Faults of Synchronization Based on GNSS Receivers and Ethernet NTP/PTP Network

Robust Synchronization & Cyber-Security In Critical Infrastructure(s) Of SMART-GRIDS

T. Widomski, K. Borgulski, J. Użycki, P. Olbrysz, J. Kowalski (ELPROMA)
e-mail: info@elpromatime.com web: www.elpromatime.com

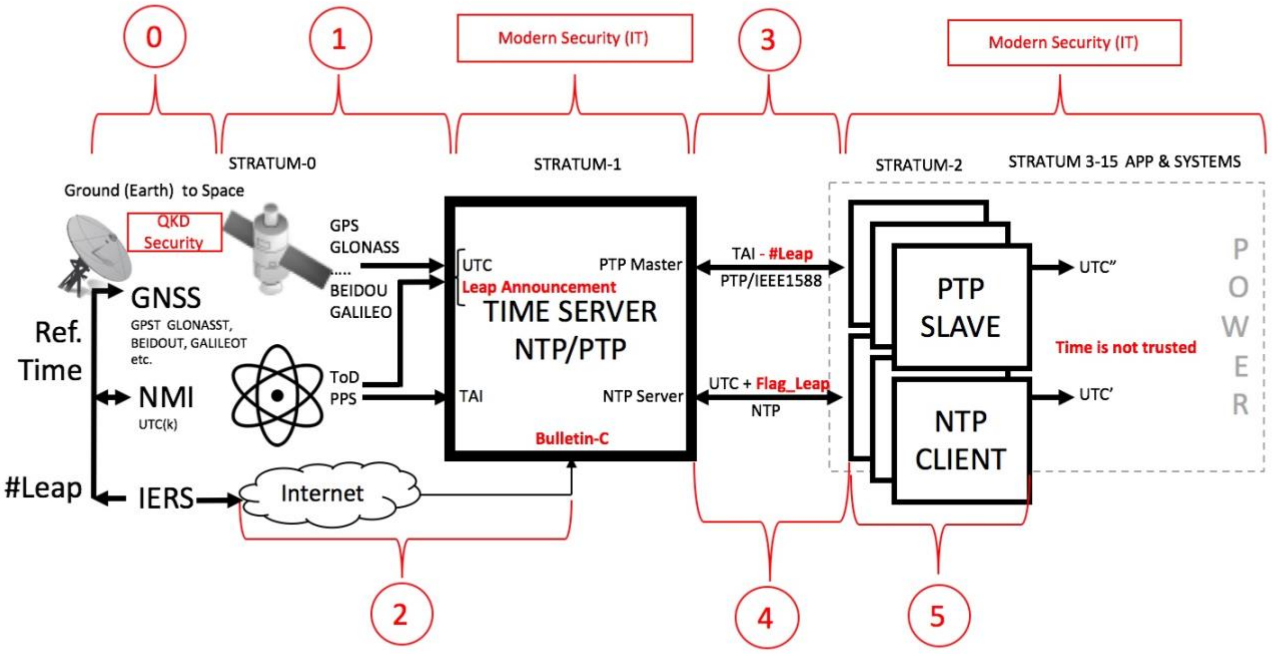


Figure 1 Five stages *of the UTC time distribution in power distribution encumbered with faults and loss of synchronization hazard* (*time gaps*)

BIOGRAPHY

Tomasz Widomski (age 52), a graduate of IT sciences (1990), at the Department of Computer Science of the Warsaw University of Technology. In 2012 he completed postgraduate studies at the Warsaw School of Economics (SGH). Chairman of the Board of ELPROMA[1] (1992-2014). He has joined several EU projects, including one related to GALILEO time services (DEMETRA[2]) and hosted by INRIM[3] , GSA[4]. Earlier he supervised ELPROMA *R&D* team working with CERN on White Rabbit[5] Project - a ultra-high precision PTP (2009-2012).

ELPROMA[1] - a polish manufacturer of the professional NTP, PTP IEEE1588 servers and RFC3161 cryptographic timestamping devices. The company participated in the domestic and international R&D projects, including: CERN White Rabbit PTP and DEMETRA Horizon 2020. Member of TA(PL), the polish group of atomic clock laboratories. The ELPROMA NTP/PTP servers are the most frequently selected products by NMI and other industry areas including: energetics, telecom, financial sector, public administration (www.elpromatime.com).

Figure 2 *ELPROMA Time Server NTS-5000 w/ PTP IEEE1588 "ENERGY" profile*

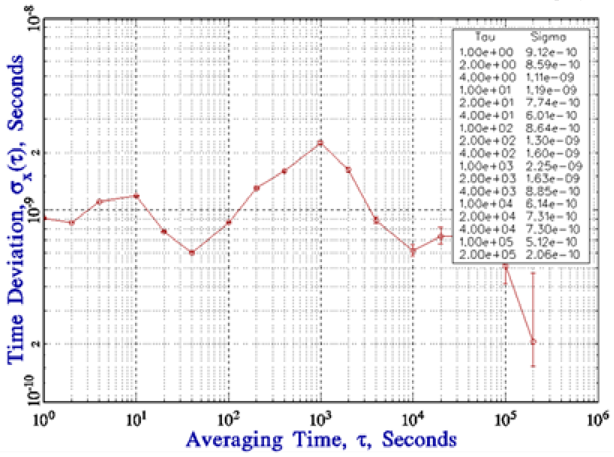


Figure 3 *NTS-5000 average 50ns time accuracy measurement for PTP/IEEE1588. Test performed January 2017 at NPL laboratory London with UTC(NPL) ref.*

[1] ELPROMA http://www.elpromatime.com
[2] DEMETRA H2020 Project https://www.demetratime.eu
[3] INRIM http://rime.inrim.it/H2020-Demetra/
[4] GSA https://www.gsa.europa.eu
[5] CERN White Rabbit (PDF PTTI 2011 link)

INTRODUCTION

In years 2015-2017 the Elproma Company participated in the international project DEMETRA[2] Horizon 2020[4]. The project provided 9 new synchronization time services[6], some supporting the GALILEO system implemented by the EU. In order to execute the entrusted task well, DEMETRA[6] was preceded by numerous market surveys that determined industry demand for the synchronization services. Numerous technical audits were conducted in the area of the EU concerning selected synchronization systems based on current satellite GPS system and the Ethernet TCP/IP network. Their results revealed numerous imperfections of the current working solutions (Figure 1).

Elproma has joined the DEMETRA[4] project as an expert in the Ethernet time distribution protocols: NTP *(Network Time Protocol)* and PTP IEEE1588 *(Precision Time Protocol)*. It was also entrusted with the task of designing a new method of secured time distribution, which could be e.g. used for secured UTC transfer, for legal applications. The conclusions from DEMETRA became the basis for continuation of the *R&D* work in other EU projects.

BRUSSELS DG-ENERGY 2017 WORKSHOP

The DEMETRA conclusions were presented during the meeting on 6th Feb 2017 at DG-ENERGY[7] in Brussels EU. A thesis was formed there by prof. Vaccaro (DEMETRA Team) of a possible successful "*A Time Synchronization Attack*" cyber-attack scenario on the synchronization infrastructure in the Smart Grid energy sector, the result of which could be e.g. a *blackout*. Even though the probability of effectiveness of this attack still seems to be small, experts are disturbed by overlapping circumstances that are conducive to this hazard:

- *terrorism and cyber-terrorism hazards,*
- *geopolitical changes observed during this decade,*
- *low level of awareness of the synchronization role in the strategic sectors of the EU states economies,*
- *numerical (digital) representation of time inside IT devices cause error to be dependent on BIT-weight positions. In such case an error of nanoseconds, seconds, hours, months and years seems to be highly the same equally probable*
- *growing complexity of IT systems interdependdence that can cause a large-scale domino effect,*
- *the niche nature of synchronization means that this segment comprises a small number of experts; it limits the possibility of information exchange on a large scale*
- *lack of alternative solutions, implementing a procedure in the case of occurrence of a cyber-attack on synchrophazors synchronization*

According to the requirements described in documents IEEE [29] [30] , the synchronising should ensure:

1) synchronization in *Time Domain*.
2) providing of 1 microsecond [μs] with the assumption of maximal number of #16 hops (switches and routers) of the Ethernet network. Each hop inputs extra 50 ns of delay on average, which defines the necessity of providing by the time server of the precision at least better than 200ns (200x 10^{-9} second). Only few time server providers meet this requirement including ELPROMA NTS-5000 PTPv2 IEEE1588:2008 with the ENERGY profile and hardware stamping
3) synchronization accuracy of 500 ns for a line state supervision and precise damage location using the *travelling wave* technique

The 1μs accuracy of synchronization is necessary to manage power distribution. The control is performed by a phase angle measurement (Figure 4) and is executed using networking PMU devices (*Phasor Measurement Unit)* determined in standard *IEEE C37.118.1a* (Figure 5)

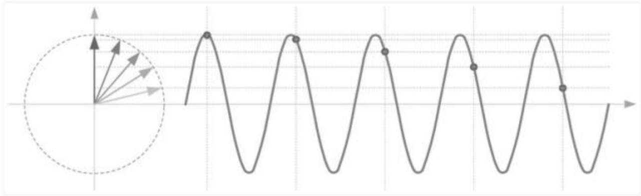


Figure 4 *Phase angle representation in the PMU Synchrophazors*

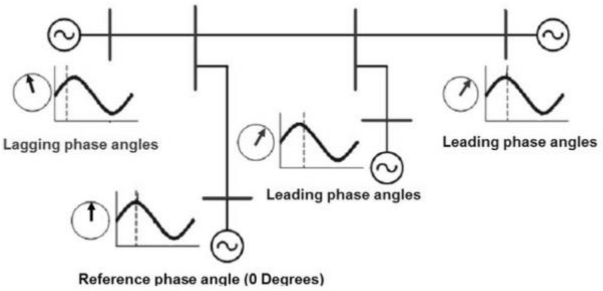


Figure 5 *Phase angle monitoring system used for monitoring power distribution*

This precise synchronization forms the critical parameters of distributing and managing electric power. The current state of the energy network is based on the estimation that is based on the current data readout from the measurement PMU systems. Therefore, the data must be transferred to the control systems with the smallest possible *delay*.

