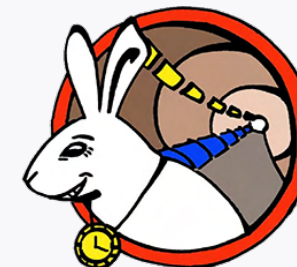
2019-2021



2015-2017



2009-2014



GNSS Synchronisation vs. Geopolitics Time – Changing Paradigm of Security



US Directive EO 13905 signed Feb 2020

GNSS sensitive geopolitics:

- US friendly => GPS + GALIEO
- CN friendly => BEIDOU
- RU friendly => GLONASS
- US & RU friendly => IRNSS+GPS+GLONASS
- US & CN friendly => GPS+GALILEO+BEIDOU
- □ ■ ■ all others => any GNSS



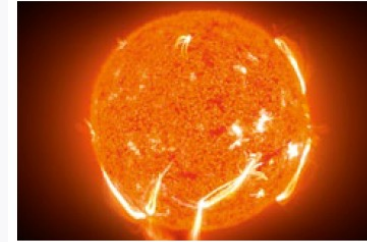
GPS, GLONASS, BEIDOU, IRNSS are military
GALILEO is civil. The NMI (e.g. NIST) time backup is recommended

AIR FORCE OFFICIAL PRESS RELEASE - GPS GROUND SYSTEM ANOMALY**JAN 27, 2016**

On 26 January at 12:49 a.m. MST, the 2nd Space Operations Squadron at the 50th Space Wing, Schriever Air Force Base, Colo., verified users were experiencing GPS timing issues. Further investigation revealed an issue in the Global Positioning System ground software which only affected the time on legacy L-band signals. This change occurred when the oldest vehicle, SVN 23, was removed from the constellation. While the core navigation systems were working normally, the coordinated universal time timing signal was off by 13 microseconds which exceeded the design specifications. The issue was resolved at 6:10 a.m. MST, however global users may have experienced GPS timing issues for several hours. U.S. Strategic Command's Commercial Integration Cell, operating out of the Joint Space Operations Center, effectively served as the portal to determine the scope of commercial user impacts. Additionally, the Joint Space Operations Center at Vandenberg AFB has not received any reports of issues with GPS-aided munitions, and has determined that the timing error is not attributable to any type of outside interference such as jamming or spoofing. Operator procedures were modified to preclude a repeat of this issue until the ground system software is corrected, and the 50th Space Wing will conduct an Operational Review Board to review procedures and impacts on users. Commercial and civil users who experienced impacts can contact the U.S. Coast Guard Navigation Center at (703) 313-5900.

Global Navigation Satellite System (GNSS)

GNSS (such as GPS, Galileo, etc.) depend on accurate time. But their signal is weak – about as powerful as a light bulb shining on the moon. Any interference distorts GNSS time stamping. Some of the more common causes of interference are as follows:



SOLAR STORMS: GNSS signals are affected by solar storms – disturbances of the Earth's magnetic field by streams of charged particles from the Sun.



URBAN CANYON EFFECTS: Dense cityscapes create urban canyon effects. Steel framed buildings totally block signals – or create reflections and false data readings.

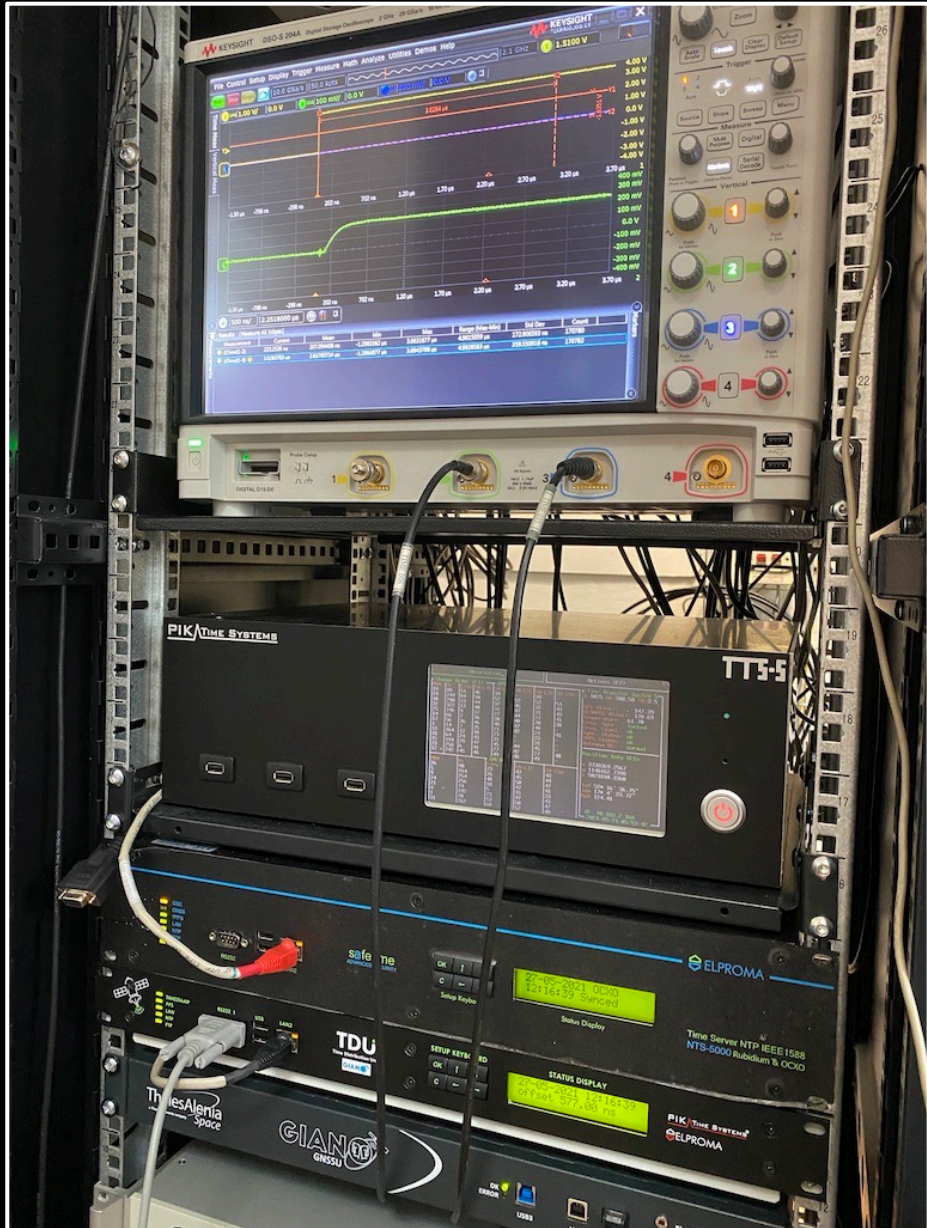


JAMMING: GNSS signals can be deliberately jammed – often by drivers dodging employers' attempts to track them. The City of London alone has 80 to 120 GNSS jamming incidents each month.*



SPOOFING: GNSS signals can be spoofed, with false signals creating false timing. Spoofing attacks could be completely undetectable.

