CYBERBEZPIECZEŃSTWO
REDEFINICJA ZAGROŻEŃ

POD REDAKCJĄ NAUKOWĄ
BOLESŁAWA SZAFRAŃSKIEGO

Cybersecurity – Redefining Threats

Under the scientific editorship of
Bolesław Szafrański

Wojskowa Akademia Techniczna
Military University of Technology

Cybersecurity – Redefining Threats
Chapter 12

Underestimated Threat – Source and Distribution of Time

Wiesław Paluszyński - Polish Information Processing Society (PTI)
Tomasz Widomski – ELPROMA

1. Introduction

There is a well-known anecdote recounted by Marek Abramowicz in the 1980s in Parisian Culture. It tells of how, in 1925, Polish Radio began broadcasting its program and at noon provided a time signal accurate to half a second from the astronomical observatory in Krakow. This high level of precision made a strong impression both domestically and abroad. The editorial office of one newspaper sent a journalist to Professor Tadeusz Banachiewicz to find out how astronomers knew when it was noon with such fantastic accuracy. Professor Banachiewicz explained how simple it was by saying, "I set my watch every morning on my way to work by passing by the shop window of a watchmaker who offers the best Swiss watch brands. Using the indications of my watch, I strike the anvil precisely at noon, and this signal is broadcast by Polish Radio throughout the country."

The journalist went to the watchmaker's shop to ask the seller where he knew how to set the clocks in the window with such high precision and heard the answer: "Every day, I turn on the radio, and at noon, Professor Banachiewicz provides the information with an accuracy of half a second about when it is noon, and I set my clocks accordingly."

No matter how amusing this anecdote is, it contains a very profound truth: there is no other method of verifying the accuracy of time shown by clocks than comparing their indications with each other[1]. Therefore, synchronization always requires a trusted, accurate reference source, and tampering with it will have far-reaching consequences for the security of people and machines.

Nearly 100 years later, in the 21st century, the importance of synchronization has started to play a particularly crucial role, changing the cybersecurity paradigm of highly automated and distributed infrastructure overly dependent on GNSS. It became such an important issue for the stability of ICT systems in the era of Industry 4.0 that in February 2020, US President Donald Trump signed a special directive, EO13905[2], recommending that American critical infrastructures become independent of GPS. It turned out that instead of breaking security protected mathematically by Public Key Infrastructure (PKI),

[1] Stanisława Bajtlik „What is time", https://youtu.be/BGE_kn1aM80.

[2] US Federal Register – The Daily Journal US Presidential Executive Order EO13905, https://www.govinfo.gov/app/details/DCPD-202000071.

it was much simpler to destabilize the infrastructure by manipulating the time delivered from GPS satellites and desynchronizing it. The EO13905[2] directive covered all branches of the US industry, forcing many changes and hence investments in new technologies, including alternative satellite PNT systems (e.g., Xona Space, Iridium, etc.) and encrypted Internet connection synchronization services with atomic time standards in NIST. This article addresses the types of threats associated with the desynchronization of critical infrastructures, as listed in Table 1.

Table 1. Types of Critical Infrastructures Discussed in the Article

National Cloud/Data Centers	Intelligent Energy (Smart Grid)	Telecommunications LTE/5G/6G
Finance and Stock Exchange (HFT)	Air Traffic and High-Speed Railways	Industry 4.0 (Smart Factory)
Autonomous Vehicles and Robotics	Smart City	Defense Industry
Public Administration	Security Management (ISO 27000/27001/27002)	Space Industry

Sector	Accuracy	Resilience	Threats	Immutability	Scale	Traceability	Intuitive
Power	1µs	★★★	★★★	★	1,000s	★	★
Telecoms	1µs	★★★	★★★	★	10,000s	★	★
Military	10µs	★★★	★★★	★★	10,000s	★	★
Finance	100µs	★★	★★★	★★★	10,000s	★★★	★★
Gambling	1ms	★	★	★★★	10,000s	★★★	★
Real-time bidding	1ms	★	★	★★	10,000s	★★	★
Gaming	1ms	★	★	★★★	10,000s	★★	★
Media	1ms	★★	★★★	★	10,000s	★	★★
GNSS Monitoring	1ms	★★	★★★	★	10,000s	★	★★
Enterprise	1ms	★	★★★	★★	100,000s	★★	★★
Smart factories	1ms	★★★	★★★	★★★	1,000,000s	★	★★
Transport	1ms	★★	★★★	★	1,000,000s	★★	★★★
Digital currencies	1ms	★★	★★	★★★	10,000,000s	★★★	★
Insurance	100ms	★★	★	★★★	10,000,000s	★★★	★
Payments	10ms	★★	★★★	★★★	10,000,000s	★★★	★★★
Health	10ms	★★	★★★	★★★	10,000,000s	★★★	★★★

To introduce the issue of destabilizing the distributed architecture of telecommunication infrastructure using synchronization, let us momentarily travel back to the 13th-century empire of Genghis Khan. This empire, the second-largest by territory in human history, began far in the east of Asia, encompassing modern-day Beijing, spanned westward across the European areas of modern-day Russia, and extended to the south covering Iran, Iraq, and India, looping back eastward through Tibet. The empire was so vast that its central administration, especially the management of dispersed frontier wars, posed a civilizational challenge. The time required for emissaries of Genghis Khan to traverse great distances measured in thousands of kilometers, delivering orders and bringing back news from the battlefields, took them many weeks of travel, and not all of them reached the Mongolian monarch. It increasingly happened that information about victorious battles reaching the emperor was already outdated, as the newly acquired territories were lost again. In such a vast empire, the time required for information flow within the governance system did not meet expectations and did not allow for effective central decision-making by the emperor. This was the beginning of defeats and, consequently, the fall of the empire.

The scale of the problem is illustrated by Figures 1, 2, and 3.

Fig. 1. Expansion of the Mongol Empire in the 12th Century
Source: Mongol Empire map.gif – https://en.wikipedia.org

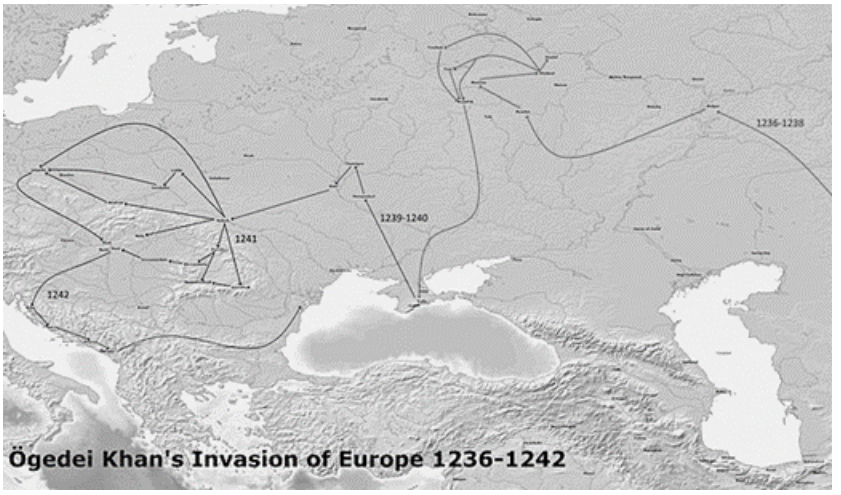

Fig. 2. Invasion of Europe

Source: 1236-1242 Mongol invasions of Europe.jpg – https://en.wikipedia.org

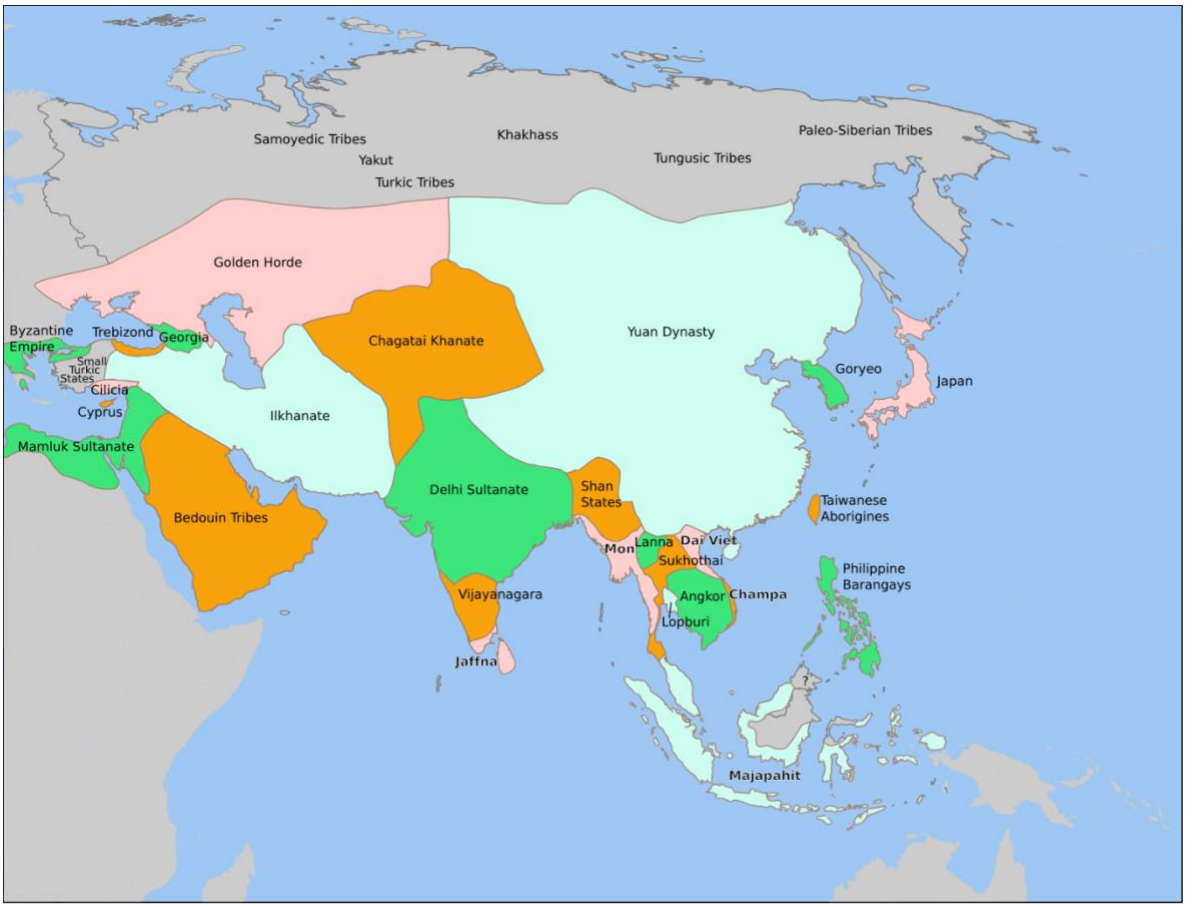

Fig. 3. Asia in the 14th Century
Source: Asia in 1335.svg – https://en.wikipedia.org

Modern technology must confront a similar problem of excessive growth. Upon reaching the limits of maximum processor speeds, the world adopted the only remaining direction to increase information processing performance—parallel computing. With the advancement of communication technologies, a continuous process of IT infrastructure decentralization commenced, which has now taken a dangerous trend of strong interdependencies within entire control systems, including those in industry.

This phenomenon has become particularly hazardous in the era of Industry 4.0 development, where predictive control of industrial automation has been entrusted to Artificial Intelligence (AI). The dependence of business and industrial processes on the time correlation of entire management subsystems exposes the parallel processing technology in the time domain (TCC – Time Coordinated Computing) to the idea and tool of cybercrime for an effective attack involving clock settings manipulation. Today, the desynchronization of time in critical infrastructures threatens failures of unpredictable consequences, especially in power systems, 5G telecommunication, banking, stock exchanges, air traffic control, and rail transport. Increasingly, there is talk of the specter of a major failure causing a domino effect, a failure on a continental scale. The use of the term "blackout" is not an exaggeration.

The excessive complexity of ICT systems and their overly tight interdependencies, including that from GNSS family satellite systems, justify incorporating the issues of time and time synchronization as a new important element of contemporary cybersecurity.

This relationship is the area of interest for the author of this publication, who, by analyzing available literature on the subject, as well as specialist publications and analyses of cases of so-called "time attacks," has synthesized the main knowledge areas concerning these threats and methods of minimizing risks associated with this area of cybersecurity.

The main thesis that the author proves in this article is the assumption that there is a possibility of conducting sabotage activities that can destabilize the operation of ICT systems without the need to break into well-protected internal networks. This changes the entire paradigm of cybersecurity today. By manipulating clocks, the correct measurement of network delays is falsified, which in turn introduces a disturbance where correct data may be rejected, and outdated information delayed by too long a journey is erroneously accepted as correct.

2. Description of the Problem

Time synchronization is a specialized and little-known issue, making it convenient for cybercriminals to exploit in an attack. In the event of an attack, it remains unnoticed for a long time; colloquially speaking, it is "beyond suspicion." Our intuition tells us that, since we know how to read clocks, the issue can't be difficult—nothing could be further from the truth. When we see the time on a computer desktop or street displays, we are also dealing with synchronization, but synchronization understood in this way does not pose a threat to the ICT system. However, precisely determining the simultaneity of events with very high accuracy and small error is essential today, as it is critical for the stability of a highly distributed infrastructure. Conformity of time on a macro scale down to a single second is also a significant challenge for the ongoing process of digital transformation in public administration and industry—certification, electronic signatures, authenticated document circulation, etc.