Pieces of information not correlated in time can provide untrue or outdated - invalid data. It can result in taking a wrong decision of redirecting power control and flow of the distributed energy. Especially deviation of the phase angle generates the hazard of a serious energetic breakdown and even a *blackout*. Losing synchronization of the PMU could cause *blackout* similar to one on the East Coast (USA) in August 2003 (Figure 6).

Note, that a time error of 1 μs corresponds to a synchrophasor phase error of 0.022 degrees for a 60 Hz system and 0.018 degrees for a 50 Hz system. A phase error of 0.57 degrees (0.01 radian) will by itself cause 1% TVE. This

[6] The official website www.demetratime.eu INRIM: http://rime.inrim.it/H2020-Demetra/

[7] DG ENERGY http://ec.europa.eu/energy/ (also see the bibliography [42])

corresponds to a time error of ±26 µs for a 60 Hz system and ±31 µs for a 50 Hz system.

Monitoring of energy distribution is executed using the SCADA systems (Figure 7) generating relevant alarms, including especially the ones informing on too large changes of the phase angle. It is equally important to transfer this data with known delay to enable the power distribution operator's reaction without the risk of a blackout breakdown. Delay has seemed to be a main reason of Italian-France-Switzerland September 2003 blackout[8].

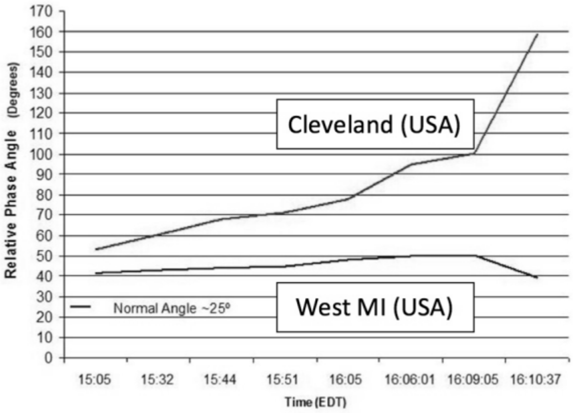


Figure 6 *Recorded blackout on the East Coast of the USA (August 2003)*

The rigour of maintaining these synchronization parameters in the energetics is regulated by the standard *IEC61850-9-2Bus&Station*. According to DEMETRA [42] it is just the fear of an efficient cyber-attack on the synchronization infrastructure that is based on GPS, which causes that until today the largest American management system *WAMPAC (Wide Area Monitoring, Protection, and Control Systems)* remains in the data supervision "read-only" mode i.e. without active control automatics redirecting the power of the distributed energy. This still remains under operator's semi-automatic control.

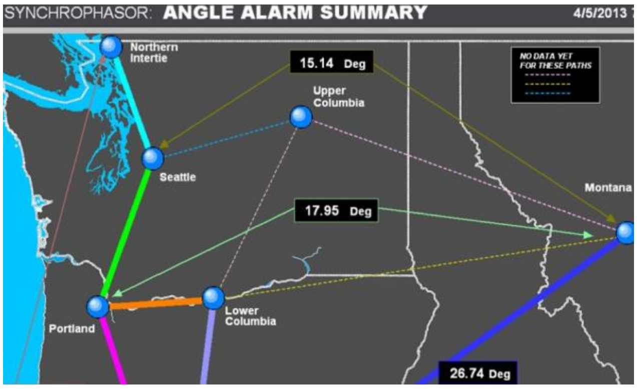


Figure 7 *SCADA monitoring the phase angles in the Boneville Company (USA)*

That is why it is so important to create a failsafe, reliable time distribution mechanism of robust synchronization, the one that unconditionally guarantees maintaining of the rigour of 1 µs accuracy for Power Distribution and Smart Grids. This requirement is described by standards: *IEEE C37.238*, *IEEEC37.128.1* updated later in in 2014 to *IEEEC37.128.1a*.

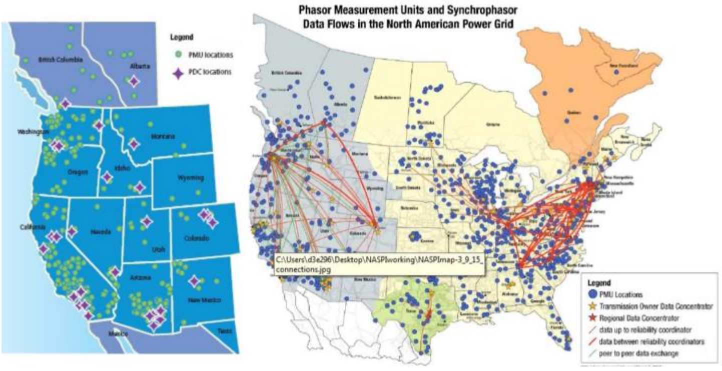

Legend
PMU locations
PDC locations
British Columbia
Alberta
Washington
Montana
Oregon
Idaho
Wyoming
California
Nevada
Utah
Colorado
Arizona
New Mexico
Mexico
Texas
Phasor Measurement Units and Synchrophasor Data Flows in the North American Power Grid
C:\Users\d3e296\Desktop\NASPIworking\NASPImap-3_9_15_connections.jpg
Legend
PMU Locations
Transmission Owner Data Concentrator
Regional Data Concentrator
data up to reliability coordinator
data between reliability coordinators
peer to peer data exchange

Figure 8 *WISP (left side)) – the West Coast area covered with the PMU connection program.* To the right there is the view of the whole energy infrastructure in USA.

All documents describe UTC to be the obligatory time scale. But as described on the next pages of the article, some of today's time transfer standards (e.g.) PTP/IEEE1588 requires/require the TAI time scale, other old IRIG systems might still operate using even *local time*.

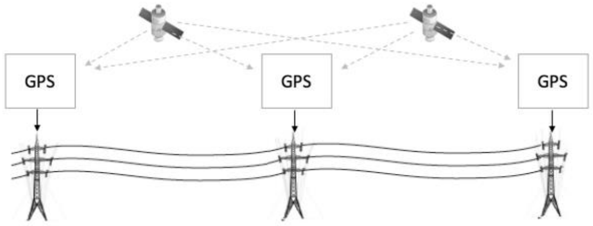


Figure 9 *De-centralised GPS based synchronization system*

Nevertheless, a modern synchronization system needs to provide reference time for a common ***Time Domain*** operation inside the whole power distribution network. Today this can be achieved on two ways described below on Figure 9 and Figure 10. For the time distribution it is also possible to use a mixed hybrid model of these two.

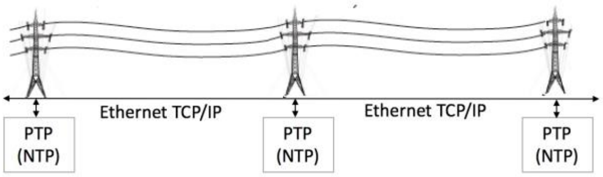


Figure 10 *Centralized time distribution system via the Ethernet TCP/IP network using PTP/IEEE1588 (earlier NTP protocol was in use)*

Each event in the network generating an alarm or warning is recorded in the LOG system with a timestamp (date and time - ToD) of occurrence. Maintaining the chronology of these events requires precise synchronization of all the system elements, including servers, controllers, sensors (incl. PMU) and even the SQL data base system (DB).

In the case of a breakdown, the LOG records will provide necessary information to identify the problem. It is possible only when the system remains synchronised keeping chronology of all events. Preserving of the cause and effect result relations allows to replay the precise sequence of the events and to determine the breakdown cause. Unauthorised changes of the LOG file content or poor

[8] Italian blackout 2003 https://en.wikipedia.org/wiki/2003_Italy_blackout

synchronization render identification of the breakdown cause impossible.