GIANO 1st SAASM GALILEO EU RCV



in collaboration to Thales Alenia Space

Robust Synchronization Systems



Multi Level Redundancy
by many NTS-5000 Rubidium Servers

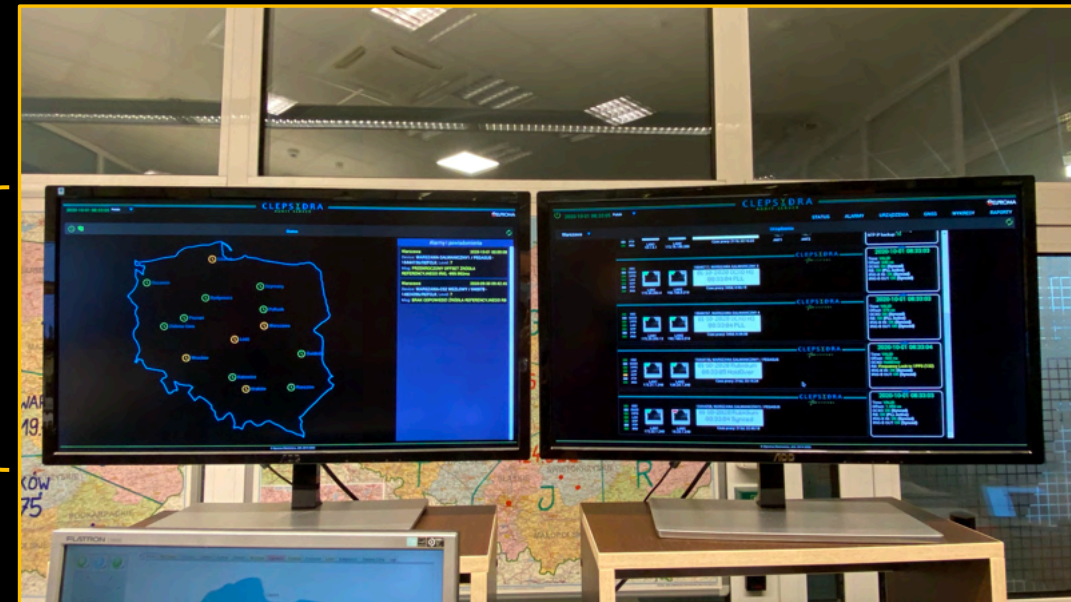
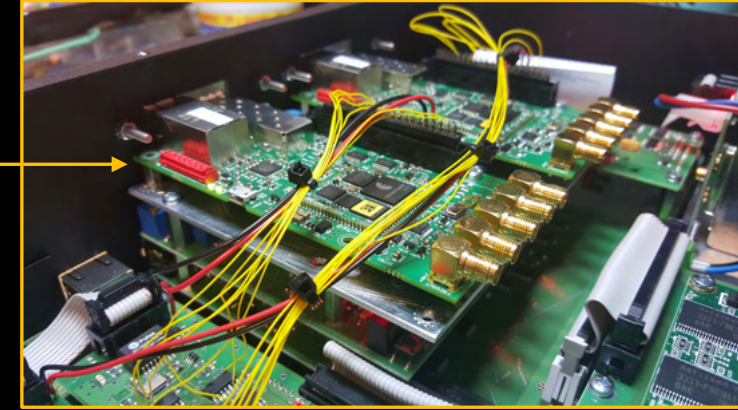
NTS-9000 Cs
Direct Cesium 5071A Time

Tracing & Audit
DATA Servers

Real-Time Monitoring
of synchronization
of critical infrastructure

The largest deployment includes
350pcs. Rubidium T-Servers [link](#)






Security & Isolation
Each NIC is autonomous grandmaster
(private FPGA per LAN)



New Security Approach - Smart Antenna

View  link for more details

1) The replaceable GNSS-receivers supports different vendors

- makes time-server independent on volatile GNSS technology
- best world leading CHIP suppliers    
- quick replacement to next CHIP module if firmware bug detected
- autogain 26-40dB smart sensing works at any weather condition
- multi-path mitigation for reflected signals 
- geopolitics settings => exclusive: GPS, GALIELO, GLONASS, BEIDOU
- single L1 or multiband L1 + L2 + L5 frequency for robust synchronization
- UTC with robust LEAP-SECOND support

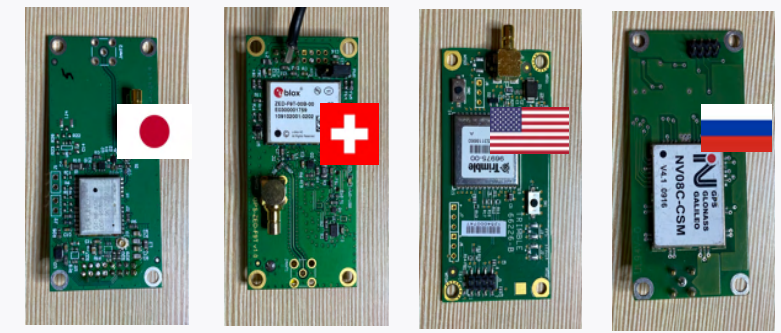
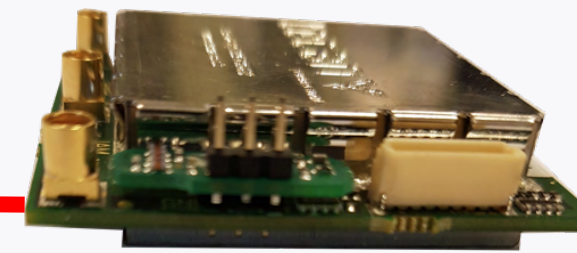
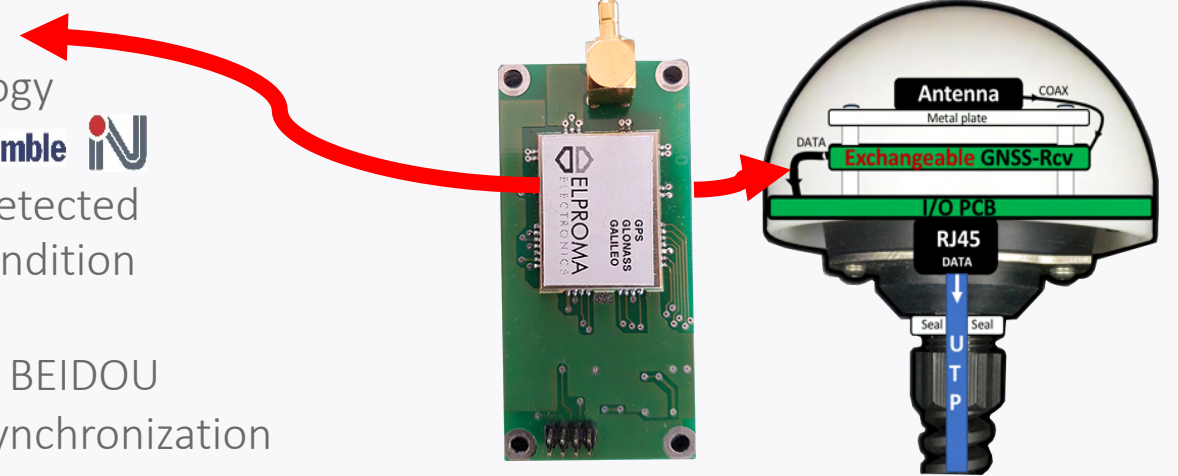
2) Built-in anti-jamming/spoofing detection and active-filtering