Today, synchronization is an element of cybersecurity. Instead of breaking into a well-protected TCP/IP internal network, it is simpler to destabilize the ICT system's operation by remotely disrupting synchronization, for example, by manipulating GPS, upon which we are too dependent[3]. By manipulating clocks and time, one can disrupt the chronology of events recorded in LOG journals. In such a situation, the chance to analyze error logic is irretrievably lost, and the true cause of a failure cannot be determined. This is a significant topic from the viewpoint of security management in accordance with the ISO 27000 family of standards. The best way to illustrate this problem is with a current example. In the so-called "Minister Dworczyk Emails"[4] case, if hackers had adequately altered the timestamps, the interpretation

[3] US Federal Register – The Daily Journal US Presidential Executive Order EO13905, https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing.

[4] Mismatched chronology of e-mails from Minister Dworczyk – https://niebezpiecznik.pl/post/mail-morawiecki-dworczyk/.

of the event could look different, and it would be hard to assume a hacker attack. It was thanks to the "unchanged" timestamps preserving the actual chronology that we were faced with a situation where the effect precedes its cause, meaning Prime Minister Morawiecki responded to questions before Minister Dworczyk asked them (Figure 4).

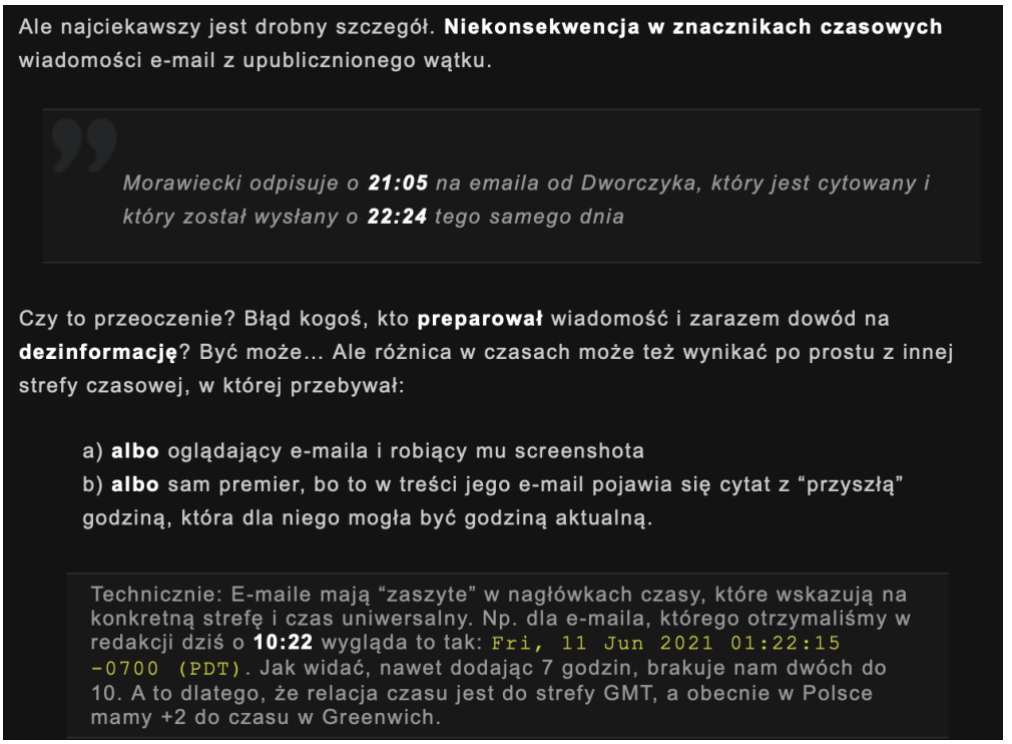

Fig. 4. Analysis of Emails in the So-Called "Polish Minister Dworczyk Affair"
Source: https://niebezpiecznik.pl/post/mail-morawiecki-dworczyk/

Currently, the risk areas associated with security are defined by two new types of attacks related to synchronization and time:

- **Time Synchronization Attack (TSA)**
- **Time Delay Attack (TDA)**

These are among the most likely and simultaneously the most dangerous for an automated and GPS[5]-dependent economy. The issue is serious enough that it is the subject of international work within ITU-R groups (WP-7A) in Geneva at the United Nations, where the national delegation of the Chancellery of the Prime Minister of Poland (KPRM) submitted the first Polish contribution in 2021, based on the work of the Polish time server manufacturer, ELPROMA. A summary of the Polish document can be found on the ITU News 2/2023[6]. Hence, there is growing talk about the increasing importance of official time as an alternative to the satellite-based GNSS (GPS, Galileo, Glonass, Beidou, IRNSS) time reference.

[5] ION/PTTI "GNSS Time Synchronization Attack Detection and Discrimination Based on Correlations of Calculated Clock Drift Time Differences" https://www.ion.org/publications/abstract.cfm?articleID=17721.

[6] ITU-News 2/23 https://www.itu.int/en/itunews/Documents/2023/2023-02/2023_ITUNews02-en.pdf.

In Poland, a project named eCzasPL[7] (eTimePL) is being conducted by the Polish Central Office of Measures (GUM). The main goal of the project is to provide a credible and reliable distribution service of official UTC(PL) time signals applicable throughout the territory of the Republic of Poland, as well as synchronization monitoring services to effectively prevent future incidents such as the Polish Railways PLK system failure[8] on March 17, 2022. Analysis of this case shows that similar failures, in both symptoms and effects, can be caused[9] by TSA and TDA attacks.

Unfortunately, ensuring effective monitoring of system clock operations in telecommunication and computer systems remains no less technically challenging than their synchronization. This involves the risk of hybrid sabotage actions that may accompany radio time attacks (TSA). Today, European industry should consider the possibility of such actions as, for example, the sabotage disrupting communications lines, which the UK experienced[10] on March 17, 2022 – exactly on the same day as Poland did, and the German sabotage act of railways DB faced[11] in October 2022. The German and UK experiences, in retrospect, recall another incident from Poland— a fire on the Łazienkowski Bridge in Warsaw in 2015. A failure of these links, combined with the accident that happened in Poland and the UK on the same date, the 17th of March 2022, raises significant questions about the security ensuring the stability of modern critical infrastructures. It also raises the question of whether we are prepared for GPS total signal jamming, too. Proper synchronization is also closely related to ATC information broadcasting systems, as several thousand passengers in the USA[12] experienced in January 2023.

The number of GPS jamming and spoofing attacks increased after the Russian annexation of Crimea in 2014. The phenomenon intensified with the active involvement of the Russian military in operations in the Syrian[13, 14] region. The 2022 aggression in Ukraine further intensified the occurrence of the described problem. The effectiveness of disruptions in radio systems is partly explained by a new type of warfare cyber-weapon, "Electronic Warfare," which has been equipped in the Russian military, as described in a Swedish[15] report from 2018. Between 2018 and 2021, Western media (e.g., CNN[16]) increasingly reported on the possibilities of manipulating GNSS signals, particularly the American GPS.

---

[7] eTimePL Project https://www.gum.gov.pl/en/projects/national/272,e-CzasPL-e-time-project.html.

[8] Niezbędnik cyber 17/03/23 https://niebezpiecznik.pl/post/cyberatak-na-pkp-ktorego-nie-bylo/.

[9] https://www.reuters.com/world/europe/technical-fault-halts-polish-railways-key-ukraine-exit-route-2022-03-17/.

[10] https://www.cornwallrailwaysociety.org.uk/latest-input--news--old-pictures-etc/17th-march-2022.

[11] https://www.reuters.com/world/europe/no-sign-that-foreign-state-was-behind-german-rail-sabotage-police-2022-10-09/.

[12]https://www.cnbc.com/2023/01/11/faa-orders-airlines-to-pause-departures-until-9-am-et-after-system-outage.html.

[13] Institute of Navigation Webinar, “First results from three years of GNSS interference monitoring from low Earth orbit”, https://www.youtube.com/watch?v=XDbn85IBIus&t=0s.

[14] Matthew J. Murrian, at all, “First results from three years of GNSS Interference Monitoring from Low Earth Orbit”, 2022, https://radionavlab.ae.utexas.edu/images/stories/files/papers/leo_int_mon.pdf.

[15] Jonas Kjellén, „Russian Electronic Warfare” https://www.foi.se/rest-api/report/FOI-R-4625-SE.

[16] [16] CNN “GPS spoofing: Russia's new cyberweapon”, https://edition.cnn.com/videos/cnnmoney/2017/11/03/russia-gps-spoofing-cyberweapon-lon-orig-mkd.cnn.

3. Working in the Time Domain – Discontinuity of the UTC Scale – The UTC Leap Second problem

Modern computing relies on the UTC (Universal Coordinated Time) scale. This scale is used by the kernel of operating systems (OS) such as Windows, Linux, and Unix, which differentiate the clock displays on the desktop depending on the current time zone, determined by the network TCP/IP routing, using built-in GNSS or language settings. Local time is used in LOG event journals, file systems, databases, archiving systems, etc. However, deep within the operating system, time is always measured in the UTC scale. The discontinuous fact of the UTC time scale (Figure 5.b) is known as the problem of the so-called leap second. A leap second is an additional second that is occasionally added or subtracted very irregularly to compensate for the difference between astronomical time, such as the historical GMT (Greenwich Mean Time), and the very stable time measured by atomic clocks that form the basis of the atomic time scale TAI (Figure 5a).

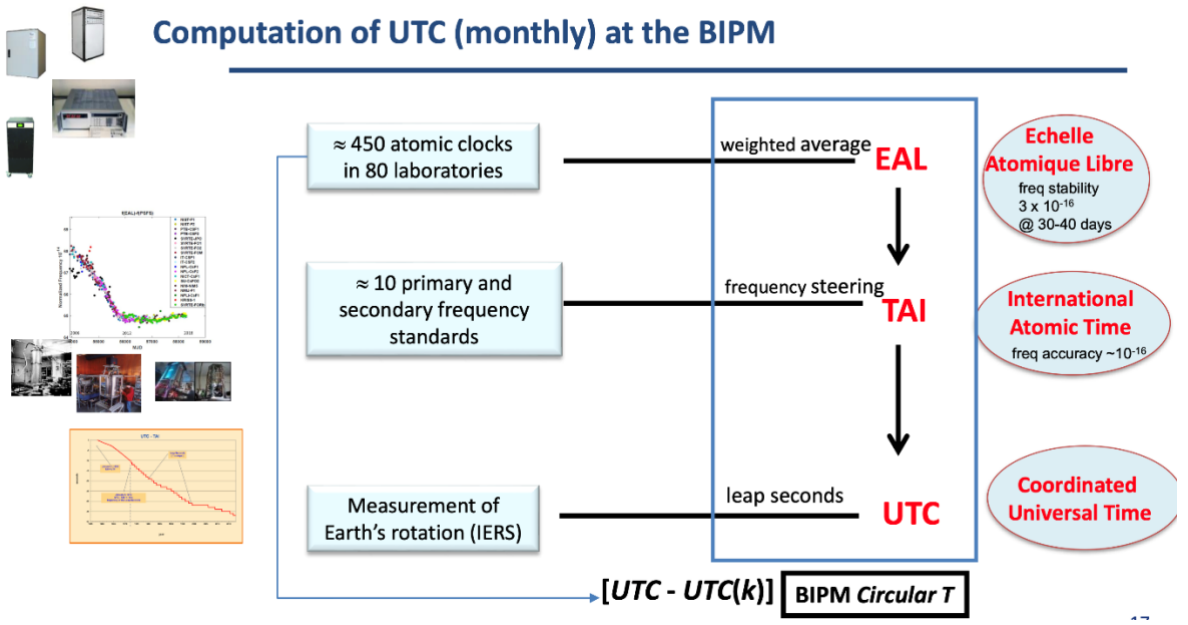

Fig. 5a. Process of Creating the UTC
Source: BIPM, Patrizia Tavella

Simply put, the UTC is based on very stable operating physical atomic clocks, but it periodically corrects for the instability of the Earth's rotational motion, which, over the long term, regularly slows down (resulting in increasingly longer days), although it can also periodically speed up (Figure 5a).