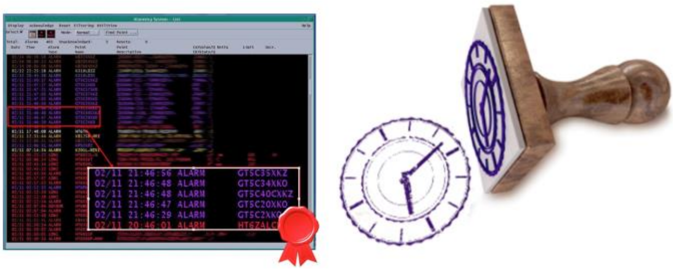
At present the LOG files are protected by the privileged user (e.g. admin) rights and breaking into the system with these rights allows for altering the records (Figure 11). Unfortunately, LOG data is mostly not strongly protected. Cyber-security is simply weak if the following properties are not taken into account:

Authentication -where source of time is cryptographically secured and therefore trusted. Trusted time stamps should be used to keep chronology of all LOG events,

***Integrity* –** a time transfer protocol (NTP/PTP) and a LOG Data, needs to be secured from unauthorized modification,

Non-repudiation means events stored in LOG are in chronology that basis on *trusted authenticated time*. Since LOG data keeps *integrity* (it is private key signed), a *non-repudiation* can be proven for each timestamped even,

Validity is achieved once the PKI electronic certificates are in use too. PKI certificates include more data information: certificate validity date, certificate issuer information and it's usage range. There is private key and *public key* tightly linked to certificate too. The validity of certificates is maintained by CA (Certificate Authority) software tools.



```
02/11 21:46:56 ALARM    GT5C35XKZ
02/11 21:46:48 ALARM    GT5C34XKO
02/11 21:46:48 ALARM    GT5C40CXKZ
02/11 21:46:47 ALARM    GT5C20XKO
02/11 21:46:29 ALARM    GT5C2XKO
02/11 20:46:01 ALARM    HT6ZALC
```

Figure 11 *The event chronology in the LOG reflects the event relations and provides the cause and result sequence necessary to identify the breakdown. Therefore, they should be cryptographically protected using Public Key Infrastructure (PKI)***.**

The synchronization is also used in energy *metering*, *in virtual trading with energy, billing and invoicing*. The synchronization faults do not bring in the direct tailspin risk here though, but they can be the reason of financial loss on different scale.

A certain sub-area of the synchronization in the power distribution that requires much precision of at least 500 ns is also worth mentioning. This precise time is used to measure the *travelling wave* - reaction to the pattern, used to diagnose the state of the transfer lines and to indicate the damaged spots. The larger the clock precision the more precise is the possibility to find the transfer line damage spot. It is applied both for the overhead as well as underground lines (Figure 12).

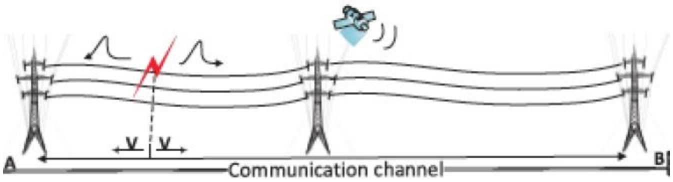


Figure 12 *The travelling wave is locating damages of the transfer line*

The breakdowns in the energy sector exert influence on other branches of the industry and especially on: industry, telecommunication (TV/radio/Internet), financial sector, public administration, transportation and in towns on water mains and sewage system, street traffic control, railway traffic, air traffic control, etc. Each larger breakdown in the energetics carries a risk of periodical destabilisation of some region. Planned surgeries are cancelled at hospitals, work of the public services is subject to numerous difficulties. Social unrest is stimulated by disinformation caused by the lack of communication and overwhelming darkness after sunset. The prospect of difficulties in accessing ones funds/bank accounts only intensifies the predominating uncertainty.

Due to these reasons the energy sector remains within the interest of groups of hackers and is exposed to attacks.
A new challenge is the protection of the energy infrastructure, which is sensitive to the results of desynchronization.

FIVE RISK GROUPS OF ERROR ARISING

During the process of time transfer the risk of synchronization error occurrence appears in the following five stages that are demonstrated on the drawing (Figure 1) on a very first page of this article:

<u>stage 0</u> – Ground Base System (sending data to satellites)
- ***internal GNSS errors***
- ***military nature of** some of GNSS systems like GPS, GLONASS, BEIDOU does not guarantee time service availability to all global civil markets*

<u>stage 1</u> – Space to GNSS receiver transfer
- ***jamming of GNSS signals** (GNSS Jamming)*
- ***on earth simulation of GNSS signals** (GNSS Spoofing)*
- ***lack of leap second handling** (Leap Second)*
- ***internal errors of GNSS satellite receivers***
- ***multi-second differences of satellite time scales: GPST, GLONASST, BEIDOUT, GALILEOT etc.***

<u>stage 2</u> – file transfer via the public Internet network
- ***lack of cryptographic file protection** e.g. bulletin-C EIRS, gives a possibility of manipulation with time based on a file substitution (no private key signature),*

<u>stage 3</u> – time transfer via the Ethernet and NTP protocol:
- ***lack of the leap second announcement signal***
- ***influence of the network asymmetry***
- ***deliberate introduction of delays** (e.g. Time Delay Attack)*

<u>stage 4</u> – transfer via the Ethernet PTP/IEEE1588:2008
- ***lack of authentication** of the data sent by the protocol*
- ***UTC complex representation** (TAI **-** #Leap Seconds)*
- ***deliberate introduction of delays** e.g. Time Delay Attack*
- ***random traffic load** increase a queue delays*

<u>stage 5</u> - hardware level internal transfer
- ***system diversification OS and firmware software***

(UTC time support, differences in the way of handling of the leap seconds)
- ***errors and delays of OS API asymmetry*** *(firmware)*
- ***human errors*** *(configuration settings, PTP profiles, etc.)*
- ***compatibility errors*** *(compatibility) PTP/IEEE1588*
- ***time scale errors*** *(representation of: UTC, POSIX, TAI)*

The scale of the synchronization error may vary in range from nanoseconds even up to whole seconds and even days and years. It is related to the numeric time representation (various weights of the particular bits representing time) when the generally known factors such as temperature or stability of network delays normally give reasonably small errors. Numeric overflows or unexpected network traffic usually generates random high-level time errors.

SYNCHRONIZATION ERROR SOURCES

1. Jamming & Spoofing GNSS

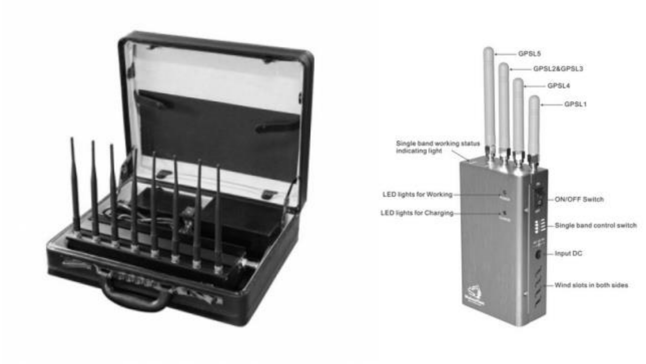


Figure 13 *Devices for jamming GNSS signals are currently adjusted precisely with the frequency and band to the beam type and even to its encrypting way*

Jamming means the ability of local "overpowering" of original GNSS satellite signals with inexpensive, but very effective devices available for sale e.g. in the Internet shops. Effectiveness of operation of the GPS jammers depends on the power of the transmitter. Contemporary jamming devices are perfectly adjusted to the frequency of the satellite signal and the jamming signal emitted by them more frequently takes into consideration the advanced properties of specific GPS carriers L1-L5. The effectiveness of jamming depends on RF transmitter power, terrain shape, town planning and satellite receiver location.

Not a long time ago, about a decade back in time, their use in the synchronization segment was accidental. Numberless instances of use were so poorly documented that it was difficult to tell the difference between deliberate real jamming from the influence of electromagnetic noise interferences. At present the use of jamming devices becomes more and more popular. Today USA and EU records incidents with their use more and more frequently.

So far as the clock #1 (Figure 14) does not have alternative for the GNSS ways of obtaining UTC ref. (e.g. from NMI and remotely accessible NTP/PTP servers), its time will gradually degrade itself depending on stability of the local holdover oscillator, giving more and more incorrect indications in respect of the UTC.