- alarm generated down to server – it lets it switch early to holdover mode
- active jamming filtering GPS L1 with option to full antispoofing GNSS L1/L2/L5

2) Real physical redundancy, 2x GNSS receivers, each from different vendor

- improves high availability of GNSS signals (2 different receivers in use)
- introduces the geographical anti-jamming if min. distance 100m between

4) Extremely Easy installation. No coax cables in use - only UTP cat5 – max. dist. 700m



From April 2021 1st public release at PTI/PIIT [link](#) to official contribution at ITU 2021



Date: the 12th of Apr 2021

PL 05-152 Czosnow, ul Dunska 2A, Poland www.elpromatime.com

The expert recommendation of activities regarding future UTC leap-second support

To Whom it may concern,

Further continuation of handling *UTC leap second* introduces a high risk of failure for IT and Industry4.0 (OT). Although the leap-second problem has always existed, currently with exponentially growing automation and the close interdependence of entire Industry4.0 systems, there is recommendation for immediate suspension of the *UTC leap-second*. Currently considered the first in history negative leap-second makes us especially worry.

The global economy is strongly dependent on GNSS, which provides the UTC reference to all modern critical infrastructures, such as distributed smart grids, telecom 5G, financial markets and broadcasting. Moreover, the observed strong migration of smaller IT/OT systems to CLOUD makes it a 5th critical infrastructure. The following problem affects all countries and all segments of each individual economy. It is complicated by the lack of leap-second servicing standard, the poor dialogue between the IT and time metrology community, the diversity of implementation of GNSS receivers, as well as different approach of serving UTC between GLONASS vs. GPS/GALILEO/BEIDOU/IRNSS.

The leap-second makes UTC time scale discrete, hence appearance of problems such as:

- 1) Time discrepancies in distributed system, where the validity of the data is determined by difference between *remote sensor timestamp* and receiving local timestamp of central server. This may lead to the acceptance of invalid data (wrongly computed DELAY) and, consequently, to the wrong predictive management. Such risk will increase with the growing popularity of TSN (Time Sensitive Networking) and TCC (autonomous Time Coordinated Computing) at Industry4.0
- 2) Failures of software and firmware of IoT devices based on the Windows or Linux/Unix kernels. Please note, that every modern IT / IoT device produced as of today has a firmware based on one of the operating systems listed above. The unexpected peaks in time introduced by the UTC leap second are dangerous for stability of the OS-kernel. They disturb the low-level event chronology, according to which concurrency management and the low-level utilization of system processes take place. Disturbing the chronology results in the "kernel panic" – risk causing crash of the operating system (OS), firmware or even a part of CLOUD.

The UTC leap second can trigger a large-scale domino effect, leading to a blackout: in telecom, power systems and Industry 4.0 automation. Sooner or later, such failures must begin to occur, unless a leap-second suspension remains effective. We consider a negative leap second, which has never been put into practice before, to be particularly very dangerous experiment on a working active production environment.

on behalf of Elproma



Tomasz Widomski
Member of Supervisory Board

Radiocommunication Study Groups



Received:

Document 7A/xx-E
26 August 2021
English only

Subject: Working document towards a preliminary draft new Report ITU-R TF.[UTC]

Poland

PROPOSED ADDITION TO WORKING DOCUMENT TOWARDS A PRELIMINARY DRAFT NEW REPORT ITU-R TF.[UTC]

As part of the preparation by WP 7A of a draft new report on UTC responding to Resolution 655 (WRC-15), | Poland proposes additions to chapter 6:

- *Chapter 6 on Impact of a possible change in the definition of UTC on radiocommunication services and other applications;*
- *creating new section 6.12 on Impact on other applications - IT and Industry 4.0, containing proposed text given below;*
- *creating new section 6.13 on Impact on other applications – not technical, containing the original text of section 6.12 without modification.*

The global economy is strongly dependent on GNSS, which provides the UTC reference to all modern critical infrastructures, such as distributed smart grids, telecom 5G, financial markets and broadcasting. Moreover, the observed strong migration of smaller IT and Industry 4.0 (OT) systems to CLOUD makes it a 5th critical infrastructure. The following problem affects all countries and all segments of each individual economy. It is complicated by the lack of leap-second servicing standard, the poor dialogue between the IT and time metrology community, the diversity of implementation of GNSS receivers, as well as different approach of serving UTC between GLONASS vs. GPS / GALILEO / BEIDOU / IRNSS.

Further continuation of handling *UTC leap second* introduces a high risk of failure for IT and OT. Although the leap-second problem has always existed, currently with exponentially growing automation and the close interdependence of entire Industry 4.0 systems, there is a need for urgent suspension of the *UTC leap-second*. Currently considered the first in history negative leap-second makes users especially worry.

The leap-second makes UTC time scale discrete, hence appearance of problems such as:

- 1) Time discrepancies in distributed system, where the validity of the data is determined by difference between *remote sensor timestamp* and receiving local timestamp of central server. This may lead to the acceptance of invalid data (wrongly computed DELAY) and, consequently, to the wrong predictive management. Such risk will increase with the growing popularity of TSN (Time Sensitive Networking) and TCC (autonomous Time Coordinated Computing) at Industry 4.0;
- 2) Failures of software and firmware of IoT devices based on the Windows or Linux/Unix kernels. It is to be noticed, that every modern IT / IoT device produced as of today has a firmware based on one of the operating systems listed above. The unexpected peaks in time introduced by the UTC leap second are dangerous for stability of the OS-kernel. They disturb the low-level event chronology, according to which concurrency management and the low-level utilization of system

ELPROMA

at SI2021 EU SECURITY



14.30 – 15.30 Panel 5: Private Sector's Perspective on the New Cybersecurity Landscape

in cooperation with the Kosciuszko Institute



Recent events such as the SolarWinds, Hafnium and Colonial Pipeline cyberattacks have demonstrated the evolution of the threat landscape – and how greatly unprepared we are. Ransomware and phishing attacks are becoming not just more common, but also more harmful. All of that is a chronic problem of global IT systems that enable such malicious activity, and the pandemic has only accelerated this process. The global community needs to take concrete actions to fix the IT system in order to fight cybercrime and mitigate risks – not just react once operations are disrupted. Particularly companies have to realign and sometimes even entirely redesign their cybersecurity schemes to protect their assets. A change of attitude towards cybersecurity is much needed as well. What have companies learned in the past few months? What kind of countermeasures have they implemented and are they effective? What should be done to use the experience gained during the COVID-19 pandemic to improve cybersecurity?