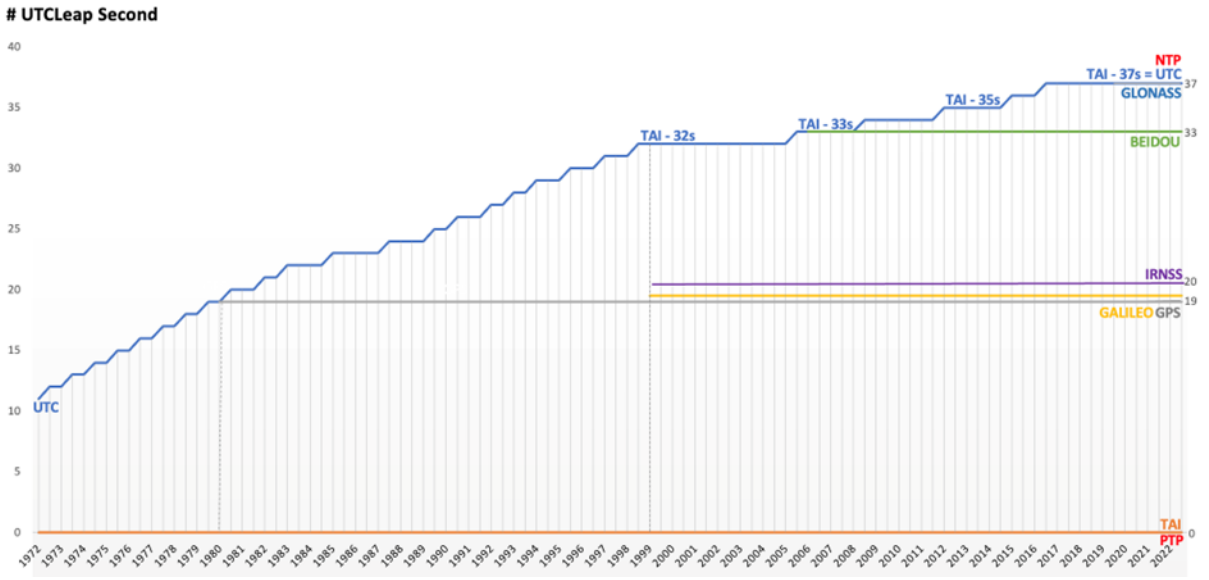

Fig. 5b. The internal time scales of individual satellite systems differ from the atomic time scale TAI by: GPS 19s, IRNSS 20s, BEIDOU 33s, GLONASS 37s.
The NTP protocol uses the UTC scale, which includes leap seconds, requiring proper handling of leap second addition/subtraction in a continuous (non-jump) manner. On the other hand, the IEEE1588 PTP protocol uses the UTC scale broken down into TAI components and the number of leap seconds.
Altering the number of leap seconds can desynchronize critical infrastructure, leading to its failure.
Source: self-prepared

The IERS (International Earth Rotation and Reference Systems Service) organization (www.iers.org) decides on the leap second correction, and the signal for this change is transmitted through the TCP/IP network, long-wave radio systems (e.g., the German DCF77 transmitter broadcasting the time standard on long waves at a frequency of 77.5 kHz with a wavelength of 3868.2897806 meters), and through GNSS satellites and many radio dissemination standards more. Unfortunately, as it has been shown in practice, such a solution has crucial negative significance for the stability, and consequently for the cybersecurity, of the developing structures of Industry 4.0 in this and the coming decades. It also impacts all critical infrastructures, leading to issues such as:

- Time discrepancies in a distributed system, where the validity of data is determined based on the difference between the timestamp of a remote sensor/computer and the timestamp received by the local central management server. This can lead to the acceptance of incorrect data (incorrectly calculated packet travel delay in the TCP/IP network), resulting in errors and failures. The risk increases with the growing popularity of TSN (Time-Sensitive Networking) and TCC (Time Coordinated Computing) distributed processing. This is especially significant for 5G telecommunications, modern two-way intelligent energy smart grids, and low-latency industrial networks.
- Software failures, including the firmware of IoT/IT devices based on Windows/Linux/Unix. It should be noted that every currently produced network device has firmware based on the kernel of one of these operating systems (OS). Unexpected time jumps introduced by the UTC leap second are dangerous for the

stability of the OS kernel and can cause a critical failure ending with a "kernel panic" message. Such a failure results from disrupting the low-level chronology of events within the OS kernel resource utilization, which is responsible for organizing the so-called concurrency, multitasking, and multithreading of the operating system. This is a very deep level of the operating system, beyond the reach of system administrators, and therefore beyond any control.

The UTC leap second changes scenario a re defined in document ITU-R TF.460-6 (link):

2.1 A positive or negative leap-second should be the last second of a UTC month, but first preference should be given to the end of December and June, and second preference to the end of March and September.

2.2 A positive leap-second begins at 23h 59m 60s and ends at 0h 0m 0s of the first day of the following month. In the case of a negative leap-second, 23h 59m 58s will be followed one second later by 0h 0m 0s of the first day of the following month (see Annex 3).

2.3 The IERS should decide upon and announce the introduction of a leap-second, such an announcement to be made at least eight weeks in advance.

Handling a UTC leap second creates another jump change in the UTC scale, causing its functional discontinuity. The jump should be seen as a kind of "time hole" or “time gap” that creates a loss of correlation between the computer’s internal world and the passage of time we experience in the Newtonian world we live in. Handling always has negative effects in IT, but their magnitude is hard to predict. Many devices require a hard restart. E.g CISCO recommended its CATALYST router clients turn off the devices several hours before the addition of the 37th leap second in December 2016. IBM Redhat Linux, due to a detected kernel bug, also warned about the possibility of triggering a OS kernel panic.

Previously, the negative effects were not as severe. It is only over time, with the increasing number of interdependencies, that the risk to telecommunication and computer systems has grown. While the adopted A and B schedules minimize the risk for business and the financial sector, it remains high for telecommunications, energy, and air & rail traffic control. The mentioned handling of this tricky second creates a particular problem. While older OS versions handle the second with a dangerous jump, newer ones often compensate for the second in the manner of the relativistic phenomenon of time dilation, i.e., by stretching or compressing the time measured inside the OS kernel. This is done by periodically redefining the interval of one second at the counter level. In practice, this is done by frequency steering (adjusting clock frequency). This way, continuity of time is maintained within the OS kernel while the user sees a jump insertion second scenario on the screen, as shown in Figure 6.

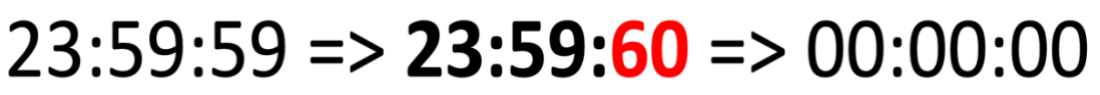

Fig. 6. Introduction of a Leap Second as Seen on Time Displays and the Computer Screen Desktop
Source: self-prepared

The side effects of time discrepancies created by new generations of Windows/Unix/Linux result from differences in approaches to the techniques of "stretching" and "compressing" computer time. Some Linux systems start the "slowing down" (or correspondingly "speeding up") process many hours before midnight UTC, using the Google Smear[17] technique proposed in 2015. In contrast, Microsoft Windows has a more abrupt approach and performs the entire operation within a few minutes before and after midnight.

The mechanism of manipulating the distribution of the UTC leap second schedule changes has not been well described so far, but experts from Polish ELPROMA point out the weakness of the system for broadcasting official information published in Bulletin-C[18] on the *www.IERS.org* website. Data is provided months in advance, and it is highly likely that many systems retrieve it in an automated manner, as shown in Figure 7. Changing this information can result in a time jump and the desynchronization of critical infrastructures important for the economy.

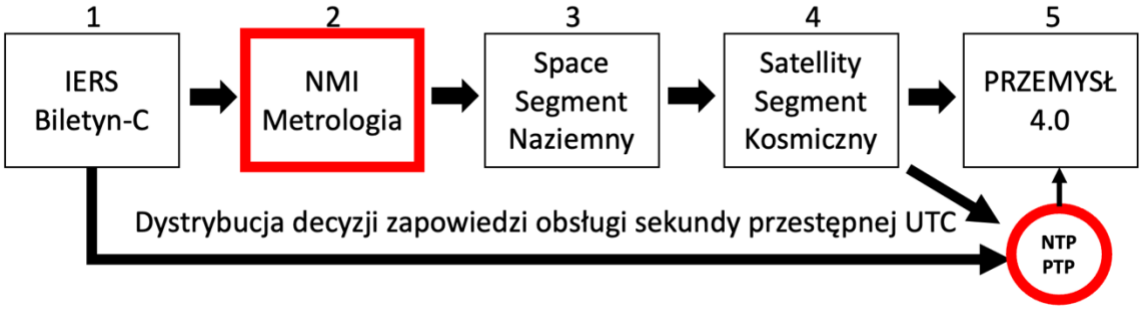

Fig. 7. Probable Scenario (Dataflow) of Automated Distribution of Leap Second Announcement

These data are utilized by some metrology laboratories, including those NMI responsible for time maintenance for GNSS satellite systems' terrestrial infrastructure. The announcement of leap seconds is also publicly available from IERS in a format compatible with the NTP protocol (Figure 8).

The IERS data are most commonly used by NTP/PTP time servers directly linked to reference atomic clocks. These are devices owned by NMI metrology centers that provide time standards to satellite systems and critical infrastructures directly[19] (via National Time Centers such as NPL in UK), whose operation must remain independent of the GNSS satellite system for security reasons. The integrity of the NTP data file is only protected by a HASH function, which, in the event of a successful cyberattack on public IERS servers and the replacement of the file in question, could have unpredictable consequences of desynchronization on a global scale. The mere act of issuing a false leap second announcement could cause unforeseen behavior in GNSS receivers not covered by simulation tests. Therefore, the risk of a successful attack on IERS servers (*www.IERS.org* website) is a significant risk element today.

[17] Google Smear Leap Second, https://developers.google.com/time/smear.

[18] IERS Bulletin-C, https://www.iers.org/IERS/EN/Publications/Bulletins/bulletins.html.
ITU TF.460-6 https://www.itu.int/dms_pubrec/itu-r/rec/tf/R-REC-TF.460-6-200202-I!!MSW-E.doc.

[19] National Timing Center in UK, https://www.youtube.com/watch?v=FpssM53sDk0.

For example, in the case of terrestrial digital television DVB-T2, the loss of synchronization of BTS transmitting masts triggers their automatic shutdown, resulting in the suspension of TV program broadcasting in the region.

At the end of this paragraph, let us add that the discussion on the introduction of the leap second has been going on for over twenty years and has always been effectively blocked by the representatives of all three monotheistic religions of the world are also opposed to the introduction, because these religions are united by the fact that important holidays for them refer to historical events and are determined based on astronomical observation time.

```
#
#       The following line shows the last update of this file in NTP timestamp:
#
#$      3882249427
#
#       2) Expiration date of the file given on a semi-annual basis: last June or last December
#
#       File expires on 28 December 2023
#
#       Expire date in NTP timestamp:
#
#@      3912710400
#
#
#       LIST OF LEAP SECONDS
#       NTP timestamp (X parameter) is the number of seconds since 1900.0
#
#       MJD: The Modified Julian Day number. MJD = X/86400 + 15020
#
#       DTAI: The difference DTAI= TAI-UTC in units of seconds
#       It is the quantity to add to UTC to get the time in TAI
#
#       Day Month Year : epoch in clear
#
#NTP Time      DTAI    Day Month Year
#
2272060800      10      # 1 Jan 1972
2287785600      11      # 1 Jul 1972
2303683200      12      # 1 Jan 1973
2335219200      13      # 1 Jan 1974
2366755200      14      # 1 Jan 1975
2398291200      15      # 1 Jan 1976
2429913600      16      # 1 Jan 1977
2461449600      17      # 1 Jan 1978
2492985600      18      # 1 Jan 1979
2524521600      19      # 1 Jan 1980
2571782400      20      # 1 Jul 1981
2603318400      21      # 1 Jul 1982
2634854400      22      # 1 Jul 1983
2698012800      23      # 1 Jul 1985
2776982400      24      # 1 Jan 1988
2840140800      25      # 1 Jan 1990
2871676800      26      # 1 Jan 1991
2918937600      27      # 1 Jul 1992
2950473600      28      # 1 Jul 1993
2982009600      29      # 1 Jul 1994
3029443200      30      # 1 Jan 1996
3076704000      31      # 1 Jul 1997
3124137600      32      # 1 Jan 1999
3345062400      33      # 1 Jan 2006
3439756800      34      # 1 Jan 2009
3550089600      35      # 1 Jul 2012
3644697600      36      # 1 Jul 2015
3692217600      37      # 1 Jan 2017
#
#       A hash code has been generated to be able to verify the integrity
#       of this file. For more information about using this hash code,
#       see the README file in the 'sources' directory.
#
#h      aa2fcda4 cccc651d e592e6f5 7051219b bc0e5481
```

Fig. 8. Information on UTC Leap Seconds
Source: IERS website, https://hpiers.obspm.fr/iers/bul/bulc/ntp/leap-seconds.list

In the case of telecommunications, desynchronization is significant for both BTS base stations and the backbone infrastructure of LTE/5G networks. Over time, the sensitivity of telecommunications to desynchronization will increase with the completion of work on defining the 6G standard, which will require control over delays, known as low-latency networking. This, in turn, necessitates very precise synchronization and monitoring of all clocks in the telecommunications network (Figure 9).

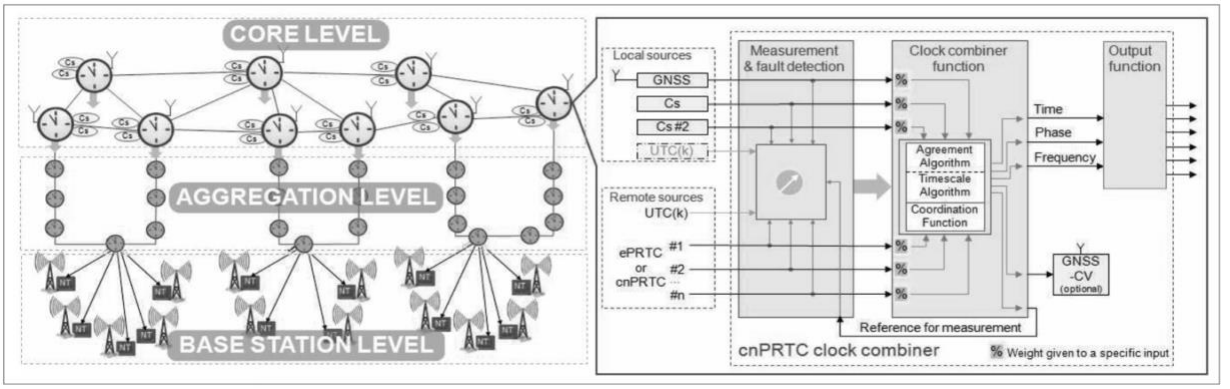

Fig. 9. Model of Synchronization for 5G Telecommunications Infrastructure
Source: P. Krehlik, H. Imlau et al., "Fiber-Based UTC Dissemination Supporting 5G Telecommunications Networks".