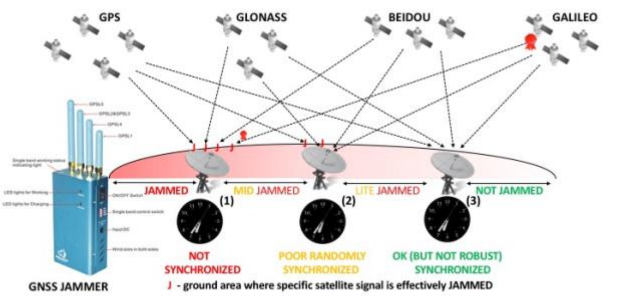
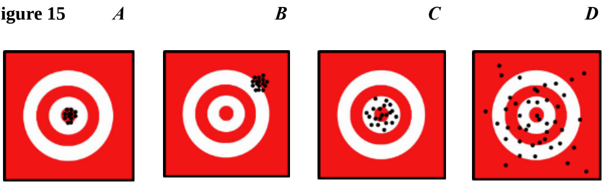

GPS
GLONASS
BEIDOU
GALILEO
JAMMED
MID JAMMED
LITE JAMMED
NOT JAMMED
(1)
(2)
(3)
NOT SYNCHRONIZED
POOR RANDOMLY SYNCHRONIZED
OK (BUT NOT ROBUST) SYNCHRONIZED
GNSS JAMMER
J - ground area where specific satellite signal is effectively JAMMED

Figure 14 *Effectiveness of the GNSS jammers range depends on the transmitter power. In the field marked with red colour (left part) GPS reception is impossible. In the central part the reception is random and occasional and in its part to the right there may occur problems with the GPS reception and therefore with synchronization too.*

If the clock features high quality oscillators (e.g. Rubidium) installed in than the degrading process (the UTC error increase rate) may be slowed down until the GNSS satellite signal reception is restored. For this to take place the oscillators must synchronise themselves to GNSS or remotely to NMI prior to this. This operation mode of the operation is called the *holdover* mode. Depending on the oscillator stability and the requested synchronization accuracy the UTC time in the *holdover* mode can be maintained (e.g. for 1μs): minutes (TCXO), hours (OCXO), or even days (Rubidium). The important and necessary to be fulfilled condition is keeping power supply and not resetting the clock (NTP/PTP server).
The oscillator unsynchronised with the GNSS works in the *FreeRun* mode providing stable frequency of the signal but not granting the UTC phase synchronization.
Synchronization and its error can be illustrated using shooting butts, the centre of which symbolizes the reference UTC (Figure 15).

Figure 15



Accurate & Stable (Sync or Holdover) — *Stable but not Accurate (FreeRun)* — *Accurate but not Stable* — *Not Accurate and Not Stable*

Clocks and NTP/PTP servers without installed *holdover* oscillators react immediately to GNSS jamming and introduce a large clock drift.

Spoofing GNSS depends on faking the satellite signal beam in order to enter the receiver into the position error and time error. Selected GNSS systems (e.g. GALILEO) foresee introduction of new protection mechanism against this kind of hazard. At present the spoofing devices remain expensive enough for the probability of their use to be much smaller than the use of the jammers. Spoofing is much more danger than jamming. Commercial GNSS receivers are not able to recognize spoofing and therefore they synchronize local oscillators to false reference of time.

There are 3 ways to prevent GNSS spoofing:

I. **The UTC ref. time diversification** (*Method 1*). Depending on simultaneous use of larger number than 3 of UTC sources (independent one from another) and the time transfer methods. The time signals can be obtained simultaneously (Figure 16):

a) from many GNSS receivers
b) from remote NMI clocks via Ethernet
c) locally from the holdover oscillators (OSC)

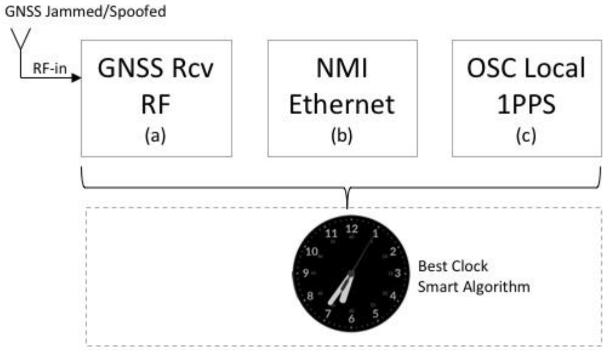


Figure 16 *Best Clock out of several available ref. UTC sources*

II. **GNSS firewall** (*Method 2*) is now available as *commercial product*. It is implementing a special case of diversification *Method 1* (above). It is ready to use "box", that neutralizes spoofing (frequently GNSS jamming too) by providing a "clean" simulated RF output signal (Figure 17).

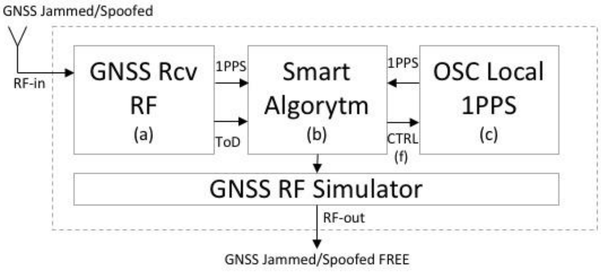


Figure 17 *GNSS firewall block scheme*

In the case of spoofing, as in the instance of jamming risk, diversification in simultaneous use of many independent ref. UTC sources is important. Diversification of the ref. time supplying method is no less important too (Figure 19). Both jamming as well as spoofing can also be identified using special devices. Some of them can even show the direction, from which the jamming signal transmission is coming (Figure 18).

Figure 18 *Device identifying jamming and showing the direction of its source*

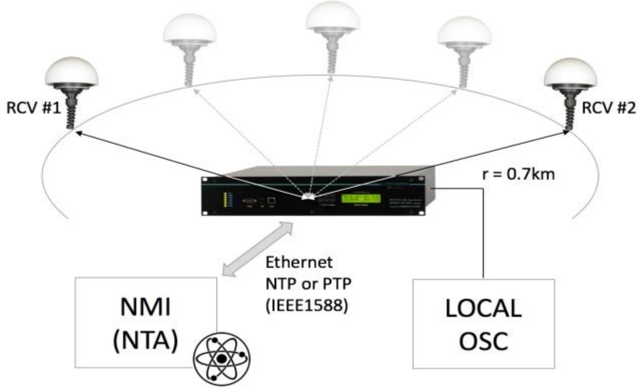


Figure 19 *Two separate GNSS receivers (each based on different GNSS chip supplier) located within the radius of 0.7km from the ELPROMA NTS-5000-time server minimalize/ minimise the effectiveness of GNSS jamming and spoofing. The fake GNSS signals can be identified and rejected if the server uses simultaneously alternative sources and methods of the time supply.*

III. **Advanced GNSS receiver** (*Method 3*). It is new concept so-called *Trusted Synchronization Node*.

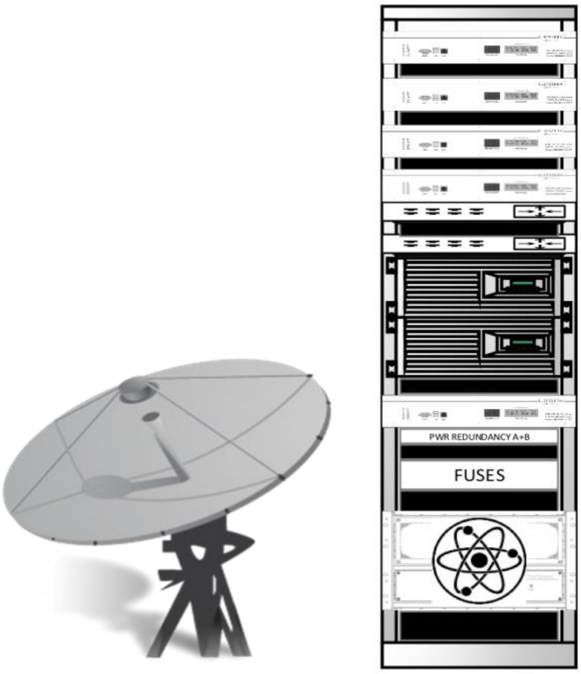


Figure *Trusted Synchronization Node (Method 3) equipped with advanced GNSS receiver, high performance holdover oscillators (Cs, H-maser, Rubidium), and multiple standard NTP/PTP IEEE1588/IRIG-B time transfer standards.*

This method is distinguished by the fact that it uses technologically very advanced (frequently custom built) GNSS receivers, and therefore it is expensive too.

In practice, *Method 3* can be enriched with non-commercial GNSS-firewall devices described above, (*Method 2*) provided assuming that the devices used will be positively verified for cyber security. However, if *Method 3* is specifically limited to a competent satellite system (e.g. GALILEO) and uses its functional extensions (e.g. QKD – a Quantum Key Distribution or single photon, entanglement protection) devices such as GNSS-firewall will not be necessary. A *Trusted Synchronization Nodes* should be considered to cover specific region of town, country side, country. It should be equipped with high accuracy oscillators Cs/H-maser/Rubidium to perform autonomous holdover operation in case of GNSS internal errors, advanced jamming and spoofing attacks. Trusted Synchronization Nodes also should provide multi-standard synchronization outputs incl. NTP, PTP IEEE1588, IRIG.

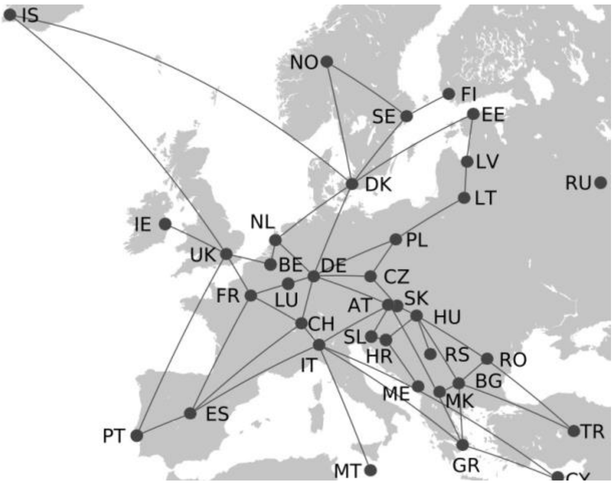


Figure. *Trusted Synchronization Node theoretical model basing on GEANT network structure*

Disadvantages of methods 1-3:

Method 1 implementation is time consuming, requiring experience, experts and access to NMI clock resources.