SPEAKERS:

- [Tomasz Widomski](#), Member of Supervisory Board, ELPROMA, Poland
- [Matjaž Breskvar](#), Director, Beyond Semiconductor, Slovenia
- [Rok Prešeren](#), PhD, Director, ICT and Network Services, Telekom Slovenije, d. d.
- [Guido Lobjano](#), Vice President and Director General for Europe, ITI – The Information Technology Industry Council (tbc)
- [Cezary Albrecht](#), CLO, T-Mobile (digital speaker)
- Moderated by: [Luigi Rebuffi](#), Secretary General, European Cybersecurity Organisation (ECISO)

15.30 – 16.00 Coffee Break

Server Cybersecurity Approach

1) Each LAN network card is the autonomous GRANDMASTER

- ensures uninterrupted performance for each LAN
- no peak times redistributed between NIC cards

2) Security, the LAN cards are 100% isolated from each other

- they use analog PPS+ToD signals used internally to SYNC
- no use of TCP/IP makes hacker attack not possible

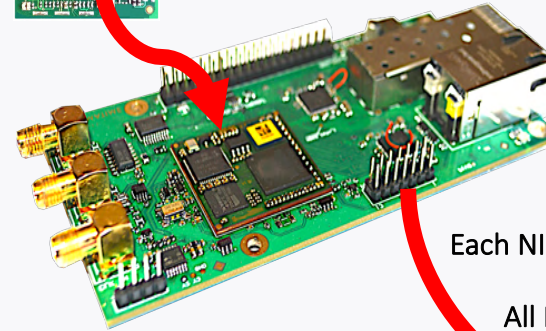
3) Private: PTP-stack, IP-stack, FPGA for each single LAN card

- ensures SYNC stability resistant for RND-traffic and DDoS
- single LAN HW failure makes no impact on other LANs

4) Private PTP IEEE1588 different profiles for each LAN card NIC

- simultaneous support different profiles on each NIC
- simultaneous supports MASTER/SLAVE for server
- new PTP profile conversion (any to any IEEE1588 profile)
- new GATEWAY (isolated clock) feature

Private FPGA



[View !\[\]\(aab88c0d099e5d18d6533a97b13ec28d_img.jpg\) link for more details](#)

Each NIC is autonomous grandmaster w/ analogue sync

All NICs are 100% isolated from each other (no TCP/IP)



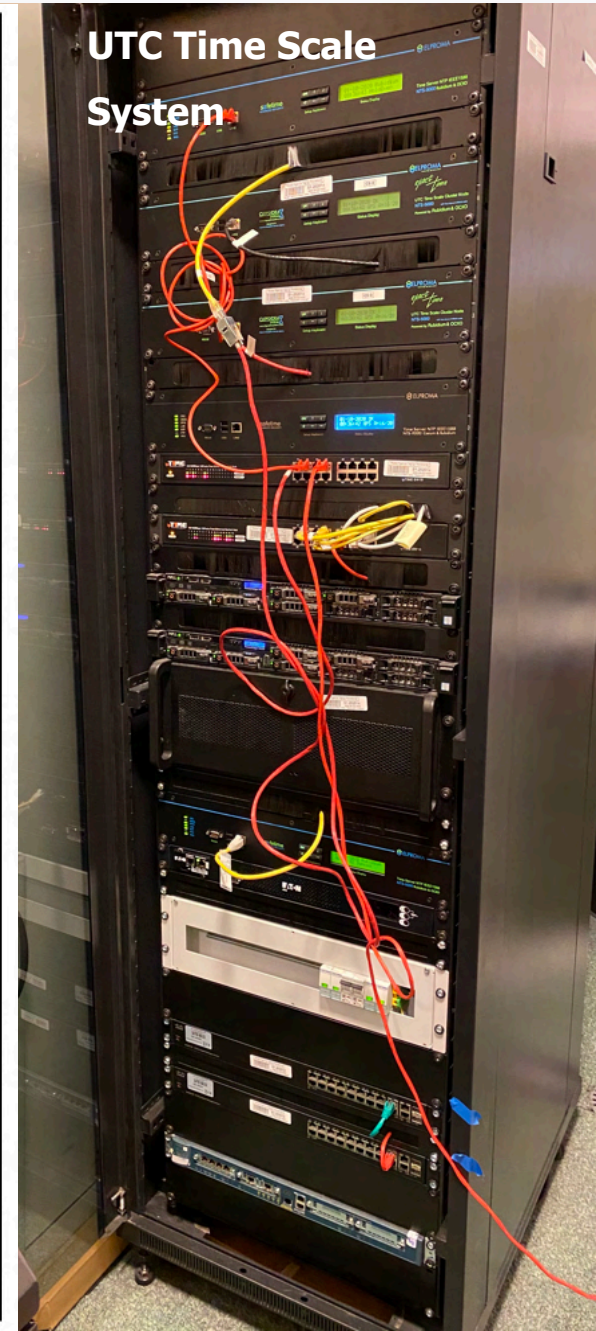
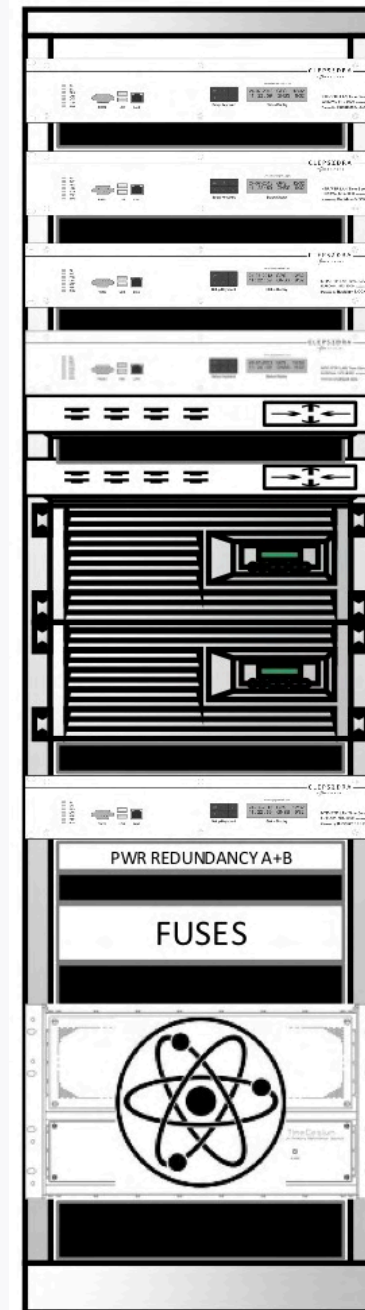
NTS-5000 family