The role of time synchronization is very important for the latest intelligent two-way smart-grid energy systems. It is necessary to differentiate smart-grid from the classic one-way conventional energy systems, but by nature, energy systems are always associated with time and frequency in every case. Various sources[20] [21] indicate real threats of a Time Synchronization Attack (TSA). It is emphasized that in smart-grid energy systems, the predominant role of current power plants is limited. Many equivalent sources can generate electricity simultaneously, including renewable energy sources (RES), creating the challenge of establishing a consistent 50Hz and 60Hz voltage frequency standard. Note that the frequency parameter secures the power grid from the bottom-up, while the grid is protected from overloads and surges from the top-down. Desynchronization of the smart grid poses serious consequences, potentially even a blackout. In early January 2021, Europe experienced a mysterious frequency[22] drop below 50Hz in synchronized power grid connections. Although the incident did not cause connection failures in Europe, it put them to a significant test. Only energy supply interruptions in the Balkans were noted, and the source of the failure led to Romania, though this is not definitive. The problem illustrates that an energy failure in one country can dangerously lower frequency and cause a failure in another country, for which PMU (Phasor Measurement Units) responsible for maintaining

[20] IEEE Explore Feasibility of Time-Synchronization Attacks Against PMU-Based https://ieeexplore.ieee.org/abstract/document/8827583.

[21] Ezzeldin Shereen, „Security of Time Synchronization for PMU-based Power System State Estimation: Vulnerabilities and Countermeasures", Doctoral Thesis in Electrical Engineering KTH Sweden Royal Institute of Technology. https://www.diva-portal.org/smash/get/diva2:1607196/FULLTEXT01.pdf.

[22] Bizness Alert, Balkans source of a puzzling instability incident in Europe's power grid, https://biznesalert.com/balkans-the-source-of-a-puzzling-instability-incident-in-europes-power-grid/.

stable synchronization are crucial. In the case of smart-grid systems, PMUs require an accuracy of 1 microsecond, whereas in classical one-way energy systems, an accuracy of milliseconds is sufficient.

In summary, the synchronization problem associated with handling leap seconds is often related to GNSS receivers, which are widely used for synchronization today. Appropriate manipulation of the UTC leap second (e.g., through GNSS spoofing) creates a real threat to modern distributed critical infrastructures and may cause a domino effect of failures in interconnected systems. Described failures in receivers indicate the possibility of disproportionately large time errors, and the consequences of such failures are difficult to predict. Manipulation of the UTC leap second is possible because there are no established standards for its handling, which requires advanced techniques for seamless time correction. Its elimination is being addressed by ITU-R at the UN. Current agreements suggest the elimination could occur by freezing the leap second in 2035. According to a publication in Nature[23] in November 2022, this should become a fact. The background technical problems have been released in ITU-News[24] 2/2023, and the major world experts have spoken. Page #28 of the magazine includes the essence of the official contribution of Poland.

4. The Problem of GNSS Receivers – Susceptibility to Overflows – Internal GNSS Errors

Although the UTC leap second is a primary risk, it is not the only one. Since the 1990s, when the first commercial GPS receiver appeared, hundreds of millions of commercial GNSS satellite receivers have been deployed on the global market and are still in use as a reference source for the UTC scale. All of them calculate UTC fractionally differently, due to differences in internal algorithms and depending on the GNSS constellation used. The accuracy of the determined UTC also depends on weather conditions, antenna installation quality, interference, and the previously mentioned jamming/spoofing of GNSS satellite signals.

It is widely accepted that the main problem with the American GPS and other GNSS systems is their military nature. Apart from the European Galileo, all other systems cannot provide a trusted, resilient source of UTC in crisis situations and can be subject to manipulation. A special directive on this matter was issued back in 2004 by U.S. President G.W. Bush[25.] However, it is the U.S. President Donald Trump's directive EO13905[26], cited in this article, that begins to change the market approach. It recommends that American distributed architecture IT/OT critical infrastructures become independent of their own GPS. There are also other relevant government directives that allow for the limitation of satellite signals without prior public notice. There are also ordinary failures of these systems, transmission errors in Earth-Space telemetry, such as the one known as SVN23, which introduced a 13.5 microsecond error to the GPS system on January 26, 2016 (Figure 10).

[23] Nature, https://www.nature.com/articles/d41586-022-03783-5.
[24] ITU News, https://www.itu.int/en/itunews/Documents/2023/2023-02/2023_ITUNews02-en.pdf.
[25] G.W Bush, EO 2004, https://insidegnss.com/wp-content/uploads/2018/01/novdec08-coverstory.pdf.
[26] D.Trump, EO13905, https://www.govinfo.gov/app/details/DCPD-202000071.

The effect of the SVN23[27] error is illustrated in Figure 10, which shows a 13.5 microsecond discrepancy between five different synchronization devices (including NTP/PTP IEEE1588 servers) from various manufacturers, synchronized with the same GPS system. The devices react at different times, not overlapping, because their receivers vary in the algorithms calculating UTC. The visible inertia (diversity in the reaction of devices) can be explained by the diverse handling of emergency operations with a holdover oscillator. All of them will show a UTC discrepancy compared to the linear (non-jump) characteristic of other devices that used non-GPS subsystems during the failure, such as GALILEO, GLONASS, BEIDOU, or IRNSS. The official US Air Force Press Release related to GPS ground anomaly is presented below.

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.

Fig. 10.a The copy official US Air Force Press Release related to GPS ground anomaly. Source: ISBN 978-952-60-6703-2 (pdf) [27].

[27] GPS SVN23problem 13.5μs, https://aaltodoc.aalto.fi/handle/123456789/19833.

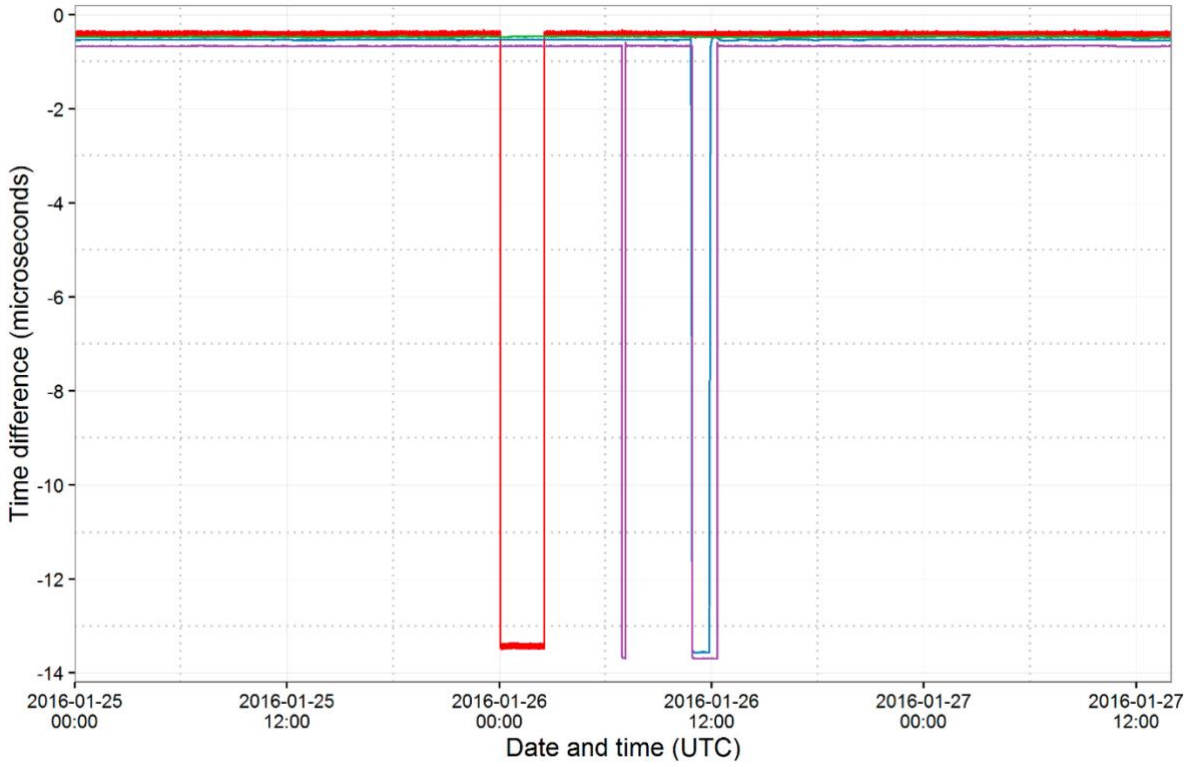

Fig. 10. Discrepancies of 13.5μs in the GPS System on January 26, 2016
Source: ISBN 978-952-60-6703-2 (pdf)

In the EU case, especially the East Europe part, the synchronization should rely on the European Galileo system supported by the American GPS. However, due to the possibility of restrictions on the emission of the military GPS signal (G.W. Bush directive – 2004, D. Trump directive EO13905 – 2020), it is crucial to support synchronization with time distribution from NMI, such as the Central Office of Measures of the Republic of Poland (GUM) through the eCzasPL project or NPL-Time Project in Great Britain (UK). The satellite receivers used for synchronization should keep close hardware compatibility, including firmware revision (version) compatibility too. It is also recommended to ensure operation mode without GNSS, i.e., holdover mode, which utilizes the internal built-in OCXO and Rubidium oscillators.

The biggest challenge in maintaining synchronization compliance across a large country area are commercial GNSS receivers. They are most commonly embedded in devices like NTP/PTP time servers. It turns out that in GNSS-based synchronization, an error of one year is just as probable as a jump of one millisecond. This happens because the time inside a GNSS receiver is represented numerically and undergoes processing, showing significant susceptibility to overflow errors. This is especially true when the manufacturer “packs” both the time and date into a single byte at the GNSS receiver. In such cases, it's easy to carry over the millisecond overflow bit to the date field, resulting in large time jumps. The forced data compression is related to the optimization of the solution, which needs to be small in size and energy-efficient. The GNSS receiver itself has a lot of calculations to perform and many opportunities to make errors. We often incorrectly assume that time and position are sent to us from space. Both time and position are determined here on Earth within the GNSS

receiver. Each receiver does this differently, but each must account for the correction resulting from Einstein's special theory of relativity, which is 7μs/24h, due to the 14,000 km/h speed at which satellites like GPS move relative to Earth in medium orbits. Another important correction is 42μs/24h due to Einstein's general theory of relativity and the effect of gravity impact on time dilation. Time on Earth flows more slowly than in space. Both values have opposite signs, so the daily time correction that the receiver must calculate for the GPS system after receiving telemetry from satellites is as much as 35μs per day. This is quite significant, considering that modern 5G telecommunications allow a maximum error of one microsecond, and sources for the smart grid require Ethernet network accuracy even much below one microsecond (200 nanoseconds for sources like NTP/PTP time servers according to IEEE C37.238 standard). All these factors increase the susceptibility of the GNSS receiver to numerical overflows.

The most well-known consequence of a clock register overflow error is the failure of the Patriot missile battery system during the first Gulf War in 1991. Due to inaccurate position calculations, the Patriot missile battery in Dhahran, Saudi Arabia, failed to intercept an incoming Iraqi SCUD missile, which struck barracks and killed 28 people. According to the GAO/IMTEC-92-26[28] report, the error was related to the clock time recorded in a 24-bit system register, where a rounding error occurred (Figure 11).

The Specifics of the problem was time in tenths of second as measured by the system's internal clock. It was multiplied by 1/10 to get the time in seconds. Internal registers were 24 bits wide.

$1/10 = 0.0001\ 1001\ 1001\ 1001\ 1001\ 100$ (chopped to 24 bits)

Error $\approx 0.1100\ 1100 \times 2^{-23} \approx 9.5 \times 10^{-8}$

Error in 100 hour operation period

$\approx 9.5 \times 10^{-8} \times 100 \times 60 \times 60 \times 10 = 0.34$ second

Distance travelled by Scud = (0.34 s) × (1676 m/s) ≈ 570 m

This put the Scud outside the Patriot's "range gate". Ironically, the fact that the bad time calculation had been improved in some (but not all) code parts contributed to the problem since it meant that inaccuracies did not cancel out.

Fig. 11. The Clock Error in the Patriot Missile Battery in Dhahran, Saudi Arabia in 1991

[28] GAO/IMTEC-92-26, https://www.gao.gov/assets/imtec-92-26.pdf.

5. GNSS Rcv that Do Not Operate According to OEM declaration

Globalization has led to the distribution of global electronics production. In seeking to optimize production costs, many US/UE reputable manufacturers of integrated circuits and GNSS receivers moved their production to China, and are now hastily bringing it back to their home countries, due to serious cybersecurity risks. Many producers also based their designs on foreign intellectual capital from engineering sectors in India, China, and Russia, where access to cheap, highly skilled engineering staff influenced the decision-making processes of managers and investors.

Additionally, many GNSS receiver manufacturers, especially companies from Russia, aiming to level their commercial chances with trusted and wealthy Western businesses, created special foreign subsidiaries to obscure the origin and know-how of the produced products. Encouraged by the low cost and very high quality, IT manufacturers, including time server producers, used Russian components in their devices for years. Today, products from a renowned world-leading time server manufacturers perhaps still contain a components like Russian OCXO oscillators and Russian GNSS receivers. Despite halting exports to Russia and Belarus, many industry companies did not stop importing and using Russian components, even though the risk issue was pointed out by numerous international US/EU laboratories.

Fig. 12. The Russian Receiver NVS ANAI 469635.002 (on the left). It based on the GLONASS System as Primary and Its Internal NV08C-CSM (on the right) Chipset Sold Commercially Under the Swiss Brand NVS and Exported Globally.