Method 2 (GNSS firewall) is simple ready to use commercial solution. Its advantage is the ability of to track multiple GNSS (GPS, GALILEO, GLONASS, BEIDOU, QZSS, IRNSS) simultaneously. It also tracks multiple carriers L1-L5. Its disadvantage is the requirement of replacing exiting GNSS receiver by putting a commercial GNSS firewall on the front of the connection chain (Figure 20).

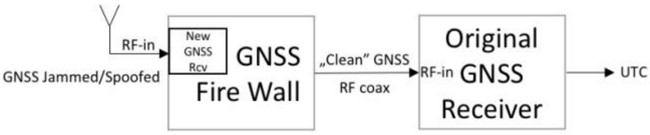


Figure 20 *Connection data flow (left to right). GNSS firewall is first in line (left) before original GNSS receiver (right), which now receives "clean" spoofing/jamming free, but a simulated GNSS RF signal.*

Furthermore, a commercially available product brings a risk of including *Trojan horse and Back door* when using, and therefore they should be well tested for cyber-security scheme (Figure 21).

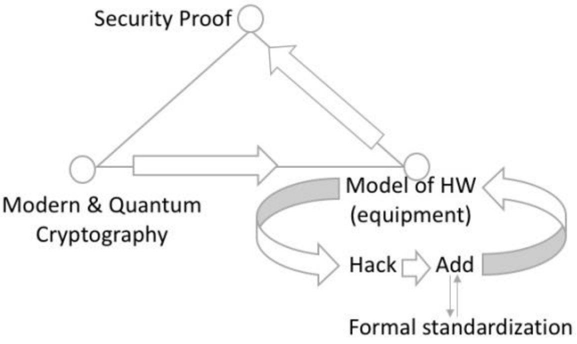


Figure 21 *Implementation security of synchronization system*

Method 3 (*Trusted Synchronization Nodes*) is requiring state (UE) level investment for each country (city).

2. Lack of resistance of commercial GNSS receivers to external GPS, GLONASS etc. system errors

The UTC error case known as SVN23[9] occurred on January 26th 2016. The internal error of the GPS satellite system input into the commercial receivers on Earth the error of 13.5µs in respect of the UTC time maintained correctly by the remaining GNSS systems like GLONASS, BEIDOU, and GALILEO and the NMI metrology institutes that had atomic clocks. The 13.5µs was invisible even by the multi-satellite GNSS receivers because the GPS is still most frequently the leading base satellite system. A part of the receivers on Earth could demonstrate other errors, e.g. smaller than 13.5 µs. This error was registered but not multiplied by the national metrology institutes (NMI) that had their own atomic clocks not dependent on GPS.

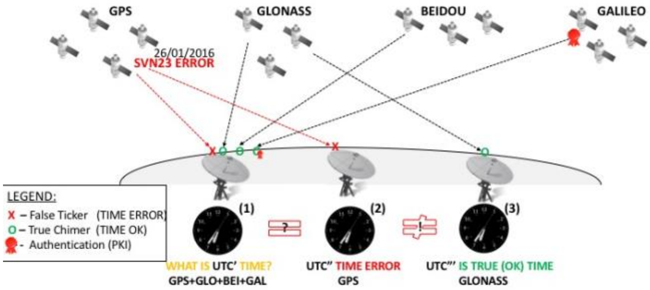


Figure 22 *Internal errors of the particular GPS, GLONASS, BEIDOU, GALILEO systems can introduce an error such as e.g. GPS SVN23 of 26/01/2016*

In the case of the GPS 13.5 µs SVN23 error it destabilised for many hours the operation of the IT systems, which was described in the media (e.g. BBC[10]). The size of the error, even though apparently small, threatened the stability of the energy and telecom sector exceeding max. permissible UTC time error. The SVN23 instance demonstrated that the GPS system was not failsafe. Perhaps UTC offset could be larger if the error concerned more significant bits of the data records representing the time numerically represented inside the GPS satellite system.

The results of the SVN23 errors do not differ from GPS spoofing symptoms and constitute exactly the same problem to be solved. In order to detect such an error, it is necessary to have access to the other independent UTC ref. source that is not burdened with an error. The national metrology institutes (NMI) have at their disposal such reference time sources that are independent from the GPS and other systems from GNSS group.

The results presented in on (Figure 23) of the 13.5µs deviations laboratory tested at NMI[11], of different GPS receiving devices (a colour is allocated to the particular measurement of different device – Figure 23) demonstrate that the tested receivers and GPS servers react with variable delay and inertia to the same SVN23 error.
It proves unexpected additional time differences between the specific GNSS receivers, which would not occur if the receivers were identical, even though still susceptible to the same GPS SVN23 error. The above once more prompts to think over construction of solutions, which would be able

[9] GNSS Inside (SVN23) http://www.insidegnss.com/node/4829

[10] BBC http://www.bbc.com/news/technology-35491962

to obtain the standard UTC time from the independent sources and with the methods independent of each other e.g. like: GNSS (RF), NMI (Ethernet) and local OSC.

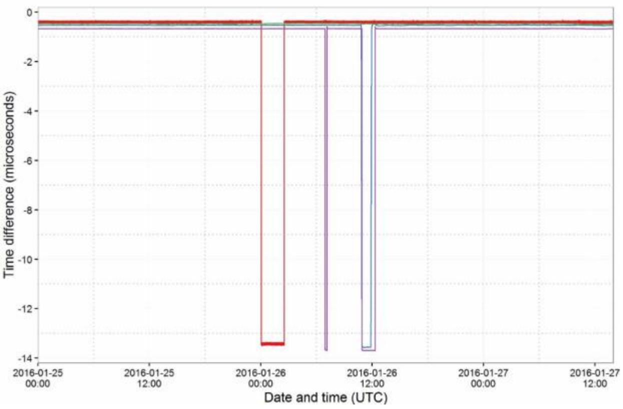


Figure 23 *The 13.5 µs error plot published from Metsahovi Radio Observatory – Technical Report Document*[11] *- release Aalto University (A")*

3. Multi-second time divergence between the timescales GPST, GLONASST, BEIDOUT, GALILEOT[12]

It is said colloquially the "*time from the GPS*", but in practice it almost always concerns the UTC time scale. Inaccurate terms and jargon, however, may lead to an error resulting in multisecond divergences in the range from 18 to 37 second (status quo Feb 2018), differing one from another with the GPST, TAI time scales and the UTC scale.

A little-known fact is that the particular satellite systems of the GNSS group use time scales internally differing one from another for many seconds[10]: GPST, GLONASST, BEIDOUT, GALILEOT (*the T extension meaning time*). These scales are rendered accessible as an option of the commercial receivers (output time) setting. Wrongly set they can render accessible on the output of e.g. a PTP/NTP server the time with a multi-second error in respect to the expected UTC.

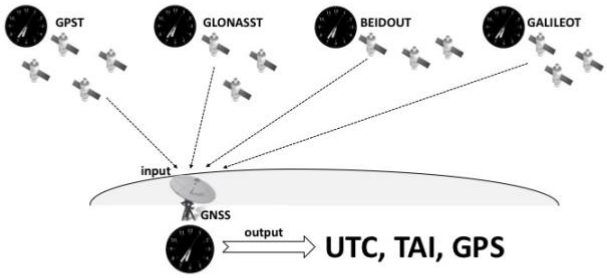


Figure 24 *Time of the receiver OUTPUT and the GNSS server can be expressed in the UTC, TAI or GPST and other time-scales*

The resulting UTC time received on the output of the satellite receiver is calculated in this particular receiver. Receivers (e.g. GPS) are frequently treated in the way similar to a LAN network interface card (NIC) i.e. as if they received the time from a satellite and transferred it further on to the IT system. Is is a large simplification.

In order to determine the correct UTC time, the receiver must not only receive and decode the information from the satellite, but also it must also take into consideration a number of mathematical corrections related to the satellite movement (e.g. time dilatation resulting from the Einstein's special relativity theory, microwave carrier beam propagation in the atmosphere etc.).

The final quality (exactness and precision) of the UTC time produced by the GNSS commercial receiver internally depends on the algorithm implemented in the firmware, hardware efficiency (clocking frequency, processor architecture, available memory size, sensitivity of radio-receiver etc.) The receiver can either weight in favour (e.g. GPS) or diminish the role of the particular other systems of the GNSS group increasing or decreasing their weights during averaging of the UTC determining. The algorithm and values of the weights always remain confidential information of the OEM manufacturer and are not indicated in the technical specification of a commercial GNSS receiver.

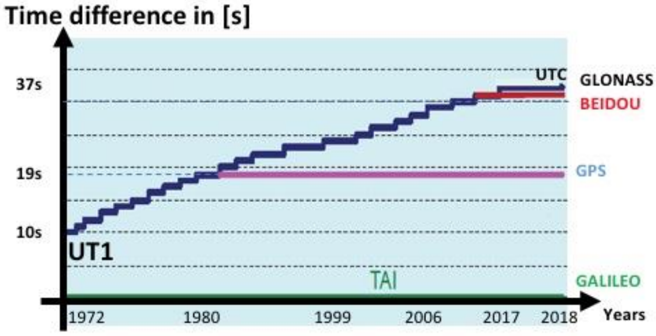


Figure 25 *Historical evolution of the time scales*

Conclusion! *One should not think, though, that an e.g. American company manufacturing commercial GNSS receivers can guarantee its customers that the output UTC will be dependent on GPS time, unless this is clearly written on product that it does.*

4. GNSS receivers – PPS error

It could seem that it is impossible, when struggling for high precisions of synchronization expressed in nanoseconds, microseconds, milliseconds, to fall easily into a much larger error trap of even one second. The "*one second trap"* is related to a correct connection of two output signals generated inside the GNSS receiver: 1PPS-out (frequency) and information ToD-out (phase) of the ref. UTC.

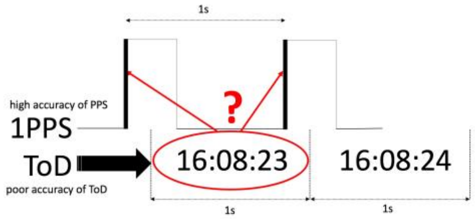


Figure 26 *Which of the 1PPS signal (left or right) determines correctly the beginning of the ToD hour 16:08:23*

The 1PPS (*pulse per second*) is a very precise frequency reference determining the beginning of a second in the UTC time-scale. It corresponds to a pendulum in a

[11] Metsahovi Radio Observatory - GPS Time Disruptions on 26-Jan-2016

[12] NAVIPEDIA
http://www.navipedia.net/index.php/Time_References_in_GNSS#GPS_Time_.28GPST.29

gravitational clock. The PPS does not include information about the hour, minutes or the number of seconds. This information is indicated by ToD (*time of a day*) and it is completed with the Gregorian calendar information (year, month, day). The reason for the possibility of a "*one second trap" error* occurrence is the difficulty to allocate the correct 1PPS slope to a correct ToD marker (Figure 26). The synchronization failures and time divergence errors related to it should be explained by a poor cooperation between groups of engineer's and time experts. When one group assumes failsafe operation of the purchased GNSS receivers the second group thinks that the presented problem is obvious and clear for anyone. Unfortunately, this problem also affects the most reputable companies manufacturing GNSS devices, an especially risky situation is related to *leap second* support.

5. Leap Second

The reason for implementation of an additional *leap second* is slowing down of the rotary movement of the Earth that has been observed for many years. In theory the rotation could also speed up, but it has not been observed so far.
A correction helps to maintain the relation of the UTC time scale and the astronomical time that has been watched. The last 37 leap second was added at UTC midnight 31/12/16.

The decision to add or deduct a leap second is taken (and announced) many months in advance by IERS (International Earth Rotation Service). The information is published in the form of a *bulletin-C* file[13]. There are two permissible scenarios (Figure 27) of adding or deducting of the leap second:

Scenario 1
30 June time 23:59:60 UTC

Scenario 2
31 December time 23:59:60 UTC

Scale dependence formula UTC-TAI

$$\boxed{\textbf{TAI - UTC} = \textbf{\#Leap-Seconds}}$$

Figure 27 *Scenarios of changes of the leap second and TAI-UTC dependence*

There also exist two spare scenarios (3,4), not used until now, of changes with dates: 31 March and 30 September.

But, the PTP/IEEE1588 distribution protocol transfers via the network only the UTC scale components in the form of: *TAI time* and a number of leap seconds (*#Leap-Seconds*), which must be deducted from the TAI, in order to obtain the UTC time on the client side (called *PTP-slave*).

The synchronised PTP client merges the data received with the PTP/IEEE1588 protocol data himself according to the formula transferred to (Figure 27) and thereby transfers to the PTP-Slave side full responsibility for correct calculation of the definite UTC time in the client system. It can be performed on the level of the network interface, an application (APP) or inside of the kernel.

In any case this approach seems to be hazardous and can lead to arising of one second time differences resulting from various methods of losing the leap second. The PTP/IEEE1588 protocol also does not provide cryptographic authentication of the time information transferred via the Ethernet network, which forms a safety gap allowing for changing of the protocol data (e.g. the *#Leap_Second* parameter). Probably the resistance to these situations is not taken into consideration in the energetics.

For above reasons and to avoid risk of losing synchronization of (IEEE C.37.118.1a) there is not clear written recommendation to use TAI, while all other computing (including LOG event reporting from Synchrophazors) must use UTC.

The NTP protocol demonstrates the UTC time ready for use without detailing the components *TAI and #Leap seconds (as it does the* PTP/IEEE1588). The NTP protocol announces only the change of the leap second, which is to take place to prepare the NTP client system to lose one second.

The announcements of the leap seconds can be supplied both via the satellite GNSS systems and via the TCP/IP (Bulletin-C file) Ethernet network as well as via the announcement flag in the NTP and PTP/IEEE1588 protocols. However, in each case the client (NTP-client, PTP-Slave) side and his operating system or the device firmware are responsible for handling the leap second internally. The following ways to handle the leap second are possible:

1) ***Turning back of the client's system time by 1 second at the end of the leap second***, so in a new UTC day the same second 00 will appear before second 01 appears.
2) ***Turning back by 1 second in the beginning of the leap second*** (similar as in p.1 above), but second 59 will be repeated before new second 00 appears,
3) ***Stopping for 1 second*** of the client's clock
4) ***Stopping of the UTC clock with simultaneous minimal increase of time counters and stamps contents.*** *This smooth losing of one second does not cause time leaps.*

The IT systems in the energetics originating from different decades differ with the methods of handling the leap second (points 1-4). It may cause occurrence over 1 second error in the intervals from 12 hours before to 12 hours after the UTC midnight during handling of the leap second.

Lack of the cryptographic PKI authentication (protection of the bulletin-C file[14]) brings in the risk of changing of the whole file with the data concerning the number and schedule of the leap second changes. It leaves a major cyber-security gap in the IT systems security system using this file and can be used to desynchronise the whole IT system. The content of the file is in the truth protected with the SHA abbreviation function, but lack of the PKI

[13] IERS Bulletin-C: ftp://hpiers.obspm.fr/iers/bul/bulc/

[14] https://hpiers.obspm.fr/iers/bul/bulc/ntp/leap-seconds.list

authentication, e.g. in the form of a digital signature with a *private key* of IERS deteriorates substantially the synchronization safety when using automatic download of bulletin-C file. Then the lack of *authentication* of the PTP (IEEE1588) protocol and the fact of transferring with the protocol of the information split into its components (*TAI and #Leap-Sec)*, might bring the same result: a change of the leap second number. Due to the above-mentioned reasons the correct and collision free handling of the leap second for the sake of cyber-safety remains one of the most difficult challenges for the IT and NMI community in this and in the following decades. Therefore, it is important to implement the necessary legal regulations standardising the principles of handling this second in the IT systems. Handling of the leap second can be accompanied by a number of side effects. Some of them can lead to not deterministic behaviour of controllers/sensors and even of the entire IT systems. It is illustrated by the case described as: https://access.redhat.com/solutions/154793

6. Destabilization of the operating system (firmware) from UTC processing on the OS kernel level

The legible time and date presentation format known from displays (Figure 28 - upper part) is formatted in upper layers of the operating system. The deeper we go into the kernel (OS kernel) the more canonical appearance is taken by the time representation of the unique time marker represented with a number. A change of the number reflects time passing and special counters are responsible for this change that are closely related to the definite architecture and hardware (systems, PMU controllers, etc.). The time in the form of markers has a less legible form, but it allows for representation of the time with very high definition and precision (Figure 28 - left column). Process management (concurrency) and task management (multithreading) are related to *serialized unique time markers*. During handling of the leap second the display presented as the 61 second (Figure 28 - the upper central column in red), inside of the operating system OS is handled differently.

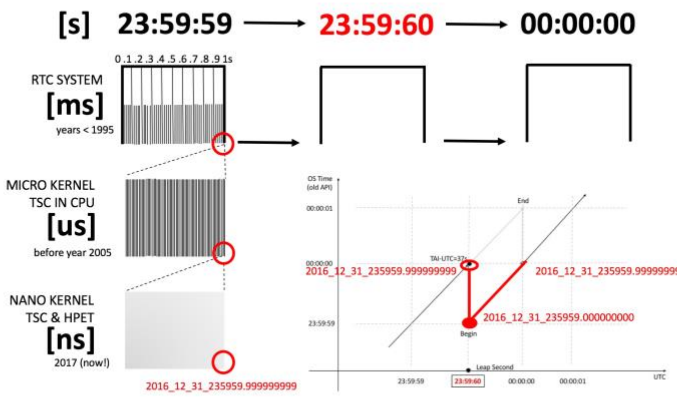


Figure 28 Time handling inside the operating system. Turning back of the client's clock (e.g. leap inserting of a second replicates events, which should not be executed twice).

After rescaling, the system goes back in time, causes repeated execution of a certain number of time markers (Figure 28 - right side, a lower part of diagram). It can cause undesirable second execution of actions. In certain cases, such as e.g. in the case of the Linux Redhat[14] system it can destabilize operation of the whole operating system (OS deadlock, kernel panic etc.).

The problem is much wider than handling of the leap second. It concerns all of the clock resets, except API calling. Turning back the system time is especially dangerous. We draw attention to this, because it seems that this action is natural in the synchronization process.

7. Time Delay Attack

The Marvell[15] Company presented a theoretical model of an attack in the network, depending on the introduction of deliberate delays (Figure 29**Error! Reference source not found.**) of synchronization NTP and PTP packages on the level of the migration and *round trip*. This attack cannot be stopped with the contemporary security protection methods because even encrypted packages are subject to delay and their content is not subject to any modification. Probably the only effective counter measure method can be in the future the quantum cryptography of the whole fibre-optic network infrastructure.

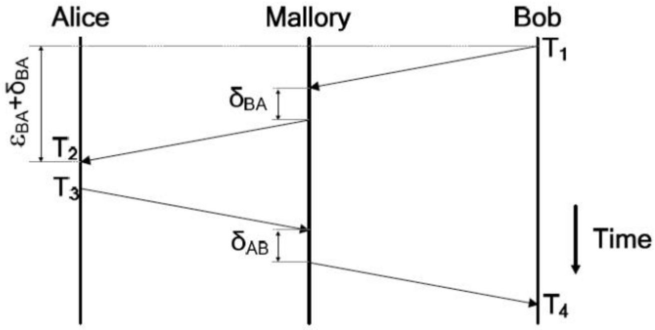


Figure 29 Mallory delays transfer of NTP/PTP synchronising packages between Bob (Slave) and Alice (Master)

HIDDEN WEAK SIDES OF SYNCHRONIZATION

Site visits of the existing GPS installations disclosed many very simple imperfections. Excessive numbers of the GNSS aerials installed on roofs closely to electrical devices, without the full sky view, very often close one to another, installed on lightning installations not only disturb their operation but also make an easy target for GNSS satellite signal jammers. The system audits performed demonstrated the picture of installation not resistant to GPS signal fading away (no holdover). The problem is also lack of continuous simultaneous operator's monitoring of so many satellite GNSS receivers. Personnel poorly trained in respect of the monitoring and operation of the receivers requires periodical training, but first of all there is lack of implemented proceeding procedures in the cases of no synchronization or synchronization loss. It is necessary to check the currently possessed installation immediately.

[15] Tal Mizrahi (Marvel) http://ieeexplore.ieee.org/document/6336612/

SYNCHRONIZATION IMPROVEMENT

In order to assure a reliable synchronization, a robust, reliable UTC ref. time source is necessary and the auditor's supervision of the efficiency of synchronization on the side of the client's applications. This approach will gain importance in the with the increase in synchronization precision. It is very important to provide a larger number number of UTC model sources independent of each other, from which the system can choose by itself the best ref. time sources and reject the faulty ones. It takes a long time to create the systems resistant to disturbances, assessing the quality of the received time model coming simultaneously from: GNSS, NMI and local oscillators. For the new European satellite GALILEO system there appears an important mission of increasing the role of the GNSS, which today is created mutually by the military systems like: GPS, GLONASS, BEIDOU.

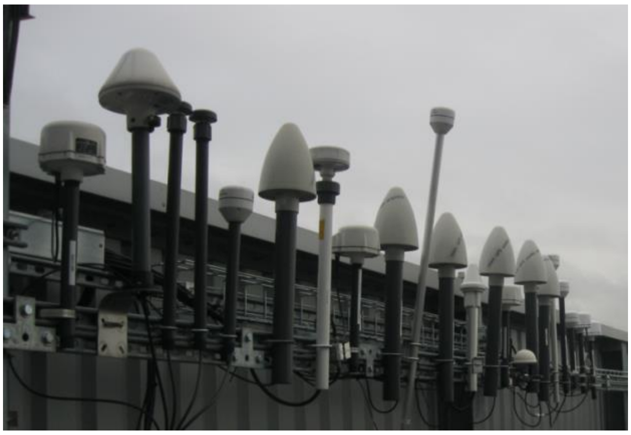


Figure 30 The example of a faulty *installation: the receivers installed too close one to another, disturb one another and are connected to the lightning installations. Photo provided by Chronos (UK) and presented during IFTS 2016 Prague meeting.*

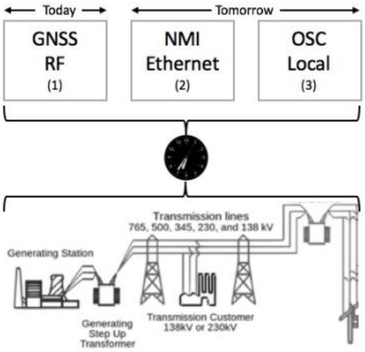


Figure 31 *The synchronization model based on 3 groups of independent time providers. Each group has a different method of time providing.*

The efficient, complimentary to the GNSS and GALILEO source of the UTC are the NMI and their remote clocks.

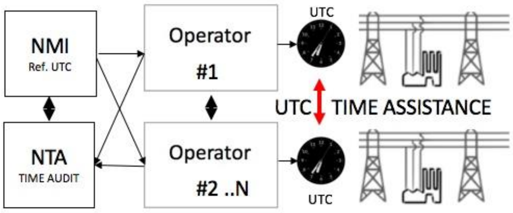


Figure 32 *Model of time distribution and audits in the energy distribution system, in which the particular operators give one another UTC time reserve*

In the future the energy distributors will no doubt organize themselves and form their own UTC time reserve reference and distribution centres. These centres should be formed in cooperation with the NMI and remain under their substantive supervision. The centres will be equipped with high quality clocks and the NTP/PTP servers providing compliance of synchronization with the domestic UTC(k) reference. The centres will be able to collect time simultaneously from the GNSS and NMI (Figure 31) and will support one another (Figure 32) in providing a reserve of the UTC model time of high quality. The solutions like these should be able to recognise the false time providers (*Falsetickers*) and to exclude them from the UTC suppliers group (similar to a virus quarantine concept). The first systems like this have already been established in the world.

Synchronization should also become the component of the energy safety strategy, even though *blackout* breakdowns occur rarely. Awareness of the risk of an efficient cyber-attack on the synchronization infrastructure, which anyway by its nature is not free from faults (which is presented in this article) gives a new insight into energy safety. The risk of synchronization destabilisation in the energetics grows with the evolution of the contemporary energy systems to the form of the *Smart Grid - the intelligent electric power network, in which there exists the two-way communication between all the participants of the energy market.* Its objective is to provide new energy telecommunication services assuring lowering of the infrastructure maintenance costs. It is also to promote development of widely understood environment friendly energy. *The Smart Grid* allows for simultaneous connection to the main of the renewable energy sources of the new generation. It can trigger a domino effect though, if it is not provided with *Robust Synchronization.*

Tomasz Widomski
in behalf of Elproma Time Team
(www.elpromatime.com)
February 2018

Acknowledgement

Special thanks to *Bill Marshal (Chronos UK)* and *Janusz Uzycki (Elproma)* for all comments.

Bibliography

[1] P. Tavella and DEMETRA consortium, “The Horizon 2020 DEMETRA project: DEMonstrator of EGNSS services based on Time Reference Architecture”, Metrology for Aerospace (MetroAeroSpace), 2015 IEEE Benevento 2015, DEMETRA http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7180634

[2] G.Daniluk (ELPROMA), T.Wlostowdki (CERN) “White Rabbit” The sub-nanosecond synchroniza-tion for embedded systems Precise Time and Time Interval Systems and Applications (PTTI), Long Beach, CA, USA, 14-17 November 2011 http://www.clepsydratime.com/file_upl/PDF/Seminaria/Elproma%20CERN%20%28White_Rabbit%29.pdf

[3] A.E. Wallin, T. Fordell, J. Myyry, P. Koponen, M. Merimaa, “Time Transfer in a Wide Area White Rabbit Network”, 28th European Frequency and Time Forum, 23-26 June 2014, Neuchâtel, Switzerland.

[4] M. Lipinski, “White Rabbit: a PTP application for robust sub-nanosecond synchronization”, IEEE ISPCS, 35-30, 2011.

[5] P. Defraigne, F. Roosbeek, A.Somerhousen “Sertting Up a NTP Server at Royall Observatory of Belgium”, PTTI 2004

[6] W. Aerts, G. Cerretto E. Cantoni and J.-M. Sleewaegen, “Calibration of Galileo signals for time metrology”, IEEE transactions on UFFC, 12/2014 61(12):1967-75.

[7] P. Defraigne et al, "Advances on the use of Galileo signals in time metrology: calibrated time transfer and estimation of UTC and GGTO using a combined commercial GPS-Galileo receiver", in Proc. of the Precise Time and Time Interval Systems and Applications (PTTI), Bellevue, WA, USA, 3-5 December, 2013.

[8] P. Defraigne, W. Aerts, E. Pottiaux, Monitoring of UTC(k)’s using PPP and IGS real-time products, accepted in GPS solutions,19 (1), p. 165–172, 2015. doi : 10.1007/s10291-014-0377-5.

[9] P.Waller, F.Gonzalez, S.Binda, I.Sesia, I.Hidalgo, G.Tobias, P.Tavella, “The In-orbit Performances of GIOVE Clocks”, IEEE Transaction on Ultrasonics, Ferroelectrics, and Frequency Control, Volume 57, issue 3, March 2010, pp. 738-745.

[10] L. Galleani, P. Tavella, “Detection and identification of atomic clock anomalies”, Metrologia, Vol. 45 Issue: 6, Pages: S127-S133, December 2008.

[11] I. Sesia, L. Galleani, P. Tavella, “Application of the Dynamic Allan Variance for the Characterization of Space Clock Behavior”, IEEE Transactions on Aerospace and Electronic Systems, Volume 47, issue 2, April 2011, pp. 884-895.

[12] Network Time Foundation http://www.networktimefoundation.org/

[13] Network Time Protocol (NTP) site http://www.ntp.org

[14] Precision Time Protocol sites:
PTPd https://github.com/ptpd/ptpd
Linux PTP Project
http://linuxptp.sourceforge.net/

[15] SyncLab RADclock http://www.synclab.org/radclock/

[16] P.Tavella I. Sesia, G. Cerretto, G. Signorile, D. Calonico, R. Costa, C. Clivati, E. Cantoni, C. De Stefano, M. Frittelli, V. Formichella A. Abadessa, A. Cernigliaro, F. Fiasca, A.Perucca, S. Mantero,
T. Widomski, J. Kaczmarek, J. Uzycki, K. Borgulski, P. Olbrysz, J. Kowalski, P. Cerabolini, L. Rotiroti, E. Biserni, E. Zarroli, V. Leone M.T. Veiga, T. Suárez, J.Diaz, P. Defraigne, N. Ozdemir, Q. Blaire
M. Gandara, V. Hamoniaux E. Varriale, Q. Morante V. Dhiri, E. Giulianini , M.Mangiantini A.E. Wallin
L. Galleani D. Hindley
European Project DEMETRA: Demonstrating Time Dissemination Services, PTTI 2016

[17] Elproma (CLEPSYDRA) Time Server site: http://www.clepsydratime.com

[18] European Securities and Markets Authority (ESMA), MiFID II regulations https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir

[19] Spanner: Googles’s Globally-Distributed Database http://static.googleusercontent.com/media/research.google.com/en//archive/spanner-osdi2012.pdf

[20] D. Mills Computer Network Time Synchronization: The Network Time Protocol on Earth and in Space, Second Edition 2nd Edition (CRC Press)

[21] Jean-Loup Ferrant, Mike Gilson, Sebastien Jobert, Michael Mayer, Laurent Montini, Michel Ouellette, Silvana Rodrigues, Stefano Ruffini *Synchronous Ethernet and IEEE 1588 in Telecoms: Next Generation Synchronization Networks (Willey)*

[22] Peter Rybarczyk Expert Network Time Protocol (APress)

[23] David Deeths, Glenn Brunette Using NTP to Control and Synchronize System Clocks (SUM Press)

[24] Mills, D.L. Public key cryptography for the Network Time Protocol. Electrical Engineering Report 00–5-1, University of Delaware, May 2000. 23 pp.

[25] Mills, D.L. Clock discipline algorithms for the Network Time Protocol Version 4. Electrical Engineering Report 97–3-3, University of Delaware, March 1997, 35 pp.

[26] Mills, D.L., and P.-H. Kamp. The nanokernel. Proc. Precision Time and Time Interval (PTTI)

Applications and Planning Meeting (Reston, VA, November 2000).

[27] Mills, D.L., J. Levine, R. Schmidt and D. Plonka. Coping with overload on the Network Time Protocol public servers. Proc. Precision Time and Time Interval (PTTI) Applications and Planning Meeting (Washington, DC, December 2004), 5–16.

[28] Mills, D.L. Improved algorithms for synchronizing computer network clocks. IEEE/ ACM Trans. on Networks 3, 3 (June 1995), 245–254.Mills, D.L. Precision synchronization of computer network clocks. ACM Computer Communication Review 24, 2 (April 1994)

IEEE STANDARDS (*Power System Applications)*

[29] IEEE C37.238 (2011) page 18

[30] IEEE C37.118.1 (2011)
IEEE C37.118.1a (2014)

[31] P. Tavella, I. Sesia, G. Cerretto, G. Signorile, D. Calonico, E. Cantoni, C. De Stefano, V. Formichella, R. Costa, A. Cernigliaro, F. Fiasca, A.Perucca, A. Samperi, P. Defraigne, N. Ozdemir, M. Gandara, P. L. Puech, V. Hamoniaux, E. Varriale, Q. Morante, **T. Widomski**, J.Uzycki, K.Borgulski, P.Olbrysz, J.Kowalski, P. Cerabolini, L. Rotiroti, A. Simonetti, A. Colombo, V. Dhiri, E. Giulianini, M.T. Veiga, T. Suárez, M.Mangiantini A.E. Wallin, L. Galleani, D. Hindley, "The Horizon 2020 DEMETRA project: DEMonstrator of EGNSS services based on Time Reference Architecture", presented at IEEE International Workshop on Metrology for Aerospace, June 2015, Benevento, Italy and available on IEEExplore.

[32] P. Tavella at All DEMETRA consortium formed by Aizoon, ANTARES, CNES, Deimos, ELPROMA, INRIM, Metec, NPL, ORB, Politecnico of Torino, Thales Alenia Space , UFE, Vega UK, and VTT, "The European project DEMETRA: demonstrating time dissemination services", presented at ION Precise Time and Time Interval Meeting Jan 2016.

[33] T. Widomski, J. Uzycki, K. Borgulski, J. Kowalski, R. Bender, P. Olbrysz, "Trusted Time Distribution with Auditing and Verification facilities Project TSI#2", submitted to Precise Time And Time Interval Systems And Applications Meeting January 2016, Monterey, California

[34] P. Tavella at All DEMETRA consortium formed by Aizoon, ANTARES, CNES, Deimos, ELPROMA, INRIM, Metec, NPL, ORB, Politecnico of Torino, Thales Alenia Space , UFE, Vega UK, and VTT, "The European project DEMETRA: demonstrating time dissemination services", presented at ION Precise Time and Time Interval Meeting Jan 2016.

[35] I. Sesia, P. Tavella, G. Signorile, A. Cernigliaro, F. Fiasca, P. Defraigne, L. Galleani,“ First steps towards a Time Integrity Service for EGNSS systems, in the DEMETRA project”", poster presented at the 30th European Frequency and Time Forum, April 2016.

[36] P. Tavella at All DEMETRA consortium formed by Aizoon, ANTARES, Deimos, ELPROMA, INRIM, Metec, NPL, ORB, Politecnico of Torino, Thales Alenia Space , UFE, Vega UK, and VTT, "Time Dissemination Services: The Experimental Results of the European H2020 DEMETRA Project", paper presented at the IEEE International Frequency Control Symposium, May 2016, New Orleans (Louisiana).

[37] J. Delporte, D. Valat, T. Junique, FX Marmet, "Progress on absolute calibrations of GNSS reception chains at CNES", ", paper presented at the IEEE International Frequency Control Symposium, May 2016, New Orleans (Louisiana).

[38] DEMETRA Consortium, "The European Project DEMETRA, Timing services based on European GNSS: First experimental results", presented at IEEE International Workshop on Metrology for Aerospace, June 2016, Florence, Italy.

[39] DEMETRA Consortium, "DEMETRA a time service demonstrator", presentation presented at International Timing & Sync Forum, Prague, 1-3 November 2016.

[40] Pascale Defraigne, ORB On behalf of the DEMETRA consortium "Demonstrator of Time Services based on European GNSS Signals: The H2020 DEMETRA Project," paper presented at ION PTTI 2017 Conference, January 31 - February 2, 2017, Monterey, California.

[41] E.Varriale, Q. Morante, Thales Alenia Space Italia S.p.A, "Synchronet service demonstration results in demetra h2020 project: a scalable high performances synchronization solution", paper presented at ION PTTI 2017 Conference, January 31 - February 2, 2017, at the Hyatt Regency Monterey, Monterey, California.

[42] Tavella, Voccaro, Widomski, "Security Aspects Related To Synchronization At Power Gird" DG-Energy, EC Brussel Security

[43] T.Widomski "Robust Synchronization, Trusted Time Distribution With Audit And Verification Facilities" ESMA MiFID London/UK 28th of Feb 2017

[44] T.Widomski, K.Borgulski, J.Uzycki, P.Olbrysz, J.Kowalski (Listopad 2017)
„Wiadomosci Elektrotechniczne" str. 49-52

[45] T.Widomski, K.Borgulski, J.Uzycki, P.Olbrysz, J.Kowalski (Listopad 2017)
„Elektronik" str. 82-84

[46] T.Widomski, K.Borgulski, J.Uzycki, P.Olbrysz, J.Kowalski (Grudzień 2017)
„NoiS – Napędy i Sterowanie" str. 40-51