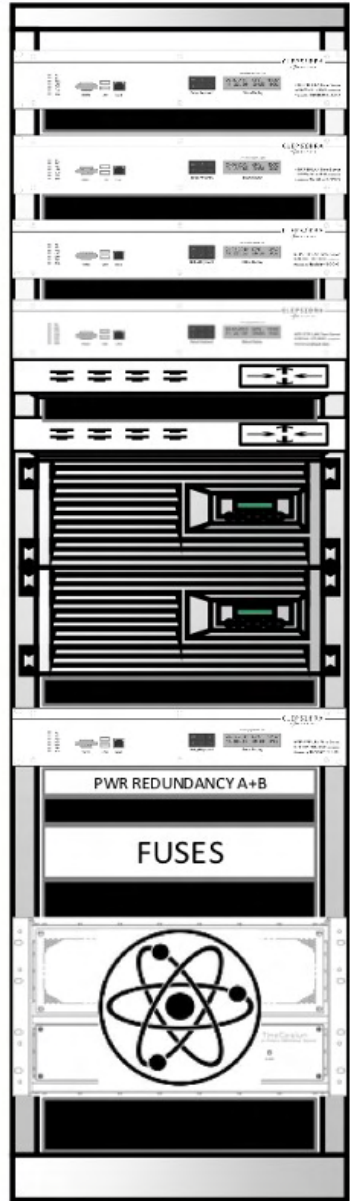
NTS-pico3

The Product Portfolio

- **NTS-pico** the smallest Time Server IEEE1588 for autonomous vehicles
- **NTS-5000** the world most secured Rack"19 IEEE1588 NTP IRIG for IT/OT
- **NTS-infrastructure** the corporation UTC time-scale system for critical infrastructures:

- | | | |
|-----------------------|------------------------------|---------------------------------|
| ➤ <i>Telecom 5G</i> | ➤ <i>Traffic Control</i> | ➤ <i>Space & Scientific</i> |
| ➤ <i>Broadcasting</i> | ➤ <i>TSN/Industry 4.0</i> | ➤ <i>Military</i> |
| ➤ <i>Smart-grids</i> | ➤ <i>Cypher & Crypto</i> | ➤ <i>Datacenters/Cloud</i> |
| ➤ <i>Financial</i> | ➤ <i>ISO27001 Security</i> | ➤ <i>Autonomous vehicles</i> |

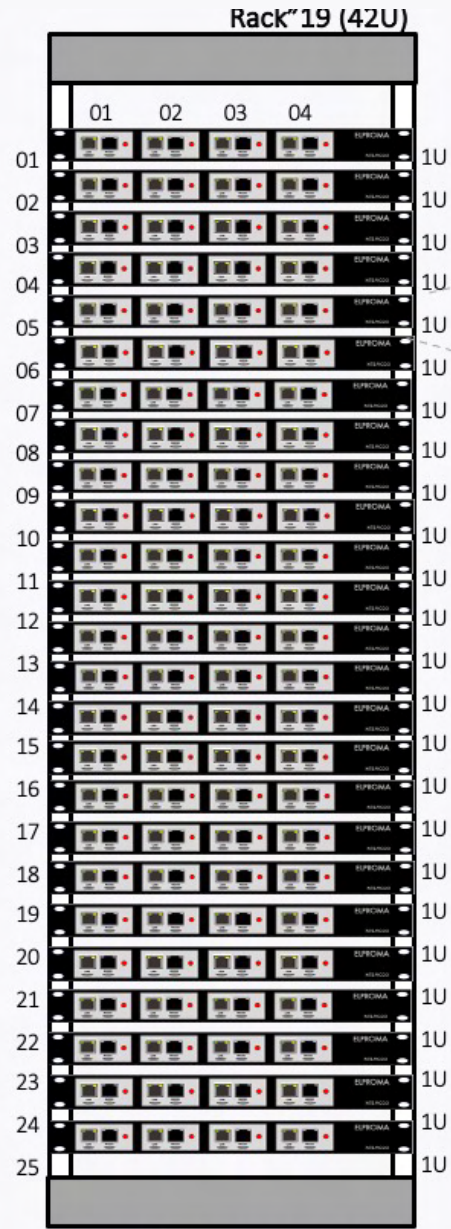




Reference
Time Domain
PPS & ToD



Distribution



100x NTS-pico MATRIX

Dedicated
Time Server for
each user



TaaS – Time as a Service
statistical approach in security at www.ntppool.org



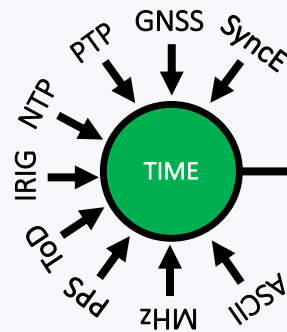
Solving Tech. Problems:

- 1** **Delivering Accurate TIME & DATE to IT/M2M Devices**
=> Is important for applications, databases, operating systems ...
- 2** **Stabilizing Frequency PPS/10MHz of IT/M2M Devices**
=> improves stability of hardware & software (less system crashes)
- 3** **Ensuring Time Domain for distributed IT/M2M Systems**
=> essential for CLOUD & TELEMETRY. Today everything is distributed system ...

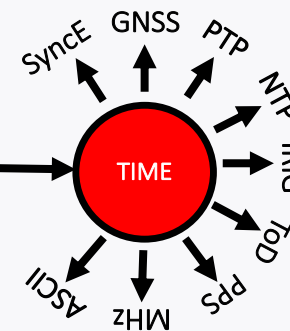
Creating Market Value:

- 4** **Keeping Events Chronology with Non-Repudiation Properties**
=> incl. RFC3161 Cryptographic Stamping prevents frauds and manipulations ...
- 5** **Disseminating TIME & FREQUENCY via Network, incl. :**
=> Ensuring robust ref. UTC to Grandmasters for Industry 4.0
=> Retrieving UTC on SLAVE side => forwarding UTC locally using IRIG, PPS/10MHz
=> Converting any time-code to any (PPS, MHz, IRIG, NTP, PTP, SyncE, ToD, ASCII)
=> Robust time distribution using NTP, PTP IEEE1588 and dedicated profiles incl. (default, telecom, power, broadcast, TSN, High Accuracy HA, White Rabbit)

INPUT TIME
(ref. UTC)



network master/slave device

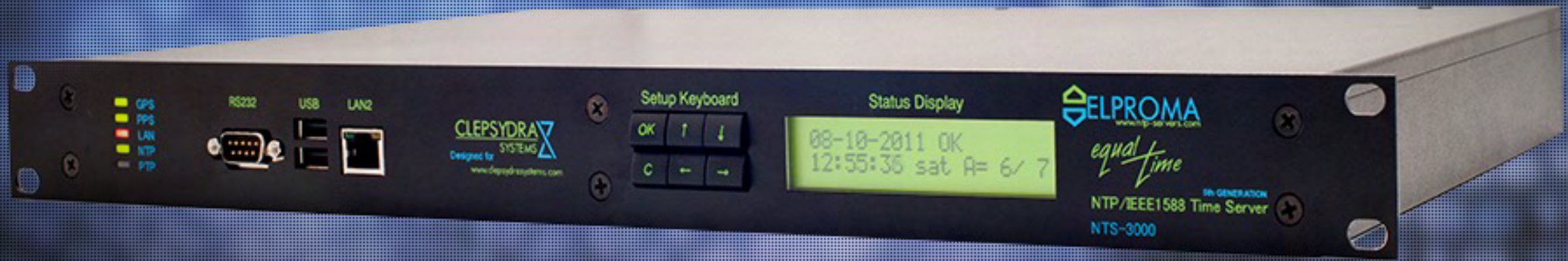


OUTPUT TIME
(retrived from LAN)

Important Note!