Signed in 2020, the US presidential directive EO13905 was most likely driven by the inability to identify and withdraw from the market devices based on Russian and Chinese GNSS receivers — chips produced in millions over the past decade and implemented in numerous IT systems of US critical infrastructures. While American companies were developing their products to support as many available GNSS constellations as possible, the Russian industry was ensuring that their local market was isolated from systems dependent on the American GPS system. Consequently, the Russian industry remained exclusively dependent on GLONASS satellites and supported by the ground-based "Chayka"[29] system – the Russian equivalent of west discontinued LORAN-C[30]. Recommendations emerged regarding manufacturers of GNSS receivers authorized for use in critical infrastructures within Russia, preceding the American EO13905 directive by many years ahead. One such recommended internal market manufacturer in Russia is NVS, registered in both Switzerland and Russia. The UTC time generated by this company's receivers shows strong coherence with the GLONASS satellite system time scale, even after the GLONASS system is disabled programmatically, leaving “only GPS” mode (Figure 12). Despite displaying the name GALILEO on the label, the NV-08 chip does not support the European satellite system.

6. TDA Time Delay Attack – network cards and devices

It might seem that since a network device operates inside a well-protected internal network, it cannot be an effective tool for cybercriminals. Nothing could be further from the truth. Figure 13 illustrates the operation of a time delay attack (TDA) within an Ethernet network. Network intermediary devices, such as Ethernet switches and TCP/IP routers, can introduce random variable delays. This disrupts the synchronization process between the client and server of NTP/PTP protocols at the points highlighted in red in the figure 13.

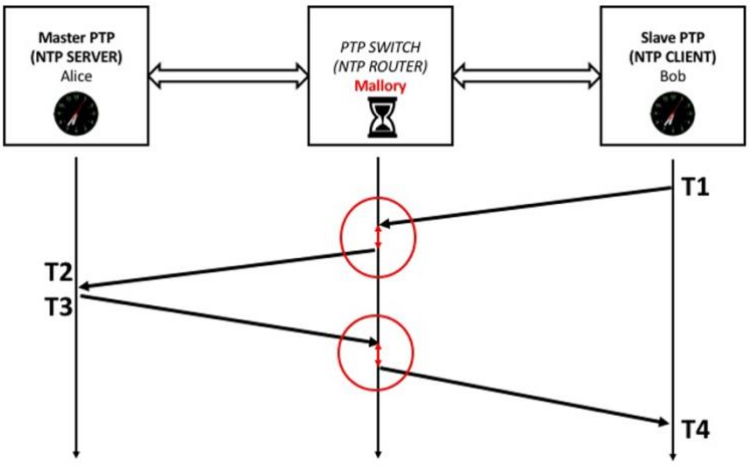

Fig. 13. Illustration of the So-Called Round-Trip Synchronization Packet (The same principle applies to synchronous broadcasting IEEE1588)
Source: Presentations by Elproma, www.elpromaelectronics.com, during the TA/PL/ Central Office of Measures of the Republic of Poland Conference

[29] https://en.wikipedia.org/wiki/CHAYKA.
[30] https://en.wikipedia.org/wiki/LORAN.

A Time Delay Attack (TDA) on a network is most commonly possible due to "bugs" implanted in devices during the production of integrated circuits (Figures 14a and 14b) or the assembly of printed circuit boards PCB (Figure 15). An intruder in the form of an additional chip can be embedded inside a legitimate integrated circuit (Figure 14a) or manually added to the PCB of a network card (Figure 15).

The identification of intruders participating in TDA is done by observing anomalies in the synchronization process, such as unexpected excessive internal link asymmetry, excessive synchronization noise, and variable delays observed under thermally stabilized operating conditions. In such cases, it is necessary to find the cause, which often requires laser decapsulation and microscopic enlargement of the integrated circuit for visual inspection (Figure 14b). This analysis can be performed by specialized cybersecurity diagnostics centers, although it is most often conducted by the device manufacturer.

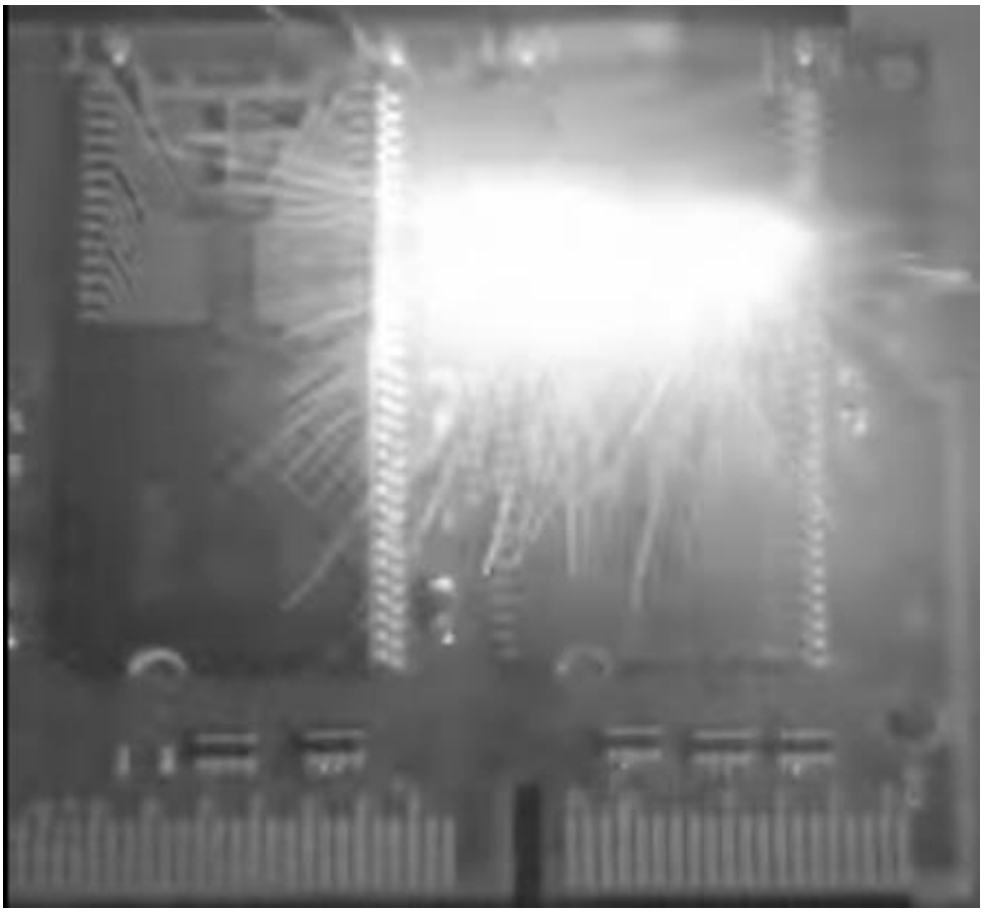

Fig. 14a. Effect of Laser Decapsulation of a Chip for Internal Inspection. This is how "planted" subcircuits are sought, which in the case of synchronization introduce noise and random delays.

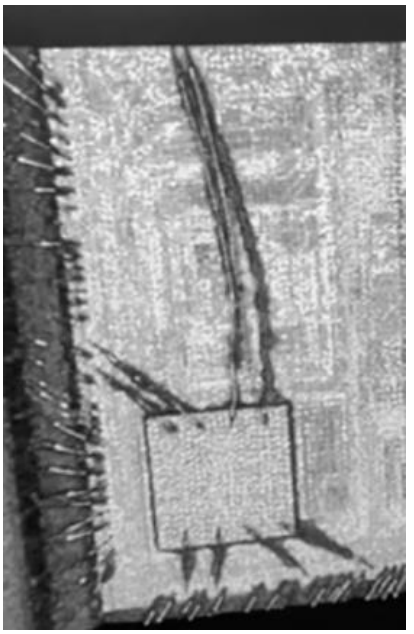

Fig. 14b. Laser-Decapsulated Chip "Intruder" inside "opened" chip.

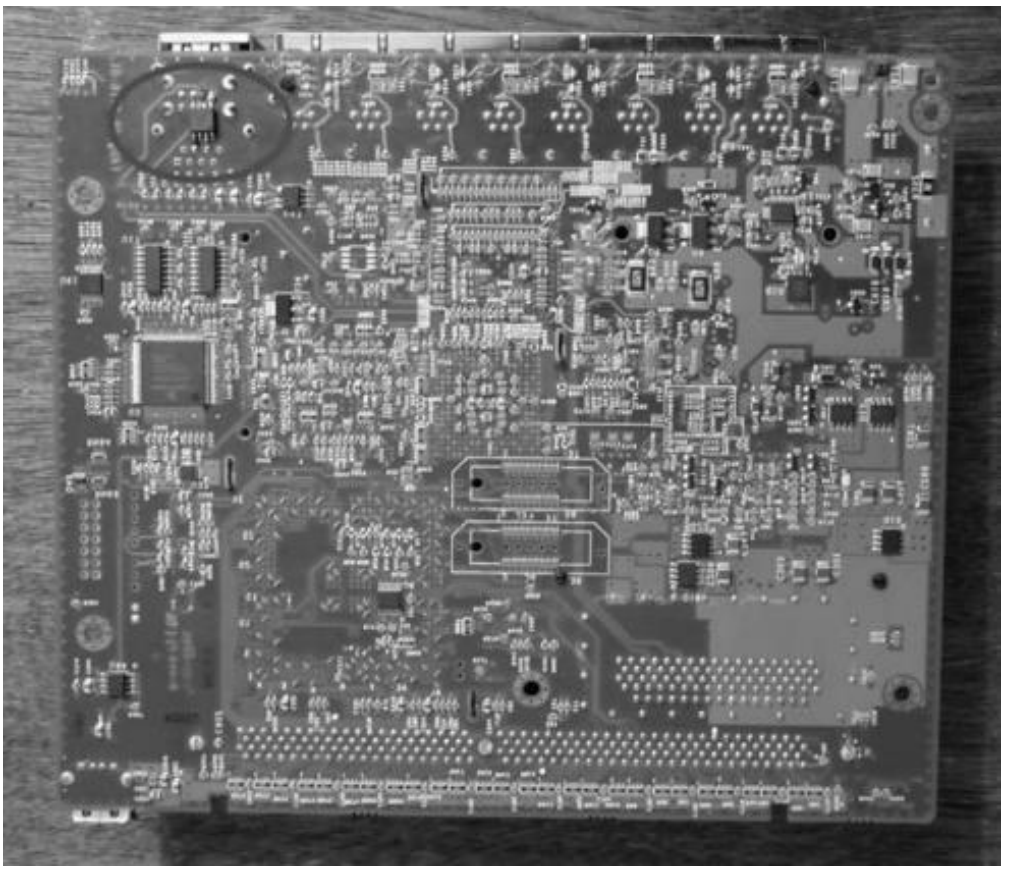

Fig. 15. Effect of Placing an "Intruder" Chip on the Printed Circuit Board – The "Intruder" Chip Added to the PCB is Visible on the Left Side in the Oval

Sources: Monta Elsins SANS Institute

7. NTPPOOL.ORG – Network Spoofing of Time over the Internet

A spoofing attack on the synchronization system can even affect IT systems that do not directly use GNSS receivers. This threat encompasses a large number of network devices based on open-source software, such as the Linux family of operating systems. Linux is used for both IT server platforms and constitutes the majority of internal hardware system firmware on which IoT devices and TCP/IP network routers are based. The standard Linux default reference source of UTC time is the group of public anonymous NTP servers gathered in the NTP POOL[31] Project. It is therefore not surprising that a group of such anonymous NTP servers poses a generally high risk of security vulnerabilities to IT/OT, and should be under constant security monitoring, including any fast-grooving changes in quantity that appear unnatural (Fig. 16a).

Table 2. Market share of public anonymous NTP servers of POOL in Europe (2025 update)

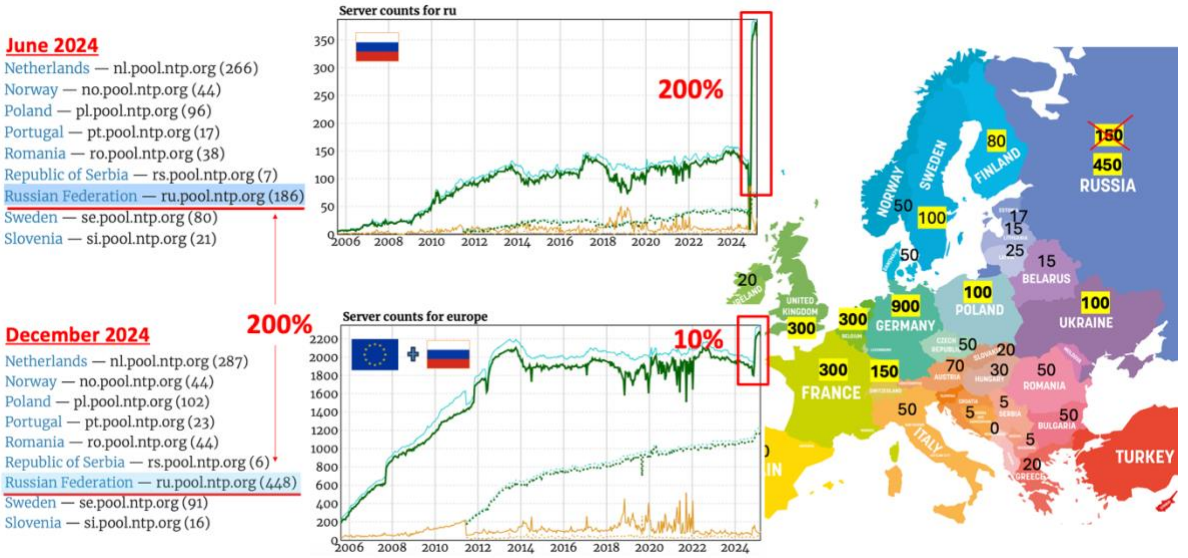

Fig. 16a. Impact of volume change in Russia POOL on the Europe after the yandex.ru incident. Sources: https://www.ntppool.org/zone/europe.