Synchronization is niche specialization. Weak synchronization does not block solutions. It is simply limits performance that frequently is not easy to detect and measure. But there are cases where synchronization is responsible for system failures that cost millions US\$. Blackouts cost much more.

Network Timing Cryptographic Time Stamping


1

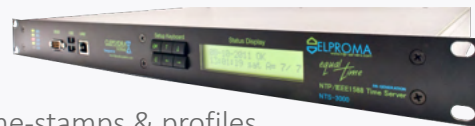
NTS-3000 GNSS (1U) [\(link\)](#)

- Simple NTP, PTP/IEEE1588 software time stamps


2

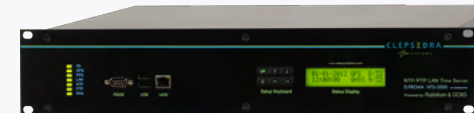
NTS-4000 OCXO (1U) [\(link\)](#)

- All NTS-3000 features
- 2x PTP/IEEE1588* with hardware time-stamps & profiles
- HQ-OCXO holdover oscillator, IRIG-B, 1PPS, 10MHz
- Redundant 2x Power Supply


3

NTS-5000 Rubidium (2U) [\(link\)](#)

- NTS-4000 & NTS-3000 functions, plus extra
- 10x LAN (1GE) w/ NTP, PTP/IEEE1588 hardware nanosecond stamps & profiles
- Quantum Rubidium Oscillator for long-term GPS-less holdover operation
- Top cyber-security with physical isolation between LANs (private PTP IP stack/LAN)


4

NTS-pico3 Ultra Miniature Time Servers

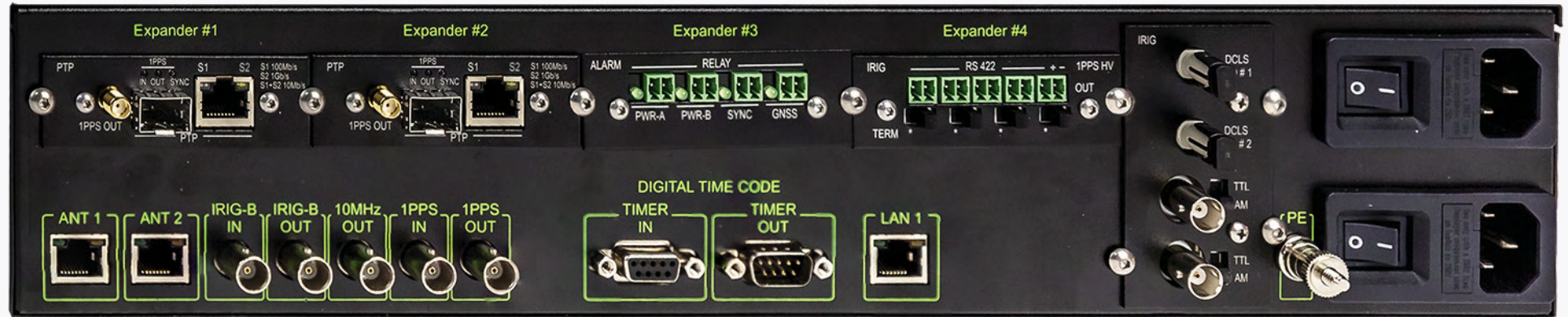
- 1x LAN, NTP, PTP/IEEE1588 software stamps
- Low-cost. Dedicated for industrial mass market use
- All-in-one antenna White Rabbit version
- Low cost SLAVE with CLK retrieving from network


[\(link1\)](#)

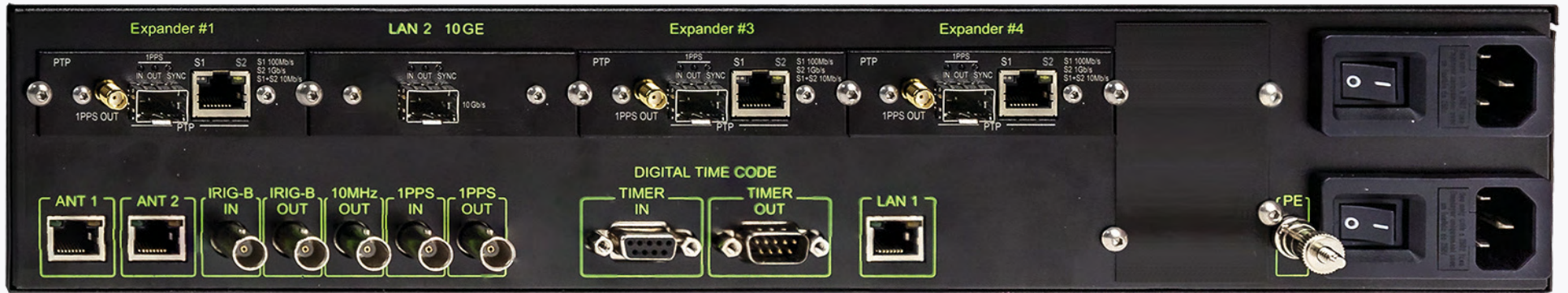
[\(link2\)](#)

Configuration Suitable to
Any Critical infrastructure

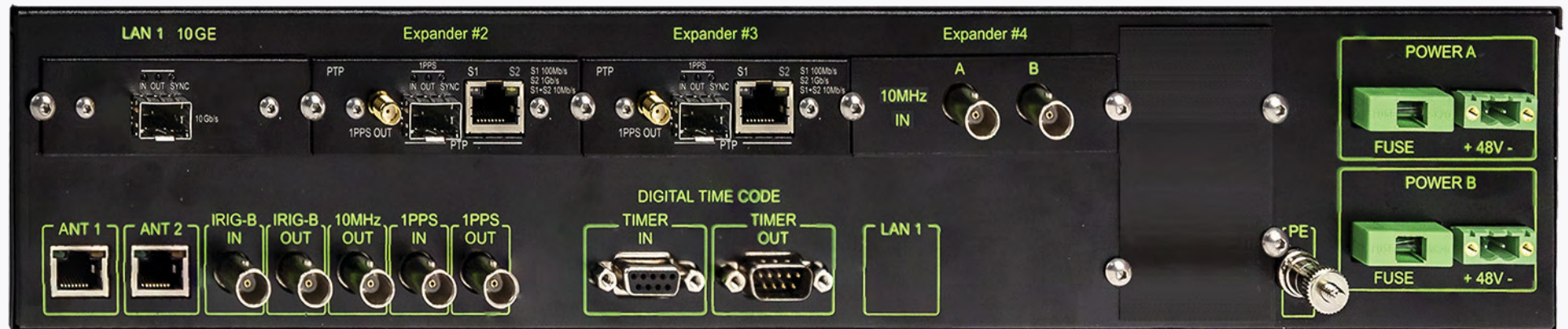
SMART-GRIDS
w/ 1GbE



DATACOM
w/ 10GbE



TELECOM &
BROADCASTING
ePRTC w/ 10GbE



Network Timing Time Domain Operation

Improving robustness of backups,
Prevents weak clustering ...



DATAKOM & CLOUD need the microsecond [μs] accuracy to let clusters operating time & frequency domain. Especially, the synchronization is essential for VM computing and OCP **supercomputers** of Facebook, Microsoft, Google etc. Currently, Equinix datacenters ensures $1\mu\text{s}$ between East and West Coast of USA. Time is conductor for distributed computing acting like symphony orchestra. Chronology of **LOG** events is important for investigating error logic. Time & date is essential for automatic backups and **archives**. At least once per decade each Date Center is experiencing serious crash because of poor synchronization. The SQL database transactions can not be completed and therefore rollback are unexpectedly more frequent. Unstable synchronization reduces **performance**. The leap-second is highly risky for instability of all distributed datacenters and can cause OS crashes.

An aerial, high-angle view of the New York Stock Exchange (NYSE) trading floor. The floor is filled with traders, desks, and computer monitors. Several large, cylindrical structures with "NYSE" logos on top are visible. The image has a halftone or dithered texture. Text overlays are present: "Network Timing MiFID II Compliant" in the top left and "Robust synchronization for MiFID II, eIDAS, MiFIR ... RTS25, FINRA, EMIR ..." in the bottom right, with a white arrow pointing right.


Network Timing MiFID II Compliant

Robust synchronization
for MiFID II, eIDAS, MiFIR ...
RTS25, FINRA, EMIR ...

Stock Exchanges & Banks need a $100 \mu\text{s}$ synchronization accuracy at $1\mu\text{s}$ resolution to ensure FINRA, EMIR, MiFID II. The HFT (High Frequency Trading) matching engines based on sequence need to understand order of trade execution. Software HFT bots need to understand the true common "now" moment for **arbitrage HFT investing**. Therefore the network low latency is important for collocation and must ensure 10mln trading's/1s. Today NYSE/LSE pushes going synchronization down to nanosecond [ns] level. Also, the e-banking, VISA/MasterCard are requiring time for keeping chronology. Here, there is no requirement for high accuracy and the milliseconds are fine. The cryptographic **TSA time-stamping RFC3161** is important for long-term preservation of financial operations.

Network Timing Synchrophasors

Maintains electric power.
IEEE C37.128.1a compliant



Synchronizing IEC61850 substation is important for modern distributed smart-grids. The Elproma ensures 100ns accuracy for IED (Intelligent Electronic Devices – the relays) and PMU (Phaser Measurement Units) according to IEEE C37.238 and IEEE C37.128 standard. *Synchrophazors (PMU)* require better than a 1μs accuracy of synchronization to secure the predictive power distribution management. It enforces IEEE1588 protocol operation in a special **Power Utility Profile**. Elproma supports world leading modern country size smart-grids in Asia.

Network Timing Telecom Lte/5G



Redefining telecom performance
ITU-T G.8275.1 compliant



ITU-T G.8275.1 & ITU-T G.8275.2 profiles ensure new 5G/6G core synchronization for Industry 4.0. They are simultaneously powered by SyncE. New next generation ePRTC/cnPRTC clocks are enabling core node 5G synchronization. The synchronization is also important for BTS (Base Transceiver Station) and for keeping RADIO frequency stable.



Network Timing
Public Administration

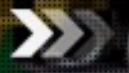
Non-repudiation & Data integrity
Crypto Timestamping RFC 3161

Cryptographic Timestamping RFC3161 (requiring accuracy of part of one second) is important mechanism for the long-term preservation of e-signatures, e-documents (data sealing) ensuring document originality, non-repudiation and authentication. Any place, where the consequences and financial penalties need to be taken into account, the TSA (Time Stamping Authority) providing trusted time stamp is important. The TSA needs synchronization of 1s.



Network Timing
Industry Process Management

From Telemedicine to Robotics,
Improves automatization



We are all living in Industry 4.0, where autonomous robots increases work efficiency. Synchronization is important for predictive maintenance of factory. Today the new standard of TSN (Time Sensitive Networking) and TCC (Time Coordinating Computing) are becoming more and more important. The smart-factory is connected to CLOUD. The EDGE/FOG computing assist Industry 4.0 introducing ML & AI, but distributed systems need stay synchronized.

Network Timing Traffic Management

Ensuring the safety is first
Air railways & air traffic control



Modern CNS (Central Navigation Systems) use clusters operating in UTC Time Domain. It is requiring synchronization accuracy better than a millisecond. For an airplane flying at a speed of about 1000 km/h, the synchronization ERROR of single second defines a position error of 300 meters. Also, a Voice Control Systems (VCS) require trusted timestamping to store pilot conversations and telemetry flight data proving event chronology at non-repudiation.

Network Timing Smart City

Improves security,
Expands remote management

Smart City is an urban area that uses different types of electronic data collection M2M sensors to supply information which is used to manage assets and resources efficiently. This concept integrates information and communication technology (ICT) using Time Sensitive Networking. The various of physical devices from different vendors are connected to the network – and they all are requiring synchronization for TSN operation. The audio & video broadcasting is in use too.