Over the past several years, the NTP POOL Project has gathered over 4500 NTP servers distributed worldwide. These are anonymous public servers, and their use is free of charge. They belong to companies, organizations, governments, and private individuals. Among them are high-quality public NTP servers provided by the US NIST, UK NPL, GUM in Poland, and other NMI (National Measurement Institutes). However, many NTP servers collected in the POOL are of mediocre synchronization quality, and their origin and UTC source remain unknown.

Any owner of an NTP server with an assigned static public IP address can submit their own server to the NTP POOL Project and make it available. Among the 4500 NTP servers are those based on ordinary end-user computers, laptops, hobbyist Raspberry Pi, etc.

[31] POOL NTP public anonymous NTP servers, www.ntppool.org.

The NTP POOL system examines DNS and IP routing, automatically determining the server's location grouping. The same POOL NTP system supports many Linux distributions and network hardware OEM suppliers. Many of them share physical time servers allocated simultaneously by different POOL groups:

Linux Distribution time domain of POOL:

1. **Ubuntu**: *ntp.ubuntu.com*
2. **Debian**: *debian.pool.ntp.org*
3. **CentOS**: *centos.pool.ntp.org*
4. **Fedora**: *fedora.pool.ntp.org*
5. **Arch Linux**: *arch.pool.ntp.org*

OEM HW time domain of POOL:

1. **Cisco**: *ntp.cisco.com*
2. **Juniper Networks**: *ntp.juniper.net*
3. **MikroTik**: *ntp.mikrotik.com*
4. **Ubiquiti Networks**: *ntp.ubnt.com*

The NTP servers with a physical public IPv4 or IPv6 address associated with devices operating in Europe are classified to join the *europe.pool.ntp.org* and simultaneously to join the local domain group of country *n.xx.pool.ntp.org* (where n is the number 0-3 and xx is the country code). Both join options do not limit the same NTP server can also be assigned to Ubuntu, Debian, and many other Linux pool groups (Tables 3 and 4).

The physical allocation of an NTP POOL server occurs automatically at the level of handling the symbolic DNS names. Linux and Windows users have no influence on the choice of a specific NTP server from the available pool, as the *ntp.conf* configuration file contains only a general symbolic domain/subdomain name under which the POOL system randomly selects the nearest geographically located server (Tables 3 and 4).

Tab. 3 Example content of the ntp.conf file for European servers (max. 4 lines only)

```
server 0.europe.pool.ntp.org
server 1.europe.pool.ntp.org
server 2.europe.pool.ntp.org
server 3.europe.pool.ntp.org
```

Tab 4. Example Content of the ntp.conf File for Servers Located in Poland

```
server 0.pl.pool.ntp.org
server 1.pl.pool.ntp.org
server 2.pl.pool.ntp.org
server 3.pl.pool.ntp.org
```

The allocation and removal of a public NTP server from a local PC operating system occur automatically in POOL without the owner's knowledge. Although POOL remotely monitors the accuracy of the NTP servers in relation to the UTC scale, it does so very rarely and cannot block the time synchronization attack (TAS) fast enough. Particularly concerning are reports describing the participation of POOL NTP servers linked to the Darknet, as such servers can secretly supply false time and alter the client's local clock settings on a server or router. Such a cyber-attack is a so-called POOL NTP *poisoning*. This phenomenon is a network substitute for GNSS spoofing, but conducted at the Internet level, and can be executed and controlled remotely from the territory of another country.

Anonymous public NTP servers from POOL gain contact with a synchronized PC through the Network Time Protocol without the owner's knowledge. If false (poisoned) servers are injected into the specific country's POOL, the probability of contact is high and the time synchronization attack rises too. While such an approach may seem ineffective, considering the covert functions of NTP POOL's automatic server switching, it provides an effective attack instrument over the long term. A hacker (owner of) a remote NTP server can physically identify the resources of the NTP client. Knowing the security vulnerabilities of the Linux operating system and firmware based on this system, the hacker can exploit this for a direct attack. The interaction between the hacker's machine (poisoned NTP server) and the user (NTP client) creates a high risk of successful DDoS attacks. Here is a quote of a white-hat hacker I have an opportunity to discuss the cyber-attack scenario:

"*I could easily set up an NTP server (e.g. using Raspberry Pi low-cost computer) , add it to the POOL NTP in the closest possible routing location near my target, wait until its score is increasing above 10. And then once it is added to the POOL NTP it will be highly probable used by a lot of systems, including the one I target. I can then (if I want to), manipulate the time I send to a specific target (selected) IP address and keep the time accurate for the NTP POOL monitoring server(s), so that they do not see that my time is off. At the same time, I can behave very fair to all other systems and users – the ones I am not interested in attacking. Then, I can start my attack by sending a different time to each individual IP address that is targeted, moving systems away from each other. Can the user protect himself against my attack? Yes, they will probably use other pool NTP servers as well and therefore may detect my attack, but if I would "poison" the pool with enough big number of my NTP servers (requiring many IP addresses), I could end up being the first, second and third source of time for a specific target IP address, especially if I add my server IPs to pool country zones that are dramatically understaffed with servers*".

8. Summary – 5 Groups of Risk for Destabilizing IT Telecommunication Systems Using TAS Attacks on Time Synchronization Systems or Time Synchronization Errors

1. **Earth.** Time Generation Process –Metrology Laboratories/ GNSS Ground Segment:
   a) **Potential manipulation of data in IERS Bulletin-C**, which changes the number of UTC leap seconds.
   b) **Discontinuity of the UTC scale** and multi-second time discrepancies between the internal satellite time scales of GPST, GALILEOT, GLONASST, BEIDOUT, IRNSST (the suffix "T" after the constellation name denotes the time scale of the specific GNSS satellite system).
   c) **Procedural errors in updating GNSS satellites** – e.g., the loss of GALILEO connectivity in 2019.[38]
2. **Earth-Space.** Satellite System – Telemetry Data Transfer to the GNSS Satellites:
   a) **Errors in telemetry data transmitted to GNSS satellites** – e.g., the SVN#23 issue on January 26, 2016.[39] Even a brief error in one system can lead to a

significant time jump in telecommunication systems dependent on other time distribution systems.

3. **Space-Earth**. Data Reception from GNSS Satellites by Receivers in Devices such as GrandMaster Clocks and NTP and PTP IEEE1588 Time Servers:
   a) **Security vulnerabilities** in GNSS receivers, particularly dangerous in the form of backdoors.
   b) **Overflow errors** in receivers, e.g., GPS Week Number Roll Over (WNRO) on April 7, 2019, which continues to cause time jumps of 19.7 years and it remind valid problem until today.
   c) **GNSS signal jamming,** classified as a "Time Attack."
   d) **Ground-based signal simulation** (GNSS Spoofing), known as a "Time Attack."
   e) **Signal capturing and delaying** (GNSS Meaconing), referred to as "Delay Attack"
   f) **Lack or artificial addition/subtraction of leap seconds** (UTC Leap Second).
   g) **Uncertainty regarding synchronization with internal** GPS(T), GALLEO(T), GLONASS(T), BEIDOU(T), IRNSS(T) **time scales.**
   h) I**ncorrect announcement or absence of a leap second announcement.**
4. **Transfer via Computer Networks and the Internet** (NTP/PTP Protocols):
   a) **Absence of leap second announcements and handling**, leading to second and minute jumps.
   b) **Impact of link asymmetry** on synchronization accuracy, noise caused by random traffic and DDoS.
   c) **Intentional introduction of delays** through network devices (TDA – Time Delay Attack).
   d) **Lack of authentication of the time source and no remote time audit** (poisoned or DARKNET servers inside POOL NTP). Falsification of unauthenticated NTP and PTP sources and lack of client-side verification of their time settings.
   e) **Errors confusing the UTC scale with the atomic TAI scale and local time**.
   f) **Impact of link asymmetry** on synchronization accuracy.
5. **Client-Side Devices** (Submaster NTP/PTP – previously called Slave Clock), Applications, including NTP/PTP Time Servers with both Grandmaster and Submaster and standard conversion functions:
   a) **Impact of traffic** (random traffic, DDoS attacks) on the synchronization process on the NTP and PTP client side.
   b) **Compatibility problems of NTP and PTP protocol versions,** causing unplanned discrepancies.
   c) **Variations in leap second handling** (UTC Leap Second) generate multi-second errors. By manipulating the leap second announcement flag, numerical overflow in GNSS receiver firmware and network cards can be induced, leading to desynchronization measured in years.
   d) **Human errors** (configuration settings, confusing UTC vs. local time).
   e) **Time scale representation errors** – representation: UTC vs. TAI, POSIX scales, GPSd bug issues, etc., as well as data structure discrepancies. For instance, the BEIDOU satellite system numbers the days of the week from 0 to 6, while others number them from 1 to 7. Switching systems in the chip during calculations can

cause a one-day error. Firmware switching between systems most often occurs with poor-quality received satellite signals. Therefore, it is good practice to configure receivers to receive only one satellite system, which may seem counterintuitive to the principle "the more, the better."

f) **Poorly executed GNSS antenna installations on rooftops** cause interference between antennas, which, when grouped, facilitate and enhance attack effectiveness.

The magnitude of time error (jump) can vary depending on the cause, ranging from nanoseconds to seconds, or even days and years. This is well illustrated by the GPS WNRO counter reset issue from April 7, 2019, which causes errors randomly depending on the hardware and firmware versions used, leading to errors of up to 19.7 years.

Fig. 16. View of the Roof of an Industrial Plant inside EU. The number of GNSS antennas reflects the typical Industry 3.0, where single PC controls one production line and need one GPS too. The GNSS antennas are placed too close together interfere with each.

Fig. 17. GPS Week Number Rollover Error from 2019 on Tramways in Warsaw Poland. Source: self-produced

Rys. 18. GPS Week Number Rollover Error from 2019
on Being aircraft gyroscope (left side) and TAX telemetry system in Prague in Czechia.
Source: self-produced

9. Conclusions and Polish National Recommendations for Building Time Systems for Secure UTC(PL) Synchronization Resilient to GNSS Failures

Poland recognized the importance of official national time standards much earlier than the USA and the United Kingdom. The national equivalent of NIST (USA) and NPL (UK) is the Central Office of Measures (Główny Urząd Miar, GUM) in Poland. The official Polish time is defined by the Act on Official Time from December 10, 2003 (Journal of Laws No. 16 item 144), and the distribution methods are specified in the Journal of Laws No. 56 from 2004, item 548 (Figure 19).

The Polish Parliament Act of December 10, 2003 (No 56, Item 144)

On Official Time in the Republic of Poland

Art. 1. Official time is introduced in the territory of the Republic of Poland.

Art. 2.

1. Official time in the territory of the Republic of Poland is Central European Time (CET) or Central European Summer Time (CEST) during its implementation period until further notice.

2. Central European Time is the time increased by one hour in relation to Coordinated Universal Time (UTC(PL)).

3. Central European Summer Time is the time increased by two hours in relation to Coordinated Universal Time (UTC(PL)).

4. Coordinated Universal Time (UTC(PL)) is the Polish realization of Coordinated Universal Time, maintained by the Central Office of Measures and specified by national time and frequency standards.

Art. 3. The introduction and cessation of Central European Summer Time in the territory of the Republic of Poland is based on the exact calendar dates on which the introduction or cessation of Summer Time occurs, taking into account existing international standards in this area.

Art. 4.

1. The body authorized to maintain official time and Coordinated Universal Time (UTC(PL)) and to disseminate these time signals is the President of the Central Office of Measures.

2. The Minister responsible for economic affairs shall define, by regulation, the methods of disseminating official time and Coordinated Universal Time (UTC(PL)), taking into account in particular existing international standards and user needs.

Art. 5. The Act of January 18, 1996, on official time (Dz. U. Nr 29, poz. 128), is hereby repealed.

Art. 6. This Act shall enter into force 14 days after its publication.

The President of the Republic of Poland: A. Kwaśniewski

REGULATION OF THE MINISTER OF ECONOMY, LABOR, AND SOCIAL POLICY

dated March 19, 2004

on the methods of disseminating official time signals and Coordinated Universal Time (UTC(PL))

Pursuant to Art. 4, Sec. 2 of the Act of December 10, 2003, on official time in the Republic of Poland (Dz. U. z 2004 r. Nr 16, poz. 144), the following is ordered:

§ 1. Official time and Coordinated Universal Time (UTC(PL)) signals from the Central Office of Measures shall be disseminated as follows:

1. Via the Internet at the address: tempus1.gum.gov.pl
- tempus2.gum.gov.pl with the use of the NTP (Network Time Protocol) transmission protocol;

2. Via the telecommunications network using the phone number (0-prefix-22) 6548872 and the European Telephone Time Code;

3. Via public radio announcements transmitted on long wave radio every hour.

§ 2. The regulation enters into force 14 days after the announcement.

Minister of Economy, Labor, and Social Policy:
J. Hausner

Fig. 19. Excerpt from Dz.U. Nr 16 from 2003, item 144, and Nr 56 from 2004, item 548 Defining the Methods of Distributing Official UTC(PL) Time in Poland

For over 20 years, time in Poland has been legally protected and can have legal effects. Therefore, the national industry and administration should rely on official Polish time. In 2023, the Central Office of Measures of the Republic of Poland (GUM) launched the eCzasPL (eTime) system, which can deliver authenticated and cryptographically secured official Polish time UTC(PL) independently of GNSS via the Internet and dedicated Ethernet links. The eCzasPL (eTime) project extends the law with a mechanism for remotely auditing the time indications of distant NTP and PTP (IEEE1588) servers. This technology was developed in 2015-2016 by engineers from the Polish company ELPROMA participating in the European Horizon 2020 project named DEMETRA.

One of the very important features of the eCzasPL (eTime) system, particularly critical for building time systems resilient to manipulation and falsification, is the ability to create a convergent security model for synchronization, where time is obtained simultaneously from:
- **The computer network** with authentication to the NTP servers listed in the official Parliament Act Nr 56 from 2004, item 548, and continuous auditing (monitoring) of time settings on such synchronized NTP/PTP (IEEE1588) servers.
- **The European satellite system GALILEO,** supported by the backup GPS system, both subjected to **remote auditing** of UTC time indications on the end-user side (NTP/PTP server audit by the user) with reporting to the Central Office of Measures for official time certification purposes in accordance with the law.

The above model allows for the creation of secure official UTC time delivery systems resistant to manipulation. Depending on defined threat vectors, the synchronization system should dynamically adapt its configuration to operate centrally (no threats) and gradually decentralize the configuration in areas affected by GNSS jamming or spoofing as attacks.

Another very important feature of a reliable time system, particularly crucial for its operation in decentralization mode (during an attack), is maintaining the autonomy of the distributed clocks. This is achieved by using holdover oscillators to keep the time. The most popular oscillators (ordered from the least parametric but cheapest to the best and most expensive) are: TCXO, OCXO, Rubidium, Cesium, Hydrogen Masers, Optical Clocks and Cesium Fountains. The synchronization subsystem autonomy process in a reliable synchronization system requires support through clock aggregation technology, which involves connecting multiple clocks in series groups to create greater inertia in maintaining a stable passage of time.

Autonomously operating synchronization subsystems are increasingly supported by artificial intelligence (AI) and machine learning (ML). Currently, 5G telecommunications use ePRTC-class clocks that, with built-in atomic clock stability statistics and continuous learning, can behave like Cesium clocks in holdover mode. Aggregating such clocks allows for creating entire autonomous corporate UTC time subsystems known as coherent network clocks (cnPRTC). They do not require frequent calibration to GNSS. Their drawback is the high cost, so they can only be considered to support the stability of the backbone part of critical IT infrastructure. A good example of using cnPRTC network clocks is their application in building ground-based PNT (Positioning Navigation Timing) systems as alternatives to GNSS. Such solutions will play an important role in the automation of smart

city, intelligent smart grid, autonomous vehicles industry, air traffic control, 5G/6G and the related low-latency networking.

In the vast majority of cases, the construction of a synchronization system resistant to attacks and manipulation can be effectively carried out using a three-level protection model proposed by the Polish company Elproma (www.elpromaelectronics.com), supported by products from PIK Time. Both companies have closely collaborated for over a decades.

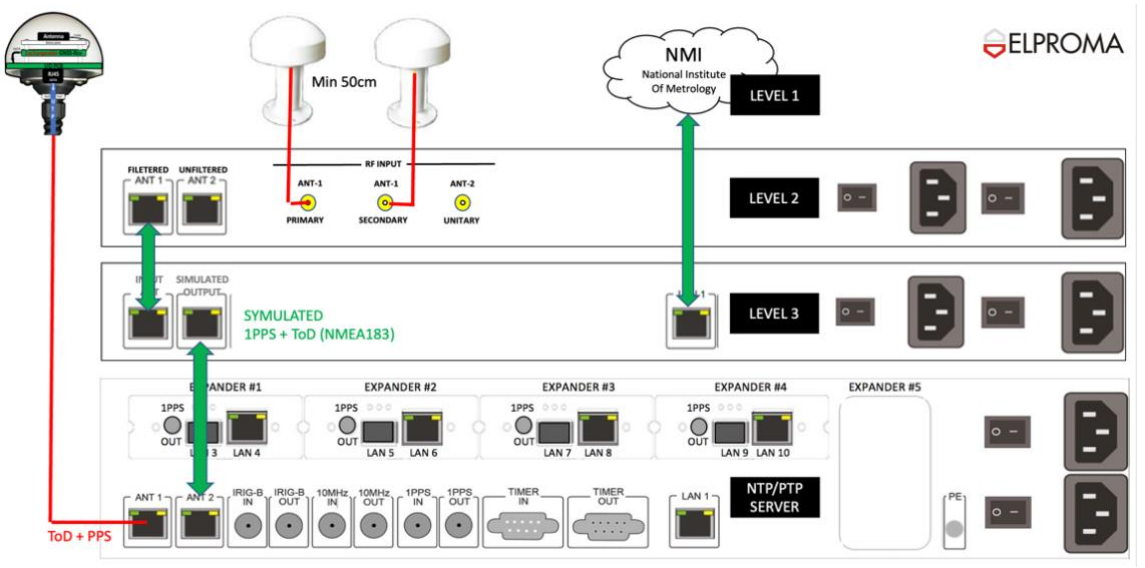

Fig. 18. Three-Level Proprietary Synchronization System by the Polish Manufacturer ELPROMA with Synchronization to the Central Office of Measures of the Republic of Poland (GUM).
Source: self-produced

ELPROMA has created a Three-Level Proprietary Synchronization System with Three-Stage Security (Figure 18):

LEVEL-1: This level features an intelligent antenna containing a replaceable GNSS receiver module. The company offers specialized adaptation of receivers to geopolitical conditions in the region or continent. In Europe, the recommended system is GALILEO supported by GPS. America, Australia, and New Zealand use antennas equipped with receivers synchronized to GPS and supported by GALILEO. The economies of countries linked with Russia choose antenna configurations with receivers synchronized to the GLONASS system exclusively. The Chinese will use the BEIDOU system, while India will use IRNSS. Other countries will select receivers based on preferences and economic and geopolitical conditions for their region. The selection of GNSS receiver manufacturers is always carried out in collaboration with the cybersecurity department of the client's critical infrastructure.

An important feature of the solution proposed by the Polish company Elproma PIK Time is the ability to correct the GNSS receiver in the antenna at any time during the system's operation. Detecting even the slightest security vulnerability necessitates the initiation of the module replacement procedure without the need to interfere with the technically advanced NTP IEEE1588 time server.

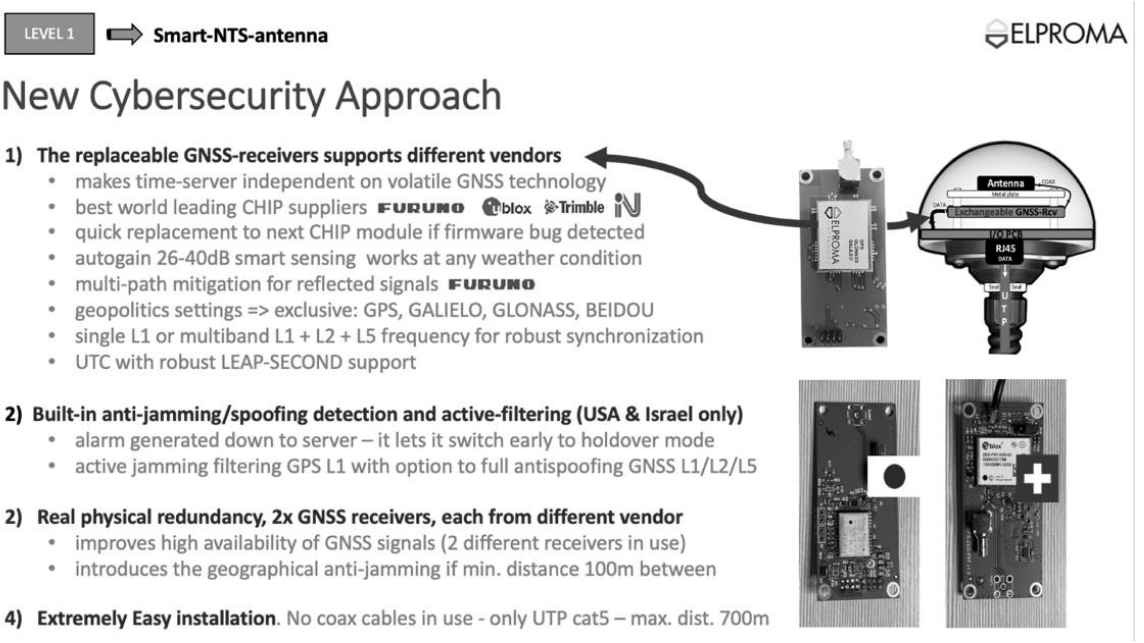

Fig. 19. Illustration from the Presentation by the Polish Company ELPROMA, showing the Interchangeability of GNSS Modules in the Receiver (Antenna) with a Proposal to Choose Japanese and Swiss OEM. Elproma Offers Several Similar Interchangeable Units. Source: YouTube, https://youtu.be/dZDs9p2Fa04

The Polish company offers several lab-tested GNSS receivers for LEVEL-1 antennas, including more advanced ones with built-in anti-jamming, anti-spoofing, and multipath mitigation functions for GNSS signals. Upon special request and for an additional fee, Elproma can integrate any satellite receiver selected by the client, including those from operators of low Earth orbit (LEO) satellite systems such as e.g. Iridium.

The advantage of such an architecture is its "turnkey" configuration and departure from the stereotype of static configurations, which are easy to recognize and consequently hack using GNSS jamming and spoofing. This particularly enhances the cybersecurity value of the Polish solution, which is highly regarded in NATO agencies in Europe (Figure 18, 19).

LEVEL-2: This level features a device for the active filtration of GPS L1 band interference using the null-steering technique. This option is targeted at clients using the American GPS L1 band at a frequency of 1575.42 MHz as a reference time source. It effectively filters out jamming of this band emitted on Earth. The filtered GPS signal becomes a fully valid time reference signal. The filter introduces a slight delay of several nanoseconds, which synchronization system designers can account for in the next level (LEVEL-3) or from the level of the NTP/PTP time server (IEEE1588 grandmaster clock).

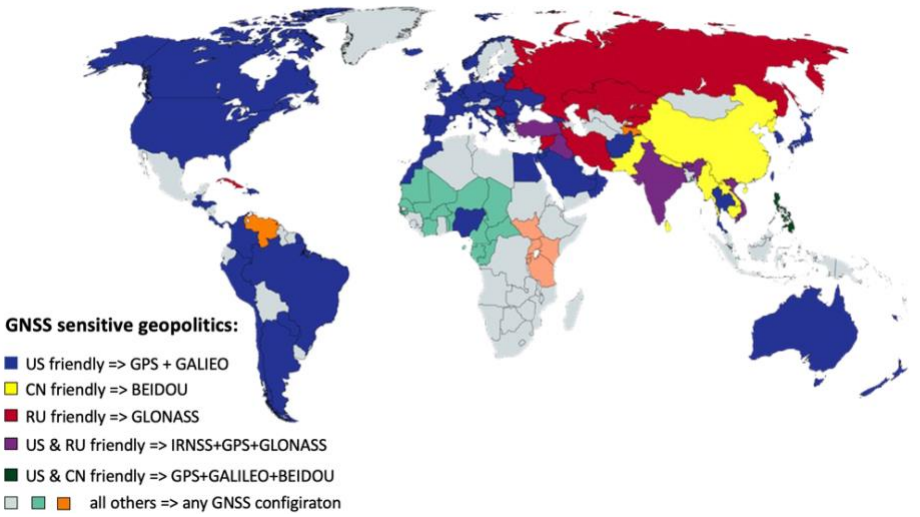

Fig. 20. Geopolitical Map Seen as BIOS of Trust in Satellite Systems: GPS+GALILEO, GLONASS, BEIDOU (without IRNSS).
Source: self-produced

LEVEL-3: This level features a GNSS-firewall class device. It includes a GNSS signal simulation layer, separating the NTP/PTP (IEEE1588) time server from physical access to GNSS satellites. The simulated GNSS signal at the output is based on the time maintained in internal oscillators or can be provided via a computer network from remote NTP servers. Deciding which time source LEVEL-3 should use is an advanced technical solution that constitutes the unique know-how of the Polish company ELPROMA. The Polish LEVEL-3 device is identified as full name "**SafeTime GNSS Guard LEVEL3"** and can independently receive cryptographically authenticated reference time over the network from the Central Office of Measures (NMI) or from local atomic clocks, including cesium 5071A. The ELPROMA has unique technology for obtaining and distributing the UTC scale directly from atomic Cesium clocks Microchip 5071A (formerly HP/Agilent 5071A) and from the HROG-10 microstepper by Spectra Dynamics USA.

TIME-SERVER: This is the main device responsible for synchronizing all elements operating within the computer network. It is a component of the fail-safe synchronization system, where the clock function is duplicated through aggregation. In the case of the Polish company ELPROMA, the NTS-5000 Rubidium (Rb) NTP/PTP time server fulfills this role excellently. An important principle applied when designing synchronization systems resistant to manipulation and cyberattacks is the philosophical principle of using multiple time sources simultaneously consisting of at least the following groups:

- A reference from a GNSS constellation
  (e.g., GALILEO supported by the American GPS)
- Built-in holdover oscillators (Rubidium, OCXO)
- An external official time source provided via the network (e.g., eTime or NPL-Time)

All within the configuration supported by LEVEL 1-3 protections described above on figure 18 and figures 21-23.

Additionally, it is worth mentioning the "galvanic informational" isolation between the NTP/PTP time server level and the synchronized network devices operating within an internally isolated network infrastructure shielded from the Internet. Such isolation is introduced when multiple LAN subnets use the common resource of a single time server. In this case, an additional SUBMASTER server level (previously referred to as slave) should be added and synchronized.

Example Application Schematics for Attack-Resistant Synchronization Systems:

In the simplest protection model (Figure 21), both physical antennas with GNSS receivers are physically separated by a distance of at least 200 meters, ensuring effective protection against amateur jamming devices (GNSS jamming). It is crucial to ensure that the interchangeable GNSS receiver modules in the antennas come from different qualified suppliers. Attention should be paid to the asymmetry of the antenna path. One of the antennas is directly connected to the time server, while the other passes through the LEVEL-3 simulator, which deactivates the receiver (antenna) and switches to holdover mode, delivering time from internal oscillators in case of a TAS attack. The LEVEL-3 device simulates the GNSS time signal to the actual time server, creating an aggregation of two clocks. The Elproma NTS-5000 time server (grandmaster) indirectly synchronizes network devices through the same server configured as SUBMASTER (previously so-called the SLAVE). This setup ensures "galvanic informational" isolation and establishes another level of clock aggregation for one of the many distributed synchronization nodes.

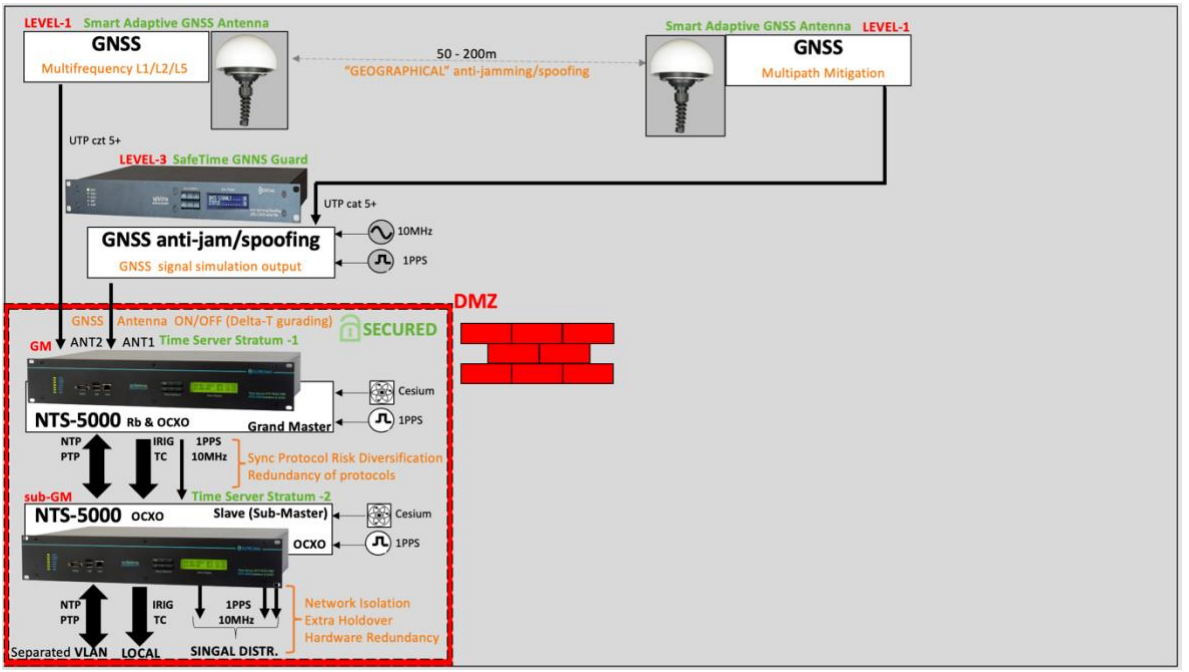

Fig. 21. Simple Sync. Model Using 2x GNSS Receivers LEVEL-1 and optionally LEVEL-3
Source: self-produced

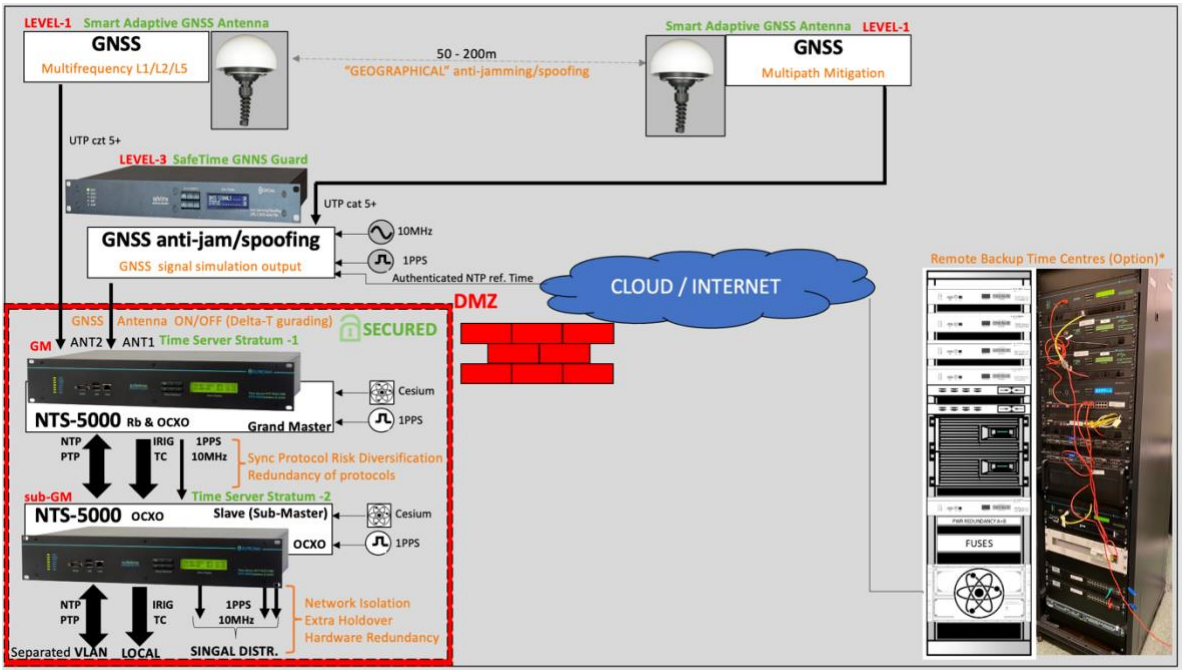

Fig. 22. Mid-Level Security Synchronization Model. The Solution Uses 2 GNSS Receivers (LEVEL-1) and a Satellite Simulator LEVEL-3 Powered by, e.g., eTime from NMI.
Source: self-produced

In the most complex protection model (Figure 23), an active LEVEL-2 filter is added to the path with the LEVEL-3 GNSS simulator (satellite firewall). It is important to note that the principle of asymmetrical configuration of the antenna paths (number and type of devices used in each antenna path) is still maintained.

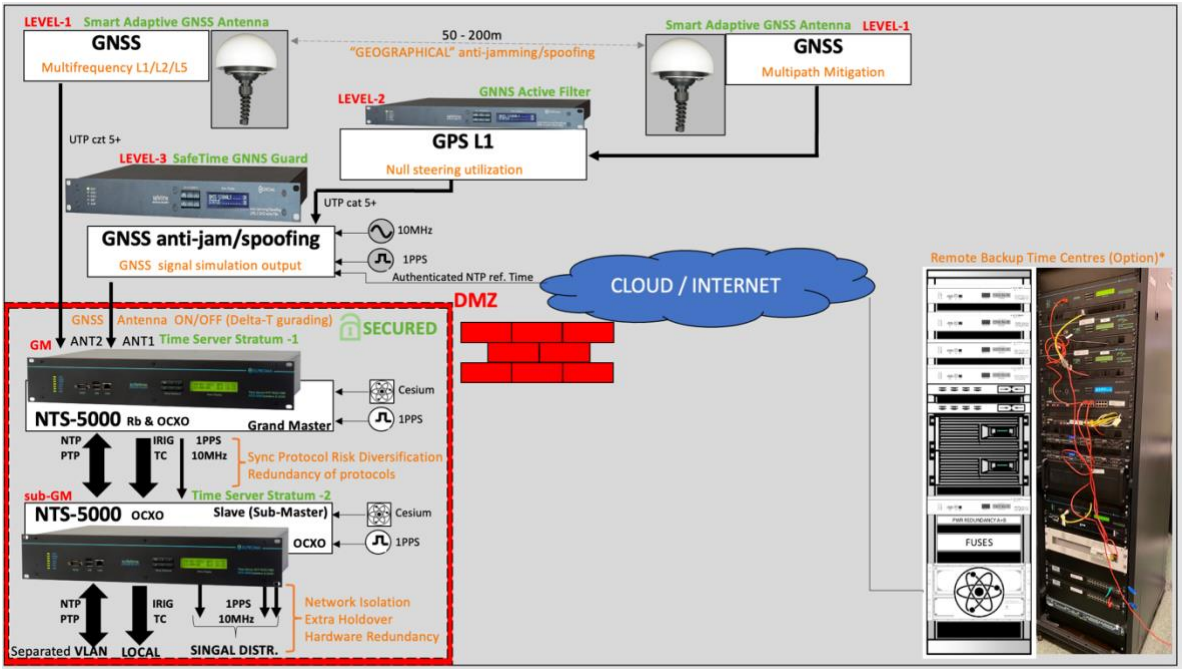

Fig. 23. Advanced Security Synchronization Model.
The Solution Uses 2x GNSS Receivers (LEVEL-1), Active GPS L1 Filters (LEVEL-2), and a LEVEL-3 Simulator Powered by the Backup Time Center at GUM (e-CzasPL Project)
Source: self-produced

The priority in building a time management system is the fundamental assertion that secure synchronization cannot rely on a single time server. As a necessary minimum when constructing such systems, it is considered essential to use multiple time servers within a single node, configured to work in a redundant setup and also ensuring clock aggregation.

Fig. 24. "Clepsydra " Time Synchronization System Node at the Polish Air Navigation Services Agency (PANSA), a Part of the Distributed Synchronization Architecture Possessed by PANSA in an Intercity Convergence Setup. The Presented Node Contains 5x NTS-5000 Class Servers, Including One Atomic Server linked to Cesium Atomic Clock.
Source: self-produced

Fig. 25. Front Panel View of the Elproma LEVEL-2 Active Filter. The Device Filters GPS L1 Interference of Jamming/Spoofing Class Using Null-Steering Technique.

Fig. 26. Front Panel View of the Elproma LEVEL-3 GNSS Simulator. This Network GNSS Simulator Receives Information from Remote NTP/PTP Servers at GUM RP (eCzasPL) and Converts it into a Simulated Antenna Signal for the NTS-5000 Time Server.

LITERATURE

[1] ITU-News Nr 02 2023 (kwiecień 20203) „The Future of Coordinated Universal Time", (strona 28 T. Widomski "The impact of UTC on Industry 4.0")
[2] California State University „Time Synchronization Attack – Pulse Delay Attack".
[3] DEMETRA H2020 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.
[4] DEMETRA Consortium, "DEMETRA a time service demonstrator", presentation presented at International Timing & Sync Forum, Prague, 1–3 November 2016.
[5] DEMETRA Consortium, "The European DEMETRA Project: demonstrating time services based on the European GNSS", abstract submitted at the 32nd International Union of Radio Science General Assembly & Scientific Symposium, August 19–27, 2017, Montreal, Canada.
[6] DEMETRA Consortium, "The H2020 European Project DEMETRA: Experimental Time Services based on European GNSS Signals", abstract submitted at the European frequency and time forum & international frequency control symposium, Besancon, France, July 2017.
[7] E. Shereen, „Security of Time Synchronization for PMU-based Power System State Estimation: Vulnerabilities and Countermeasures", Doctoral Thesis in Electrical Engineering, KTH Sweden Royal Institute of Technology, 2021.
[8] M. Smache, A. Olivereau, T. Franco-Rondisson, "Time Synchronization Attack Scenarios and Analysis of Effective Self-Detection Parameters in a Distributed Industrial Wireless Sensor Network", in: 17th International Conference on Privacy, Security and Trust (PST), IEEE, 2019.
[9] Mingyu Han, P.A. Crossley, "Vulnerability of IEEE 1588 under Time Synchronization Attacks", IEEE Power & Energy Society General Meeting 2019.
[10] P. Defraigne i inni, "Demonstrator of Time Services based on European GNSS Signals: The H2020 DEMETRA Project", w: *Proceedings of the 48th Annual Precise Time and Time Interval Systems and Applications Meeting*, PTTI 2017, pp. 127–137, Institute of Navigation ION, 2017.
[11] 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.
[12] P. Tavella i inni, 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.
[13] P. Tavella i inni, 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).

[14] P. TavellaiI inni, "Security Aspects Related to Synchronization at Power Gird", DG-Energy, EC Brussel Security.

[15] P. Tavella, T. Widomski, K. Borgulski, J. Kowalski, J. Uzycki i inni, "The Horizon 2020 DEMETRA project: DEMonstrator of EGNSS services based on Time Reference Architecture", w: *2015 IEEE Metrology for Aerospace* (*MetroAeroSpace*), 2015.

[16] W. Alghamdi, M. Schukat, "Precision time protocol attack strategies and their resistance to existing security extensions", *Cybersecurity*, Vol. 4 (2021).

[17] Weiyu Gao, Hong Li, Jianfeng Li, Mingquan Lu, "GNSS Time Synchronization Attack Detection and Discrimination Based on Correlations of Calculated Clock Drift Time Differences", w: *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, September 2020, pp. 3854–3865.

[18] T. Widomski, J. Uzycki, K. Borgulski, J. Kowalski, "Trusted Time Distribution with Auditing and Verification Facilities Project TSI#2", *Conference Precise Time and Time Interwal Meeting*, January 2016, Monterey, California.

[19] T. Widomski, K. Borgulski, J. Uzycki, J. Kowalski, "Robust Synchronization, Trusted Time Distribution with Audit and Verification Facilities", *ESMA MiFID*, London, UK, 2017.

[20] Ziyang Guo, Yuqing Ni, Wing Shing Wong, Ling Shi, "Time Synchronization Attack and Countermeasure for Multi-System Scheduling in Remote Estimation", Cornell University 2019.

[21] E. Varriale, Q. Morante, "Synchronet service demonstration results in DEMETRA H2020 Project: A scalable high performances synchronization solution", ION PTTI 2017 Conference, Monterey, California.