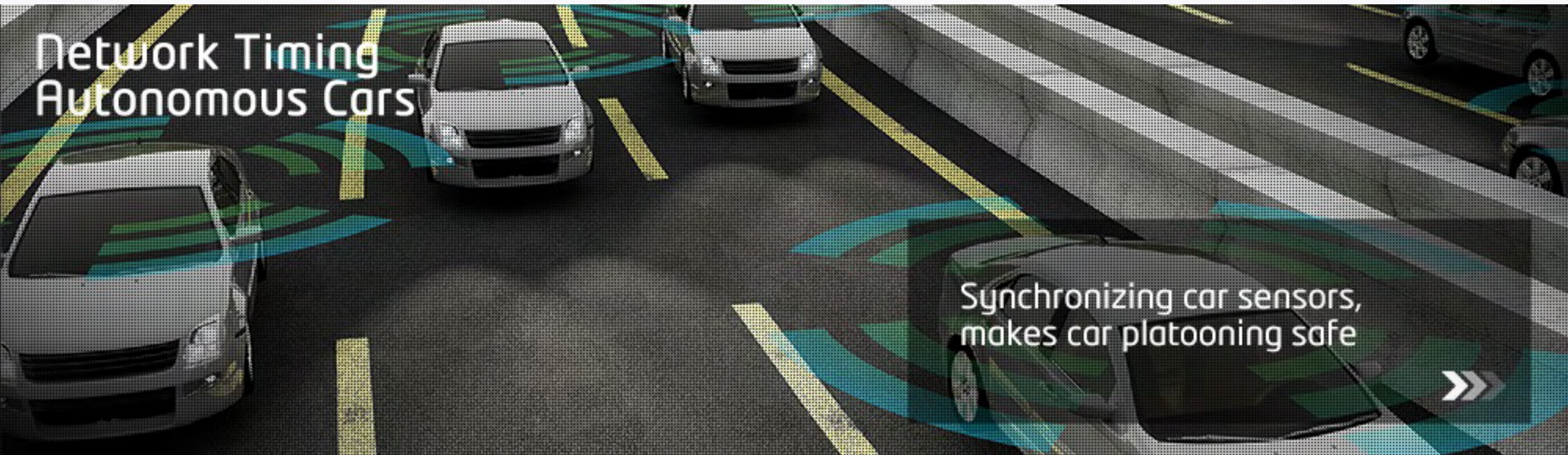


Network Timing
Gaming

From cryptosystems to gaming
RND generation, CCTV timestamping



EGM is an example of devices where synchronization requires each internal module including: computer responsible for the game scenario, support for rhythm and dynamics of the background music, colours and intensity of lighting, payment system and withdrawals that require cryptographic time stamping to prevent forgery. EGM machines work together and exchange information that affects the player, and which remains at the next EGM. CCTV and numerous installed IP sensors constantly monitor the work of the casino to prevent frauds.



Autonomous vehicles synchronization uses nanosecond level and AES67/IEEE 802.1AS PTP profile. Vehicle platooning is part of a suite of features that self-driving cars might employ. A platoon is a group of vehicles that can travel very closely together, safely at high speed. Each vehicle communicates with the other vehicles in the platoon. Modern communication such as Wireless, GNSS positioning, radar/lidars sensing plus drive-by-wire steering and throttle allows for computers to take control of cars – assuming they are all highly accurate and secure synchronized.

Network Timing Blockchain Entropy



Ensures chronology & non-repudiation
for AI-algorithmic, Big Data, Data Mining



Blockchain (BC) gives the ability to store all history of any transaction. It is a continuously growing list of records, which are linked and secured using PKI cryptography. Each block typically contains a cryptographic hash of the previous block, transaction data and a **timestamp**. Records are handled in timestamp order. Usually, the BC does not require accuracy of synchronization, but it strongly depends on stability. By design, a blockchain is inherently resistant to modification of the data. But it therefore has a weak point – the synchronization and time synchronization attack.

Network Timing Cryptography



Supports cyber-security
for Modern & Quantum Computing

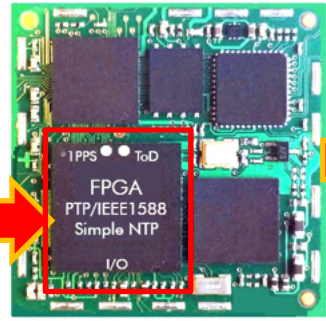


In cryptography, a timing attack is a side channel attack in which the attacker attempts to compromise a cryptosystem by analyzing the TIME taken to execute cryptographic algorithms. It exploits the data-dependent behavioral characteristics of the implementation of a cipher algorithm like RSA. Timing attacks are often overlooked in the cyber-security design phase. Furthermore, the Quantum Cryptography (QKD) uses Time & Frequency Domain for decoding single photon information. Here the accuracy of synchronization is counted in single picoseconds.

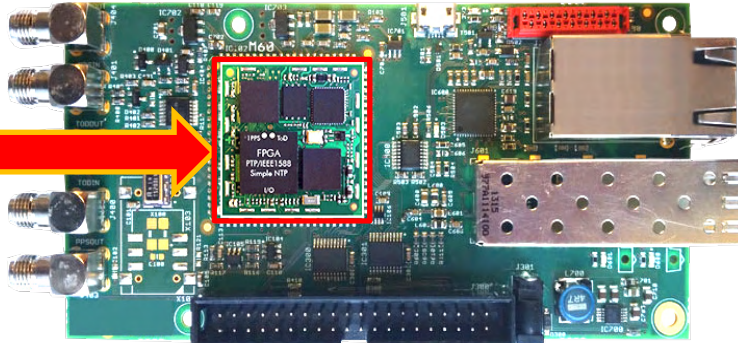
1. IEEE1588 FPGA



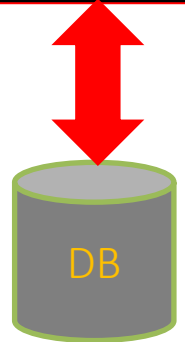
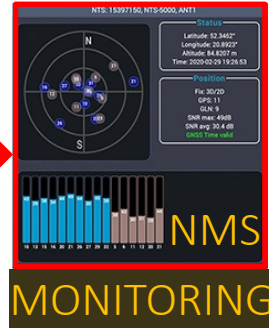
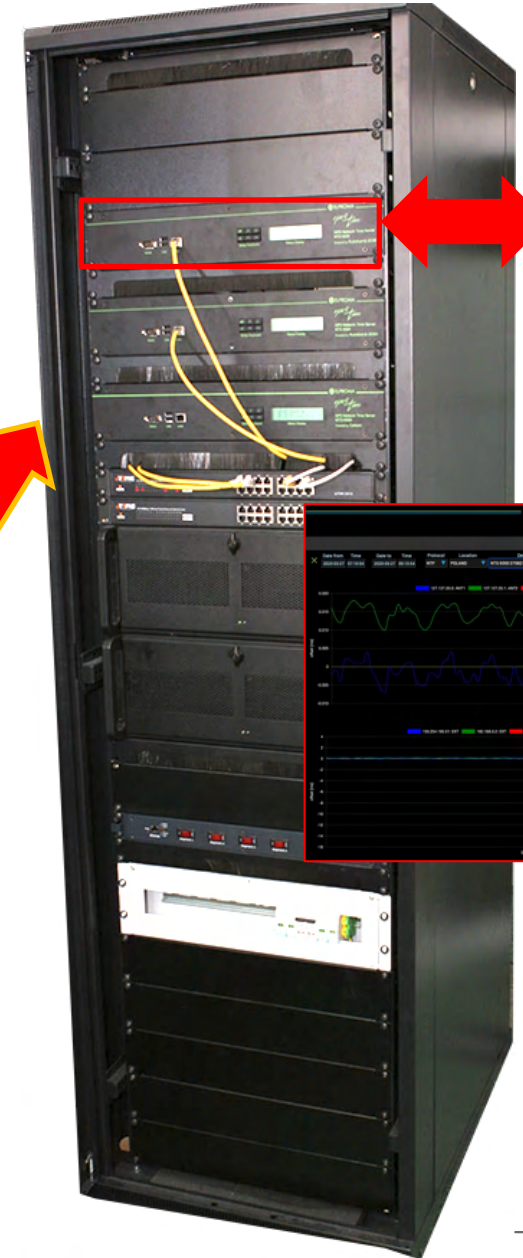
2. EMBEDDED PCB



3. AUTONOMOUS GRANDMASTER NIC



5. TIME DISTR. & AUDIT SYSTEMS



TIME-ARCHIVES

4. TIME-SERVER

a) MASTER

b) SLAVE (RETRIEVING CLOCK FROM NETWORK)



Partial list of organizations which trust ELPROMA technology:

