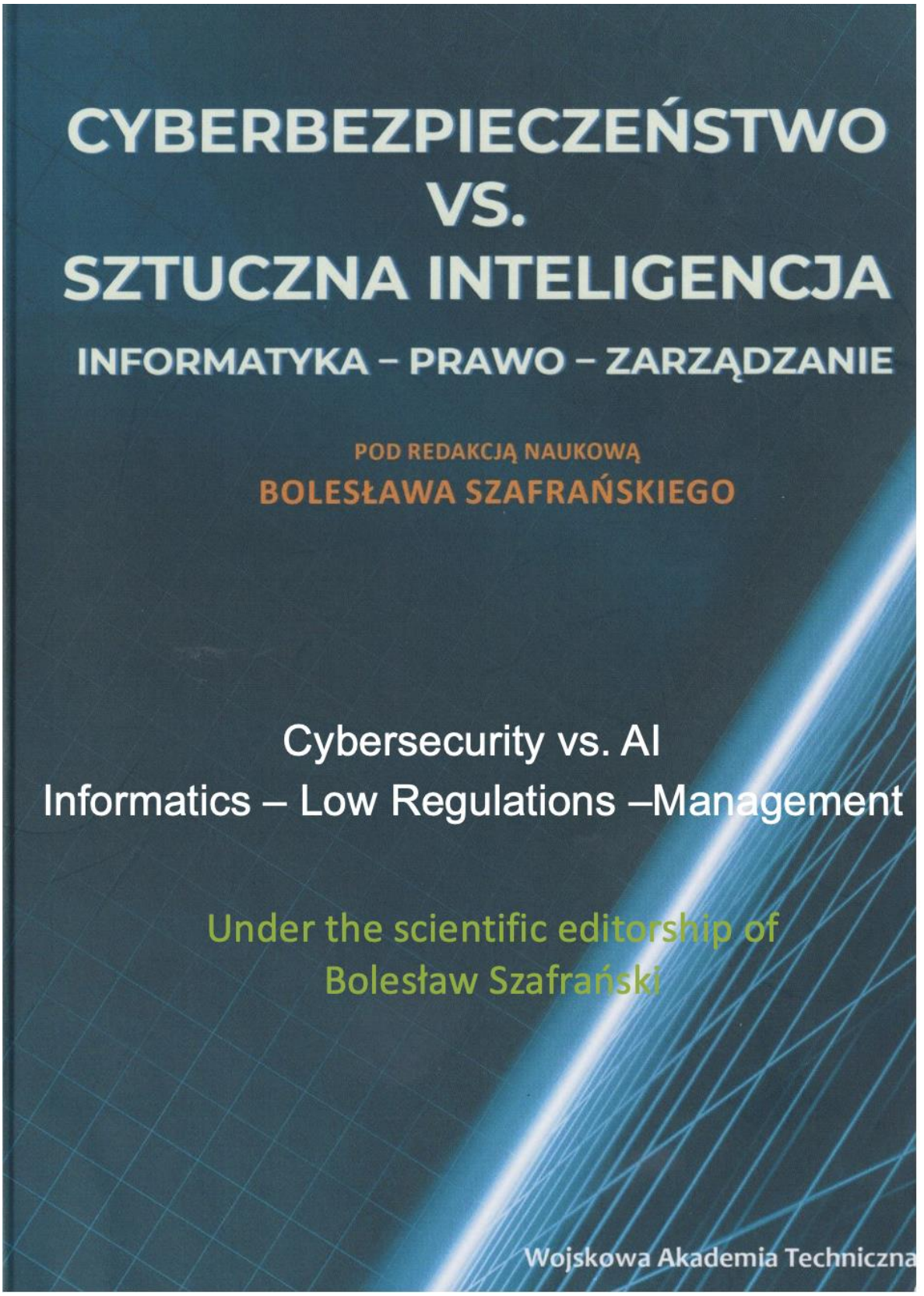

CYBERBEZPIECZEŃSTWO
VS.
SZTUCZNA INTELIGENCJA
INFORMATYKA – PRAWO – ZARZĄDZANIE
POD REDAKCJĄ NAUKOWĄ
BOLESŁAWA SZAFRAŃSKIEGO
Cybersecurity vs. AI
Informatics – Low Regulations –Management
Under the scientific editorship of
Bolesław Szafrański
Wojskowa Akademia Techniczna

Cybersecurity vs. Artificial Intelligence
Chapter XV

Desynchronization of IT/OT Critical Infrastructure – How to Monitor and Prevent

Tomasz Widomski
ELPROMA Elektronika Sp. z o.o.
05-152 Czosnów, ul. Duńska 2a

Artificial Intelligence (AI) is playing an increasingly significant role in computer science, also in the context of researching the originality of GNSS satellite signals as sources of PNT telemetry for determining position (P), navigation (N), and time (T) in receivers operating on Earth. This supports the detection of threats such as GPS jamming and spoofing and helps locate sources of interference. Until now, this area has remained within the interests of defense, but the growing dependence of civilian IT systems and control automation in Industry 4.0 (OT) on GNSS satellite techniques forces a redefinition of security threats. We will look at where AI-based technologies are used to interpret events related to GNSS, as well as the challenges posed by threats associated with GPS jamming and spoofing in ensuring the stability of critical infrastructures, as described by the latest EU security policy[1]. The author encourages readers to refer to literature[2] [1], which is an important introduction to the topic discussed here. This chapter includes extensive excerpts from the author's MBA Cybersecurity thesis titled 'Analysis of the Phenomenon of Time Desynchronization as a New Cyber Weapon Destabilizing State Critical Infrastructures' (WAT – Warsaw Military University of Technology, June 2024) [15].

1. Introduction

Russia's actions, involving the jamming of GPS in Syria and Ukraine, have revealed significant operational capabilities of Russia beyond the area of military operations. It appears that skillful disruption of GNSS signals can be an effective weapon. This allows blocking the PNT functions of any satellite receiver on Earth, and in conditions of hybrid operations, it can effectively support the destabilization of a nation's critical infrastructures. In the event of a conflict, it may therefore impact NATO's logistical depth. This has become possible due to the excessive dependency of IT/OT systems on PNT functionalities, especially on the GPS satellite system, but also other systems of the GNSS family (Figures 1 and 2).

[1] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en.

[2] W. Paluszyński, T. Widomski „*Underestimated Threat – Source and Distribution of Time*", [in:] B. Szafrański "*Cybersecurity – redefining Threats"*, page. 177–214, pub. WAT, Warsaw Poland (EU) 2023.

Fig 1. The stability of NATO's logistical depth depends on rail traffic management systems, which rely heavily on GPS. The failure of NTP time servers on March 17, 2022, halted train operations in eastern Poland, Source: *Elproma presentation at the 5th "Railway Safety" conference (EU, Poland, Gdynia, December 2023)*

Fig. 2. Stable synchronization of distributed OT systems is essential for coordinating production processes in Industry 4.0. Additionally, the air defense systems protecting this industry also rely on such synchronization. This impacts the stability of logistical depth during armed conflicts.
Source: Adobe license for press and books

The Industry 4.0 revolution and the ongoing digital transformation increase the level of threat to the stability of IT systems by introducing strong, invisible connections between various IT and OT solution groups that were previously independent (see Figure 3). Today, the scenario of a crisis escalation based on deliberate GPS signal interference, and consequently the desynchronization of an increasingly large and dispersed IT architecture, should be taken into consideration (see Figure 4).

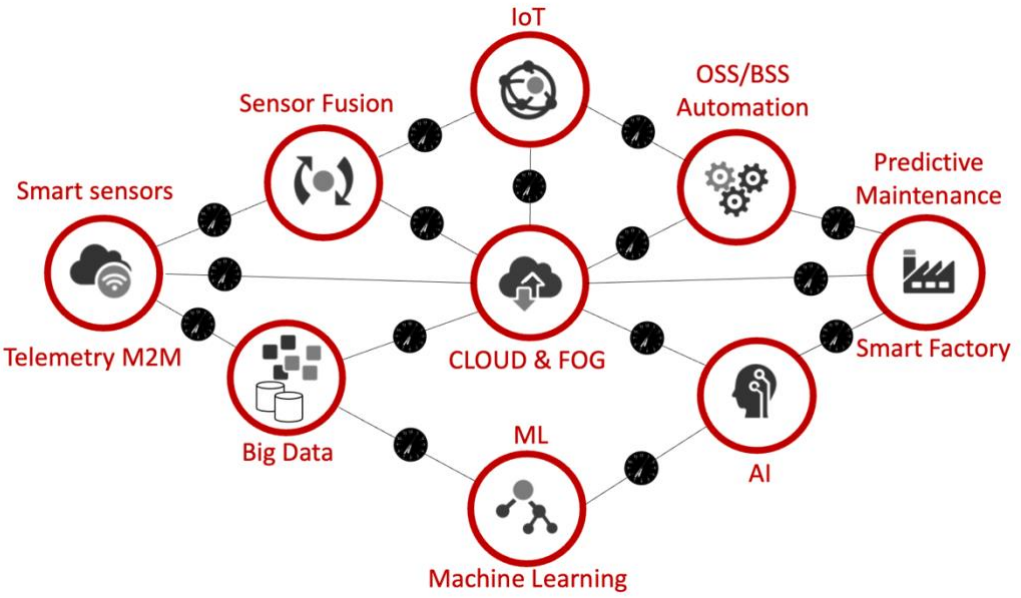


Fig. 3. Correlated interdependence of system groups in Industry 4.0 within the UTC time domain.
Source: Own work presented at the ITSF 2021 conference in Brighton, United Kingdom.
Source: *Original work for MBA Cybersecurity at Military University of Technology (WAT).*

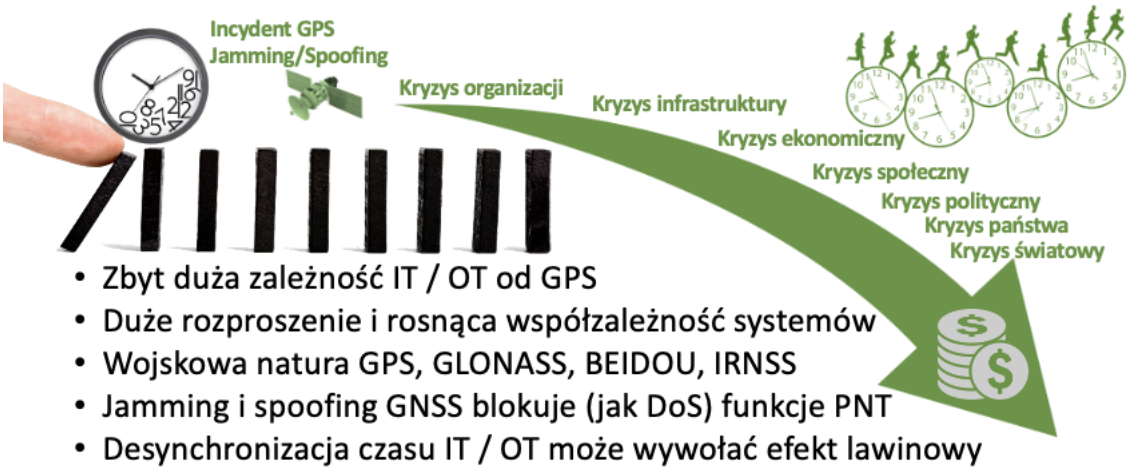
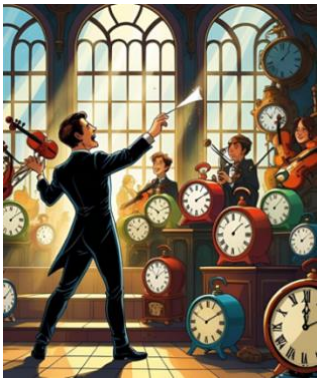


Fig. 4. GPS jamming incident introduces the risk of a cascading effect of technical failures in IT and OT, leading to an escalating crisis.
Source: *Original work for MBA Cybersecurity at Military University of Technology (WAT).*

In modern technology, it has become evident that destabilizing entire IT/OT systems by manipulating time (through low-level adjustments of software clocks in operating systems and device firmware) is simpler than hacking into well-secured, isolated internal networks. Critical infrastructure networks rely on precise timing to synchronize their resources. Accurate time coordination functions like an orchestra conductor, harmonizing the operations of independent communicating devices. This ensures the functionality of solutions based on the fusion of individual network elements, efficiency (optimal resource utilization), and stability, which is responsible for the reliability and security of every distributed modern IT/OT architecture. Synchronization can be relatively easily manipulated, for instance, by using GPS jamming and spoofing, on which technology has become overly dependent in recent years. All sectors of the economy and their supporting infrastructure networks, as described by the EU NIS2 Directive, are vulnerable:



- **Energy** (renewable/atomic/fossil/biomass, smart metering, smart grid, lte/5G etc.)
- **Transport** (aviation, rail, road, port management)
- **Banking** and insurance
- **Stock and commodity exchanges**
- **Public health**
- **Water** (production and distribution)
- **Waste** and pollution (disposal)
- **Digital infrastructure** (DNS servers, routers, networks, cloud and data centers)
- **Public administration** (related to digital transformation and paperless processes)
- **Defense** (military, space industry, science)
- **Food** (production, processing, and distribution)

Desynchronization of IT/OT infrastructure networks can lead to failures with unpredictable consequences. There are increasing warnings about the specter of a major failure that could trigger a domino effect. Therefore, synchronization has become an element of cybersecurity. The risk of effective use of GPS jamming and spoofing cannot be overlooked. The rigor of maintaining synchronization discipline is imposed by recommendations from ITU, IEEE, ESMA/SEC. They define time and frequency (T&F) parameters and requirements for maintaining them within increasingly precise limits. For example, in smart grids, time accuracy is specified by the IEEE C37.238 document, which requires time servers to have an accuracy better than 200 nanoseconds (ns). Within 5G infrastructure, an accuracy of UTC relative to GPS greater than 10 nanoseconds is needed to maintain device synchronization levels below 1 microsecond (μs) over a large area of the country. The T&F accuracy parameters for 5G telecommunications are defined by the ITU SG15 and its work cooperate to ITU WP7A, responsible for the UTC time scale. Failure to meet the recommendations threatens the stability of logical bands in fiber optics and radio BTS, affecting the performance of the entire 5G network. In the case of terrestrial DVB-T2 television, desynchronized BTS will automatically shut down, cutting off access to television

in the region. The financial sector is subject to the ESMA MiFID II directive. On stock exchanges, the phrase "time is money" has a literal meaning and a very measurable value of losses. Automated HFT (High Frequency Trading) investments are subject to the rigor of ensuring 100 μs UTC accuracy for all financial exchanges worldwide. For this reason, the server rooms of the American company Equinix are synchronized with an accuracy oF 1 μs. This is the maximum error between the east and west coast server rooms of Equinix in the USA requiring nanosecond synchronization of backbone. A summary of the required accuracies is illustrated in the table (Figure 5).

However, we often underestimate not the significant ones, but those seemingly minor millisecond (ms) accuracies of solutions operating around us. We forget that synchronization determines the completeness of transactional SQL database backups. Correct time and date are used in SSL authentication certificates and encryption, including VPN. Even blockchain requires certain small synchronization accuracies. Such accuracy reminds crucial for Microsoft Active Directory authentication that needs synchronization to prevent replay cyber-attacks. Correct time determines the chronology of event recording in LOG journals. Lack of chronology in LOGs makes it forever impossible to identify the cause of a failure. Timestamps are used in the operating system's file system and in the OS kernel. In most cases, the underappreciated role of time results from the hidden functions it performs in the background of the operating system (e.g., managing concurrency, organizing RAM resources, file defragmentation). Who among us remembers on a daily basis that synchronization is important during the boot phase of software loading in a multiprocessor environment (CPU).

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	★★★	★★★

Fig. 5. Comparison of the accuracy of NTP, PTP, PTP+PTM, and White Rabbit protocols.
An overview of the precision requirements across segments and the desired resilience to threats.
Source: *Network Time Foundation in collaboration with EUSPA*.

Today, precise time is no longer solely a matter of national metrology institutes (NMI), but also constitutes a significant factor connecting information technology (IT) and operational technology (OT), affecting their security and performance. Therefore, desynchronization has become a modern cyber weapon. The degree of threat varies. It depends on the complexity, type of distributed architecture, and the legally required maximum permissible time error. The greater the required accuracy and stability of synchronization, the more susceptible the solution is to desynchronization attacks. In most IT and OT systems, distribution is understood in terms of external vastness, but it can also mean an increase in internal complexity within the boundaries of a single device or system (Figure 6).

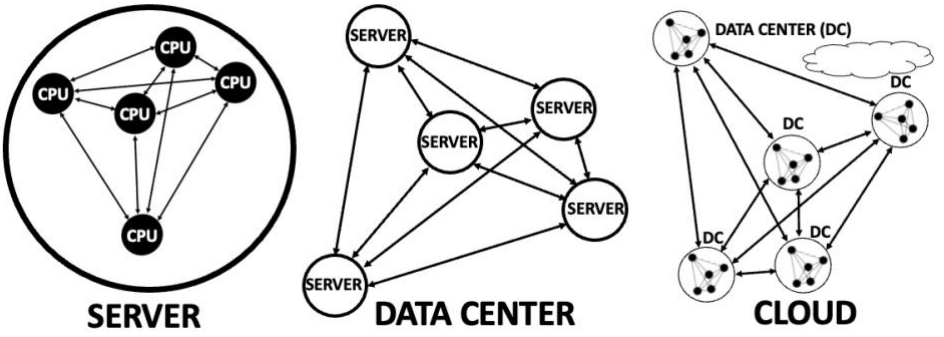


Fig. 6. (a) internal distribution (b) distributed LAN/WAN network (c) complex hybrid model
Source: *self-prepared*

A simple example of an external distributed architecture is a classical computer network (Figure 6.b), where computers and other devices are connected to exchange information. Distribution can also be considered an internal feature of a single device. Examples include multiprocessor disk array controllers, motherboards, and modular server clusters (Figure 6.a). There are also complex hybrid distribution models that combine both external and internal elements into a multi-level, often highly complex structure. An example is the cloud (Figure 6.c). Cloud synchronization is a real challenge because it encompasses many levels, from the nanoscale of multiprocessor disk controllers, through network devices, to the distribution of entire data centers using variable-time encryption to protect communication channels. A forgotten feature of the cloud is equal data access time, independent of the physical location of the user (access point). Conversely, the proper partitioning of data (fragmentation), compression, duplication of backups, and their global distribution give the cloud the ability to recover lost information even in the event of very large failures.

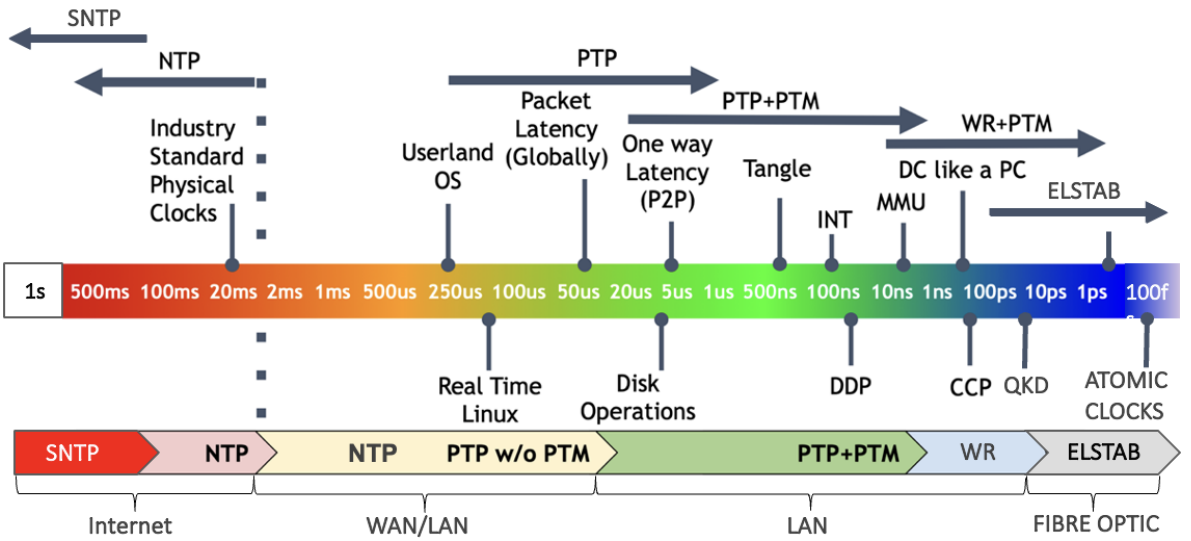


Fig. 7. Comparison of synchronization protocols: NTP, PTP, PTP+PTM, and White Rabbit (W*R)*.
Source: *Ahmad Byagowi (Facebook). Update by Tomasz Widomski (Elproma)*

Therefore, the synchronization of IT/OT distributed architecture is based on a hierarchical model of software clocks operating at the kernel level of operating system (OS). The synchronization network topology may differ from the physical network topology and other logical TCP/IP data flow, although both are based on the same physical backbone network. An example of such differentiation is the IEEE1588 PTP (Precision Time Protocol) synchronization protocol, which can operate simultaneously (independently) from the NTP (Network Time Protocol). Both protocols are susceptible to desynchronization. The PTP protocol meets the demand for high accuracy, while NTP handles the lower accuracies (Figure 7). High single nanosecond and picosecond level accuracy requires the use of special dedicated network interface cards (NICs), Ethernet switches and in some cases dedicated leased lines – the dark fibers. For this purpose, so-called hardware timestamping is used. This involves calculating and correcting the delay introduced by the operating system until the data is sent over the LAN (UDP). PTP configuration ensures nanosecond (ns) accuracy, and in the case of White Rabbit (WR), can even achieve a picosecond (ps) accuracy. Since 2020, all OCP (Open Computing Project) cloud operators, including Facebook, Microsoft, Google, AWS, etc., have begun the process of implementing IEEE 1588 PTP while maintaining NTP redundantly as a backup synchronization protocol. Some cloud operators like e.g. Cloudflare offers NTS secured NTP synchronization, as a public service to its users and customers.

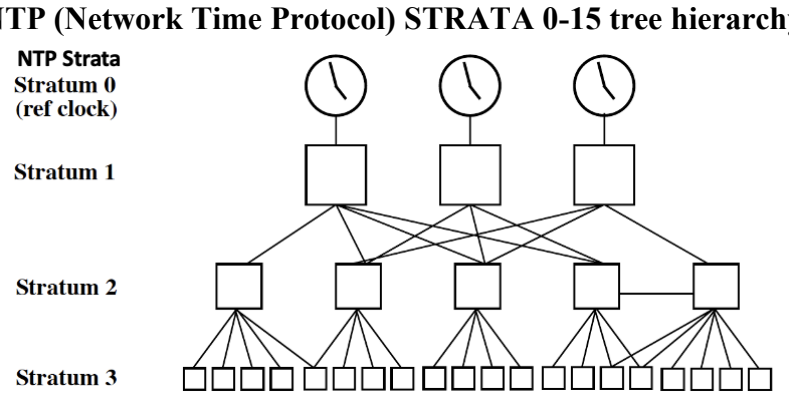


Fig. 8. STRATUM 0-15 tree topology of NTP synchronization
Source*: self-prepared*

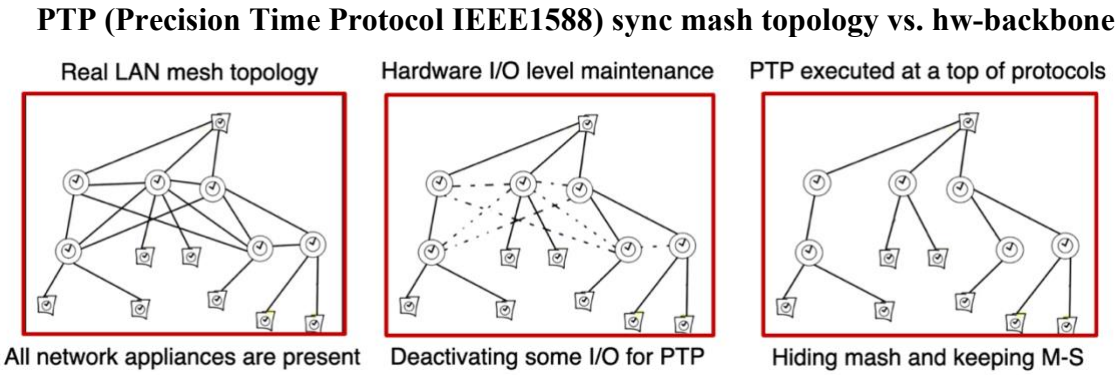


Fig. 9. Physical network topology vs. PTP synchronization topology. The transmission of regular data and PTP synchronization packets should occur via different paths.
Source: *self-prepared*

2. Underrated Threat – Source and Distribution of UTC Time

Desynchronization, in other words, is the loss of synchronization of the clocks. All modern IT/OT devices connected to a computer network are equipped with a hardware RTC clock for timekeeping when the device reminds in power off and no operational mode. Every modern operating system, including Windows and Linux, have a software clock at the kernel level that requires synchronization to UTC time scale. According to Wiesław Paluszyński[3] from the Polish Information Processing Society, desynchronization poses a serious threat[4] to modern critical infrastructures because it can disrupt operational parameters at various levels of hardware, system software, communication, and applications. This can be compared to arrhythmia in the human body. Desynchronization in IT and OT can lead to reduced communication efficiency, functional irregularities of the solution, and, in extreme cases, critical system-wide failures or blackouts

Table 1. Comparison of the impact of heart arrhythmia on the human body and desynchronization disruption of GPS

Heart Arrhythmia (human body)	GPS Disruption (critical infrastructure)
• Organ failure, • Illness or collapse, • Death	• Reduced performance of IT/OT systems, • Incident or failure • Critical failure - infrastructure blackout

The desynchronization of clocks in network devices connected to the network also indirectly leads to disruption of the correctness of delay calculations in the flow of information. This is reminiscent of the problem faced by messengers in the great Mongol Empire of Genghis Khan in the 13th century, where information relayed to the ruler was already outdated due to the vast distance to be traveled, and the conquered territories could have been lost again by then. In the case of industrial OT systems, this can lead to the use of outdated data and rejection of accurate information. Consequently, IT systems increasingly controlled by AI prediction may make incorrect management decisions. The inspiration for predictive control came from industrial QoS (Quality of Service) systems utilizing machine learning. By closing the analysis of read data in a feedback loop (PLL), a predictive control mechanism was created, allowing the prediction of future states and precise adjustment of control parameters accordingly. Furthermore, disrupting the chronology of events logged in the LOG creates a paradox where the effect may precede its cause. This will make logical error analysis impossible, ultimately preventing the determination of the true cause of failure. It presents a new type of threat and defines two types of new cyberattacks:

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

[3] [3] W. Paluszyński, T. Widomski „*Underestimated Threat – Source and Distribution of Time*", [in:] B. Szafrański "*Cybersecurity – redefining Threats"*, page. 177–214, pub. WAT, Warsaw Poland (EU) 2023.

[4]Interview w/ PTI, Wiesławem Paluszyńskim dla eCzasPL: https://youtu.be/smRxpEoyEDw.

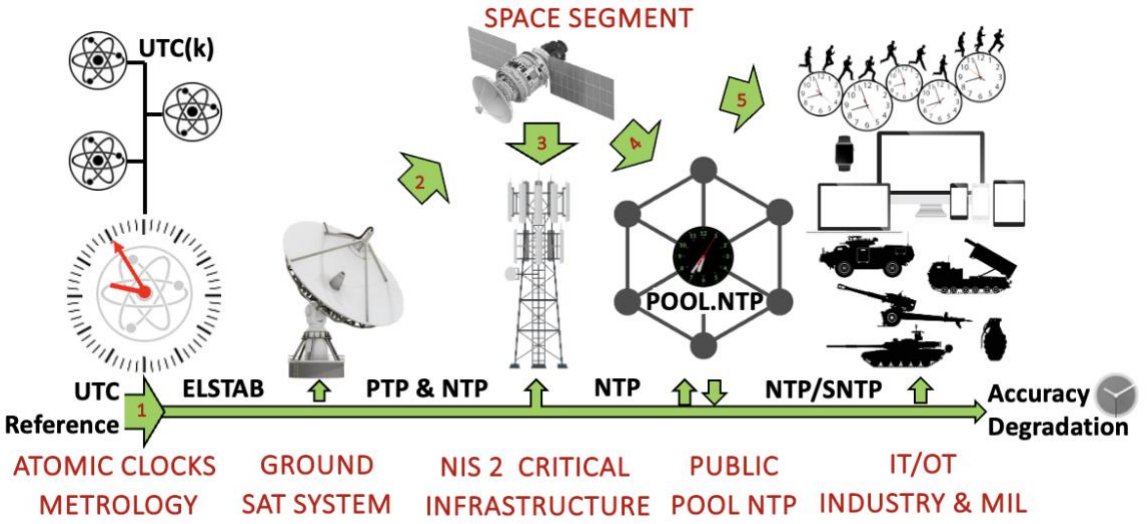


Figure. 10. The structure of UTC generation and distribution from left to right (from step 1 to 5), from the creation in the national metrology laboratory NMI, through distribution via Fiber Optic Ethernet networks and RF radio (e.g., GPS or LW), to intermediary UTC public redistribution (e.g., public NTP POOL), and finally to end-users (industry, administration, business, military). Source: self-prepared

Computer technology relies on the so-called universal time scale UTC[5]. It is not the only time scale, but it is one of the most important for our civilization. It is used in the kernel of operating systems (OS) such as Windows, macOS, Linux, Unix, and their derivatives. These systems automatically adjust the user desktop time to the current time zone, but somewhere deep inside kernel of the OS, they do not distinguish their geographical location and use the consistent UTC time. Local time zones are important for us humans and remain irrelevant to machines. UTC has an irregular nature resulting from the well-known problem of leap seconds[6]. These leap seconds, added (if positive) or subtracted (if negative) very irregularly, aim to compensate for the difference between observable astronomical time, such as historic GMT[7], and the very stable time kept by atomic clocks defining the second's standard. The Earth's rotation is influenced by atmospheric friction, changes in the geological structure of a tectonic nature, convective movements of the Earth's liquid core, changes in the location of water resources (including the melting and movement of glaciers), the weakening of the Earth-Moon gravitational interaction (as a result of the Moon moving away from the Earth by 2 cm per year) etc.

There are currently 37 such UTC leap seconds. Each new leap second, whether positive or negative, poses a significant cyber threat to IT/OT network devices, which do not know how to handle this single second without desynchronizing the entire information system. The problem is so severe that it led to an informal code of silence among the major Silicon Valley players gathered at the Open Computing Project (OCP). In December 2015, due to the upcoming leap second, Cisco issued a notice recommending users to turn off their Catalyst routers a few hours before midnight UTC and to turn them back on the next day.

[5] https://en.wikipedia.org/wiki/Coordinated_Universal_Time.
[6] https://en.wikipedia.org/wiki/Leap_second.
[7] https://en.wikipedia.org/wiki/Greenwich_Mean_Time.

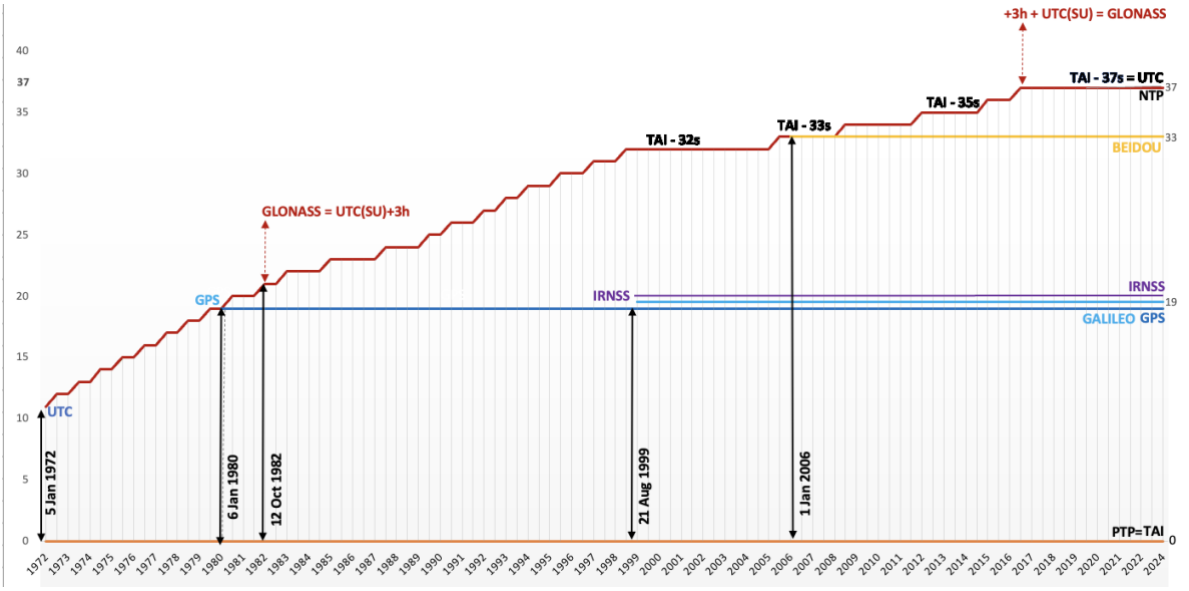


Fig. 11. Comparison of UTC, TAI, NTP, PTP, and internal satellite GNSS time scales. Source: self-prepared, based on 2024 data

The UTC scale contains "time gaps" caused by the presence of each of leap second. These are responsible for the step-like (discontinuous) characteristic of the UTC (Figure 11). The lack of a standard for handling UTC leap seconds causes the desynchronization within IT/OT infrastructure. Some systems lose this second smoothly in “slew adjustment”, while others in jumps (so-called “step adjustment”), creating a maximum error of 1 second. Older radio standard like German DCF77 does not support negative leap second that will possibly provide a 2 second synchronization error inside IT that bases on this specific reference.

Unexpected errors larger than a second are possible too and result from numerical overflows inside GPS receivers and directly involving NTP/PTP network time servers. This raises the question of the technical possibility of indirectly influencing desynchronization to cause hardware and software failures in traffic control systems similar to the Polish Railways[8] failure on March 17, 2022. Furthermore, already during the announcement of the leap second via GPS, even several weeks before its introduction, dangerous large jumps measured in days, weeks, months, or even years can occur due to internal numeric overflows at firmware level. The largest documented synchronization error occurred on April 6, 2019, and amounted to 19.7 years. It was associated with the overflow and zeroing of the week counter sent to the receiver on Earth by the GPS telemetry system. This is a well-documented example of how data transmitted by radio can affect the instability of the satellite receiver. Similarly, by manipulating the announcement of the UTC leap second, it may be possible to affect the failure of entire IT/OT systems. This, in turn, can escalate a crisis, causing consecutive failures of dependent Industry 4.0 sub-systems. Desynchronization can cause blocking of encrypted cloud transmission channels, resulting in denial of access and rejection of valid SSL certificates and VPN protection. The first coming negative[9] UTC leap second can cause Linux “*kernel panic*” and Windows “*Blue screen of death*” - both ends with the OS halt.

[8] https://www.straitstimes.com/world/europe/technical-fault-halts-polish-railways-a-key-ukraine-exit-route.
[9] ITU News 2/2023, https://www.itu.int/en/itunews/Documents/2023/2023-02/2023_ITUNews02-en.pdf.

The UTC time scale is not uniform. It is a set of many UTC(k) co-created by NMI laboratories worldwide. The national UTC(k) scales differ slightly at the nanosecond level. With near each decade, these accuracies are improving by factor x10, as atomic clocks frequency steering algorithms systematically "learn" clock instability now by a direct fiber optic comparison. For example, the UTC(USNO) time scale for the GPS satellite system is the scale of the US Naval Observatory in the USA and will differ from laboratory UTC scales providing the standard to the GALILEO, GLONASS, BEIDOU, and IRNSS satellite systems. All will differ from Poland's official UTC(PL) time scale created by the Central Office of Measures. Besides UTC(PL), the second independent Polish time scale is UTC(AOS) supported by the astronomical observatory CBK in Borowiec. For comparison, Germany has up to four independent UTC scales, including two belonging to Deutsche Telecom T-Mobile. If more of autonomous time scales in a country than it increases industrial safety by creating backup, GNSS independent ref. UTC time sources that is very important for the security.

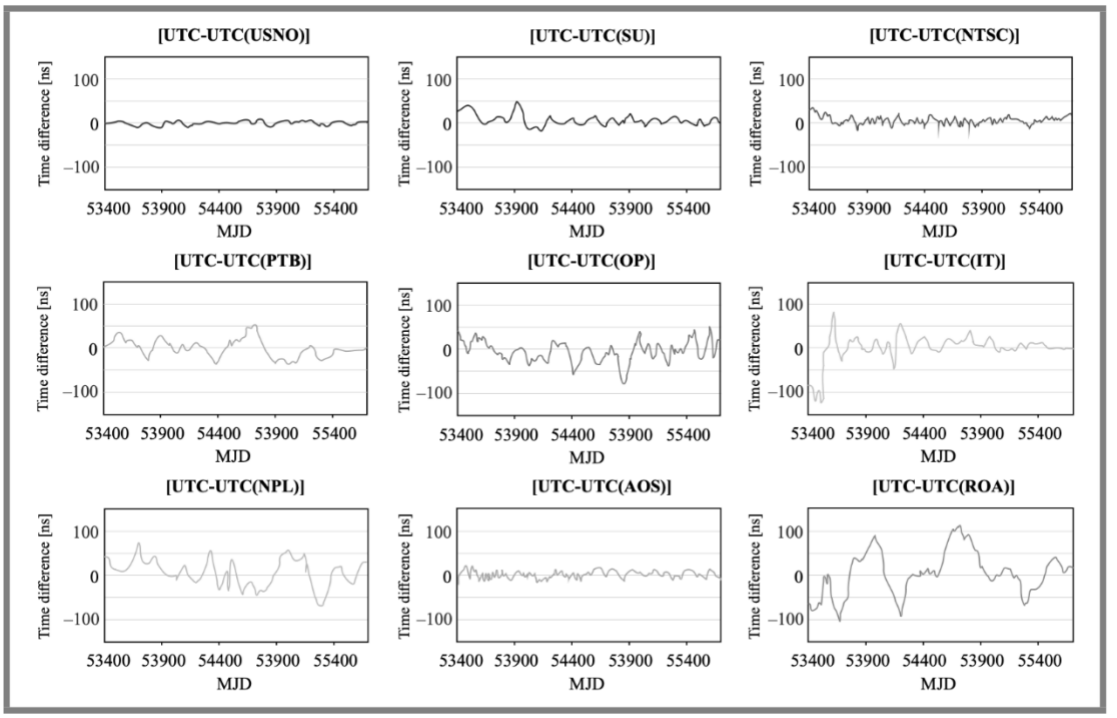


Fig. 12. The UTC scales of individual countries and laboratories differ in their characteristics. Source: W. Lewandowski, M. Marszalec – Polish Institute of Communications, Literature [4]

What significance do autonomous UTC time scales have for security? They are not dependent on the increasingly disrupted GPS, or any other GNSS constellation. Their direct use eliminates the risk of time manipulation through RF jamming and spoofing in the economy and prevents desynchronization of IT and OT systems in the industry. Autonomous UTC(k) time scales are also used for cyber-security testing of GNSS satellite receivers. The problem of security vulnerabilities in GNSS receiver has been described in literature [1]. There are commercial GNSS receivers on the market that do not operate according to the manufacturer's declaration. Many years ago, our attention to community was drawn to the company NVS[10] (Figure 13). It is registered both in Switzerland and in Russia.

[10] http://www.nvs-gnss.com/products/gnss-receiver.html.

The UTC pattern generated by the NV08C CSM receiver showed characteristics of coherence with the Russian UTC(SU) time scale (SU - Soviet Union). This is the base time-scale of the Russian military satellite GLONASS system. Despite the GALILEO name on the NV08 label, this unit does not support the European system; instead, it uses the Chinese BEIDOU.

Fig. 13. The GNSS receiver module from the "Swiss" (Russian) company NVS is sold globally, including by leading American electronic component distributors.
Source: Internet www.nvs-gnss.com

In general, it is very difficult to demonstrate that a GNSS satellite receiver configured to receive exclusively GPS is not "deceiving us" by instead following, for example, military enemy GNSS constellations. Using a GNSS simulator set to exclusive GPS mode should provide a definitive answer to the question of truth. The failure of this method (Figures 14) should be explained by the fact that the internal GNSS receiver firmware may recognize the pending GPS satellite simulation process, and the receiver will behave "properly" during such a test. If that could be a case, the risk of GNSS chipset security backdoor should be assumed, and more advanced time-scale oriented “fingerprint” testing is recommended (Figure 15).

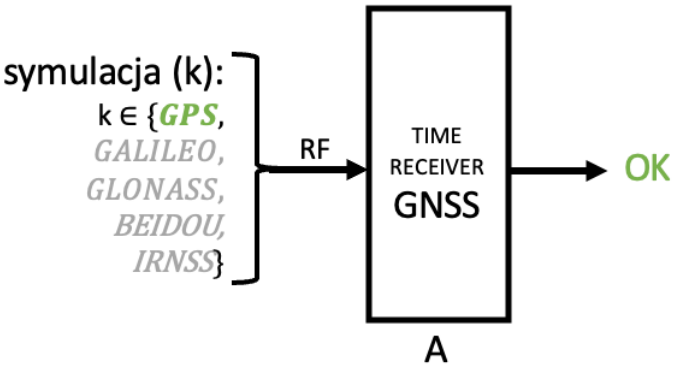


Fig. 14. The single-phase "A" testing scheme for GNSS receivers proposed by EUSPA in 2024. Setting the simulator to a selected single system (GPS, GALILEO, GLONASS, BEIDOU, IRNSS) checks whether it is supported by the tested receiver. Such a test does not detect security vulnerabilities if the receiver is "controlled" by a different system than expected (e.g., it is set to GPS, but the receiver still depends on the military GLONASS).
Source: Internet

The true intentions of the GNSS receiver will only be revealed through an extended test, where the EUSPA[11] testing scheme (Figure 14) constitutes the first phase "A" of a three-stage diagnostic structure "A-B-C" (Figure 15). Artificial intelligence (AI) assists in such testing.

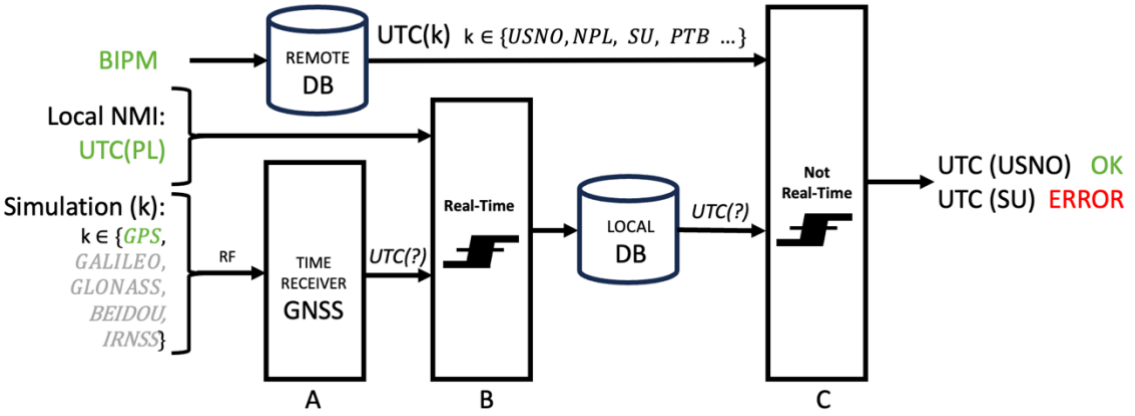


Figure 15. The three-phase "A-B-C" laboratory testing of the receiver, proposed by Poland in 2024, unequivocally confirms its hidden dependency on the undesirable GNSS system.
Source: ELPROMA for EUSPA

The extended three-phase “ABC” test of GNSS receiver scenario includes:

Phase A - extending the original test (Figure 14) by the two additional phases B, C (Figure 15). It allows more detailed analysis of the UTC output signal produced by receiver.

Phase B (Figure 15) serves as a “screening” or “volume” test and can be performed continuously in real time. The effectiveness of identifying security vulnerabilities in the tested GNSS receiver depends on AI algorithms supported by machine learning and the existing knowledge base of correlations between the UTC(PL) standard and other time scales recorded in the BIPM databases. This allows for a preliminary answer to the question of whether the AI-assisted test receiver is “pretending” to be under the authority of system k (e.g., GPS), while in reality, it may be subordinated to another enemy GNSS constellation.

Phase C is a “qualitative” examination of the receiver based on a retrospective comparative analysis of UTC(k)-UTC(PL) with the archive UTC(k) from BIPM databases. The result is provided with a one-month delay, as this is how long it takes for data to be collected from national metrology NMI laboratories to BIPM. In the hypothetical case analyzed, finding “fingerprints” of UTC(k) coherence provides a 100% certainty of the test receiver’s dependence on the military (enemy) satellite system. It is crucial to conduct the three-phase test A, B, and C, considering the events of:

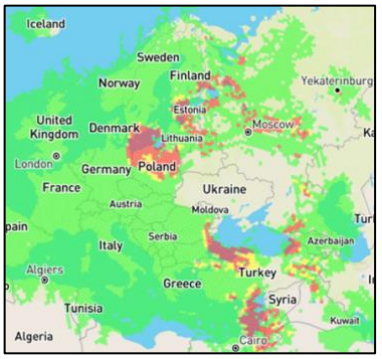
- **cold start of the tested GNSS receiver**
- **reacquisition of satellites by the tested GNSS receiver**

The tests should be conducted in a sandbox simulation environment with access to physical satellites and we should only examine the impact of individual GNSS constellations.

3. How to Monitor and Identify the Source of GPS Jamming?

In the released by Warsaw Military University of Technology book titled "*Cybersecurity- Redefining Threats"*, edited by professor B. Szafrański, the author of Chapter XII, titled *"An Underestimated Threat – The Source and Distribution of Time"*, W. Paluszyński from PTI, reviews various system desynchronization techniques, extensively illustrating different types of threats and the consequences of possible time attack (TAS) and delay attack (TDA). We encourage readers to explore this publication, as it provides an important introduction to this and next sections.

We will focus on a specific threat: the desynchronization of IT/OT systems using satellite signal jamming techniques, specifically targeting the GPS system. A key source of information on GPS signal disruptions has recently become the online service - *gpsjam.org*, which displays a map of areas where GPS reception anomalies have been reported by air traffic. On December 26, 2023, for the first time, red spots indicating interference appeared public on the GPS jamming map within Poland. That day, disruptions covered a vast area stretching from Denmark across the Baltic Sea to virtually the entire western coastline of Poland. Until that day Poland experiences near everyday GPS jamming and spoofing.



23/03/2024
https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-03-23
02/03/2024
https://gpsjam.org/?lat=41.49383&lon=44.65934&z=2.1&date=2024-03-02
14/02/2024
https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-02-14
02/02/2024
https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-02-02
19/01/2024
https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-01-19
16/01/2024
https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-01-16
26/12/2024
https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2023-12-26

Fig. 16. The first GPS interference over Poland was recorded 1st time on Dec. 26th, 2023. Source: *https://www.gpsjam.org*

German authorities have also admitted that GPS navigation signals have been seriously disrupted in the Baltic Sea region for some time. Consequently, the Federal Network Agency Bundesnetzagentur, responsible for, among other things, electromagnetic protection, initiated an investigation in cooperation with the Bundeswehr. German services have the capability to precisely locate sources of interference; however, no information regarding the results of the investigations has been publicly disclosed so far. Similar to the mentioned Swedish and Estonian services, German suspicions are directed toward the Kaliningrad region. For the Russian military, GPS interference is likely insignificant as they use their own military satellite navigation system, GLONASS, supported in synchronization by the ground-based Chayka[11] terrestrial radio system. For military operations, they can also utilize the support of a large number of dispersed public Russian time servers of the NTP POOL[12] network on the Internet. These can provide a UTC standard valid during the cold start and reacquisition of GNSS satellites.

[11] https://en.wikipedia.org/wiki/CHAYKA.
[12] https://www.ntppool.org/zone/ru.

The documented history of GPS interferences dates back to year 2011 on the Korean Peninsula. Subsequent cases were noted in the Shanghai region of China and the eastern coast of Russia. The escalation of the phenomenon has covered the Persian Gulf region and some European countries. GPS interference has been recorded in northern Norway bordering Russia, in the Black Sea basin between Crimea and Sochi, and interestingly also in Moscow[13], Libya, and Syria, where Russia has had military bases for some time. A gradual media narrative began to build that the world must be dealing with deliberate GPS system interference. In Poland, interference was noted by *gpsjam.org* on the December 26th, 2023.

Fig. 17. The first GPS interference was recorded in 2011 on the Korean Peninsula.
Later, it appeared on the coasts of China and Russia.
In subsequent years, in Norway, Israel, Syria, and after 2014 in the Black Sea region,
surprisingly also in Moscow.
Source: [3], CNN

Although there are many theories and attempts to explain Russia's alleged behavior, we do not even know the type of jamming that occurred in our territory. Generally, we know that there are two methods of GPS interference: jamming the original signal (GPS jamming) and spoofing the reception by providing false data that covers the original. The technique of radio retransmission called meaconing[14] is also used in this group.

Within the GPS jamming category itself, we can distinguish subgroups such as PRN jamming, CHIRP jamming, and CODED jamming. Similarly, for spoofing, there are subgroups like SYNCHRONOUS spoofing, CIRCLE spoofing, and meaconing[14] signal retransmission. At this stage, we point out a little-known fact in the media – weak jamming can cause a spoofing effect. Each receiver also reacts differently to threats. Independent research conducted by USNO [15] [16] and C4ADS [17] since 2016 indicated the location of the jamming source responsible for GPS jamming and spoofing in the Black Sea region.

The study used Doppler-measurements with the STP-H5 PHOTON sensor installed on the ISS (International Space Station) orbiting 400 km above the Earth's surface. On a daily basis, the STP-H520 was used for ionospheric research, but it could perform additional measurements for the USA during its "free moments." Using a built-in fully programmable

[13] CNN, https://youtu.be/wM5LVpH1eNo.
[14] Meaconing RF interference, https://en.wikipedia.org/wiki/Meaconing.
[15] https://navi.ion.org/content/68/4/673.
[16] https://radionavlab.ae.utexas.edu/images/stories/files/papers/leo_int_mon.pdf.
[17] https://c4ads.org/wp-content/uploads/2022/05/AboveUsOnlyStars-Report.pdf.

satellite receiver, SDR (Software Defined Radio), the GPS signals of the two L1[18] and L2[19] bands were recorded with a sampling frequency of 6 Mbps. The unprocessed "raw" data were transmitted to Earth during a special sixty-second transmission slot from the ISS. The data underwent an extended DSP signal analysis. The measurement of disturbed GPS took place in an unusual GPS-Earth-ISS configuration. The STP-H5 receiver was directed downward towards Earth, looking "backward" relative to the flight direction of the ISS. On Earth, AI was used in the data analysis to visualize the type and location of the CODED GPS jamming interference (Figure 19).

Fig. 18. STP-H5 sensor, installed on the International Space Station (ISS) at an orbit of approximately 400 km above Earth, is equipped with a GPS receiver designed for ionospheric research. Decoded data revealed a value of 0 in the LNAV fields, indicating the presence of "coded jamming."

Source: *Literature [3]*

Figure 19. Recording of a disrupted GPS signal in the Black Sea region, conducted in 2017 from the International Space Station using the STP-H5 sensor.

Source: *Literature [3]*

[18] GPS civil freq: 1575.42 MHz (L1) 1176 MHz (L5), https://en.wikipedia.org/wiki/GPS_signals.
[19] GPS military L2 o częstotliwości 1227.60 MHz, https://en.wikipedia.org/wiki/GPS_signals.

Research has focused on the Black Sea region, where significant GPS interference has been recorded since 2014. Numerous reports from commercial vessels navigating these waters have documented GPS anomalies. Some captains claimed that their ships' navigation systems virtually relocated them hundreds of kilometers away to an airport in Moscow [16 17].

During the decoding of GPS L1 C/A message frames on Earth, it was found that they had the correct format, but a strange observation (anomaly) appeared. When a satellite passed over the Black Sea area suspected of GPS spoofing, the LNAV message value was read with zero values on all available registered channels (Figure 18). The zeros disappeared after leaving the interference region. There was no doubt about intentional GPS interference; however, it did not match classic GPS jamming, as the decoded information was not disrupted by random noise at 1575.42 MHz (L1)[18]. Similar observations applied to the military GPA L2[19] band. This indicated that it was not typical GPS spoofing, as no falsification of LNAV telemetry data was demonstrated, but it was effectively zeroed out. Spectral analysis confirmed the presence of artificial L1 and L2 interference signals. Therefore, the Americans called this type of interference "coded" GPS jamming. Today, we are entitled to state that this is a form of DoS cyber-attack, blocking the PNT functions of the GPS receiver, especially when it has to perform a cold start or reacquisition of satellites. Coded jamming thus constitutes a potential invisible trap for the receiver, in which, if it falls, it may remain. It is suspected that a forced receiver restart with a reset of data about the satellites' positions relative to Earth (the so-called almanac) is particularly dangerous. Such an effect might be activated remotely, e.g., with a strong electromagnetic pulse. Furthermore, the zeroed LNAV navigation message positions are also such an unusual value for a GNSS receiver that it can cause some satellite receivers to go into an unsteady state without reporting an error message. This would then be an effective spoofing attack without the attacker imposing a target position. This situation may include not only civilian GPS L1 and L5 receivers, but also some military L2 frequency receivers cryptographically protected for anti-spoofing purposes.

Therefore, all together, it becomes justified to assume that perhaps at present we are experiencing in Poland a certain kind of "getting us used to" the presence of GPS jamming signals, solely so that we do not build resilience in terrestrial IT/OT systems to a threat that may only come in the future. But Poland is only one of many countries experiencing it today.

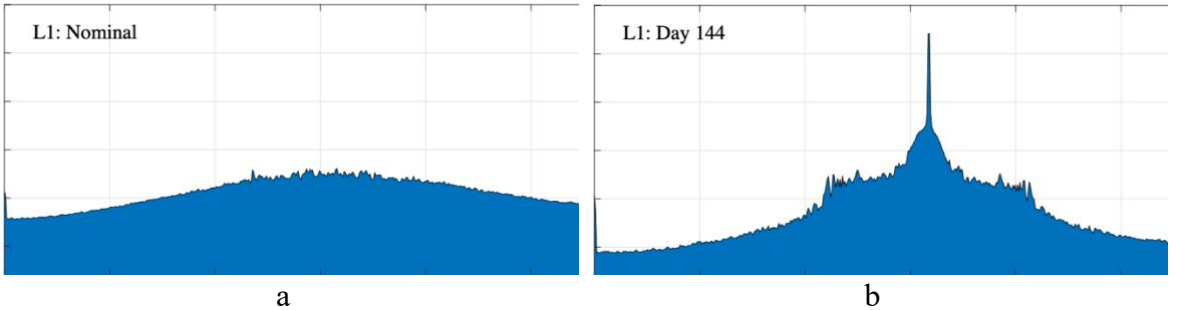


Fig. 20. (a) Spectrum analysis of the unjammed GPS L1 frequency at 1575.42 MHz during tests. (b) Interference in the L1 band visible in the central part proving there is GPS jamming or spoofing. Source: *Literature [3]*

By far the most interesting challenge was the attempt to determine the location of the GPS interference emission site. The Americans recalled the "*Story of the Russian Sputnik 1"*, from 1957. It emitted a signal in the radio wave band with a frequency of about 20.005 MHz and 40.002 MHz. This simple signal had a characteristic "beep-beep-beep" sequence, which

was heard during satellite space transposition all over the world, and became a symbol of the beginning of the era of space exploration. It was this signal that was listened to by the Americans, William Guier and George Weiffenbach, who are considered to be the creators of the idea of the GPS[20] system. Like many of their colleagues, they tracked every flyby of Russia's Sputnik1 and calculated how far it was from them. They used small measurable changes in frequency caused by the *Doppler effect*, the same effect that changes the sound of an ambulance when it passes us on a signal. The physicists focused on the analysis of the "Doppler shift" with the ambitious goal of deducing the entire trajectory of the Russian satellite's orbit and predicting its exact position at any given time.

In 2018, the Americans used the same idea as in 1957 to determine the location of the source of GPS jamming in the Black Sea region. They assumed that if the GPS interference source in question was based on a stable TCXO or OCXO quartz oscillator, then it might be possible to calculate the exact position of the jammer transmitter recorded from the ISS "Doppler history" - the exact position of the jammer transmitter you are looking for. The researchers estimated that for an average TCXO oscillator, the source location error would be max. 7km, and for a good quality OCXO oscillator the error would be only 70 m. In both cases, the prognosis for identifying the transmitter site was satisfactory. The calculations were complicated, depending on the parameters of the ISS station's orbit relative to Earth, but possible. The result of the calculations surprised everyone, because it indicated that the source of the GPS jamming "from the Black Sea" was several hundred kilometers away in the Mediterranean. It turned out that the jamming transmitter was located on the territory of a Russian military base, located in that time in Syria[21].

Fig. 21. Calculations based on Doppler history indicated that a transmitter in a Russian military base in Syria was responsible for GPS interference in the Black Sea region.
Source: [3]

It appears that GPS interference in Poland may be caused by similar GPS jamming. After several months, we have become accustomed to it, as there have been no spectacular failures so far. There are no sensational, major failure incidents, although sometimes Poland appears on the front pages of world media, e.g., when jamming forced British services and the RAF to initiate special procedures on board the aircraft carrying the British Defense Minister Grant Shapps [22] [23] during the flight from Poland to Lithuania.

[20] https://www.bbvaopenmind.com/en/technology/visionaries/the-birth-of-gps-an-unexpected-child-of-the-space-race/.

[21] https://radionavlab.ae.utexas.edu/images/stories/files/papers/leo_int_mon.pdf.

[22] https://www.theguardian.com/politics/2024/mar/14/russia-suspected-of-jamming-gps-signal-on-aircraft-carrying-grant-shapps.

[23] https://www.thetimes.co.uk/article/russia-electronic-attack-grant-shapps-plane-qltjc6gqg.

The UK Minister Grant Shapps incident was a well noisy news [24] [25] all over the west world.

Research conducted using the PHOTON STP-H5 sensor on the ISS enabled the standardization of the method for identifying sources of GPS interference worldwide. The automation of the GPS jamming and spoofing identification process was based on the statistical hypothesis testing method HTP (Hypothesis Testing Problem). The HTP involves formulating hypotheses about population parameters based on a sample of data and conducting appropriate statistical tests to assess whether the data provide sufficient evidence to support or reject these hypotheses. In Figure 22, a uniform color illustrates the 'clean' frequency with which the hypothesis is not confirmed – this is the ISS's flight over undisturbed ocean areas. As a result, the ratio of the number of recorded potential GPS L1 (upper panel of Figure 2) and L2 (lower panel of Figure 2) interference events to the total number of hypothesis tests conducted at each location on the coordinate map is exposed.

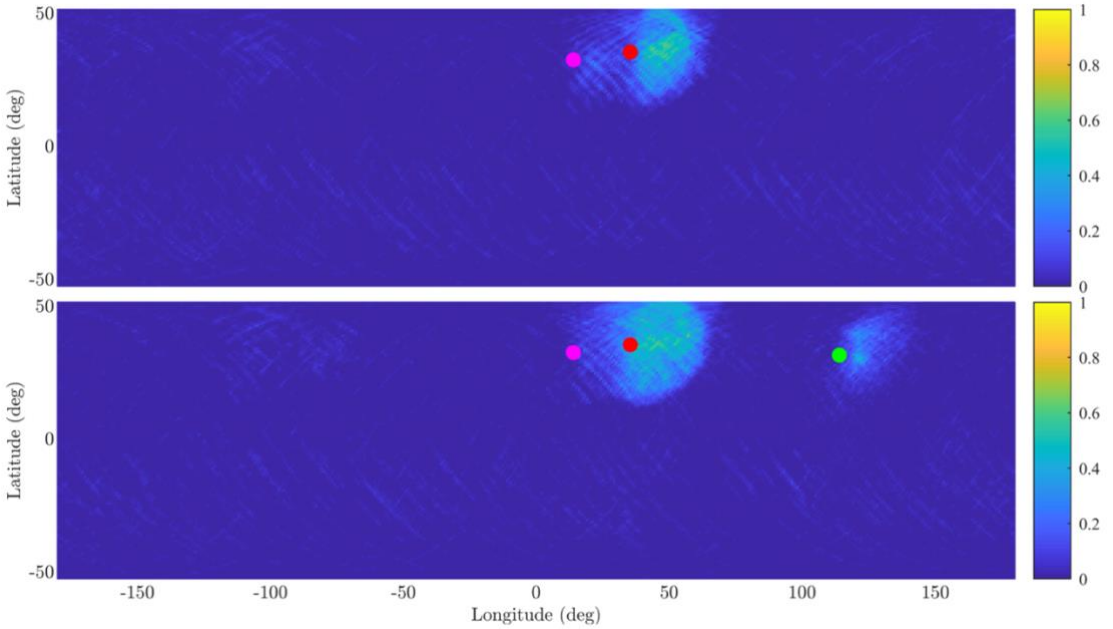


Fig. 22. Graphical visualization of GPS disturbances based on HTP statistical hypothesis testing. Source: *Literature [3]*

Red dots indicate the estimated origin of disturbances from the area of Syria. Another area of disturbances can be observed west of the location in Syria. Purple dots represent the approximate location of reports of GPS disturbances in the region of Libya. In addition to disturbances in the areas of Syria and Libya, strong interference on the L2 frequency was also observed in mainland China. The green dot at the point (32° N, 114° E) indicates the hypothetical location of the interference source based on the shape and location of the observed hotspot. The measurement technique used for graphical visualization from low Earth orbit (LEO) satellites is an emerging technology and offers promising prospects for the serialization of such studies. It has a high probability of determining the exact location and,

[24] https://www.bbc.com/news/uk-68569676.

[25] https://www.telegraph.co.uk/news/2024/03/14/grant-shapps-gps-jammed-aircraft-trip-poland-troops/.

consequently, the source and military affiliation of the disturbances. The method and mathematical description are presented in the works [2][3]. We also recommend the reader's attention to a webinar discussing the implementation of measurements from the ISS available on YouTube[26].

An important conclusion from the above example is that encoded GPS jamming appears to be an attack comparable to a Denial of Service (DoS), blocking the functionality of determining PNT (Positioning, Navigation, and Timing) by the GPS receiver, especially during the initial phase of a cold start and reacquisition of available satellites. To better understand this threat, we will explain the principle of PNT determination by any GPS satellite receiver. For simplicity, we will assume that the GPS system operates without considering the Earth, that is, as if our planet did not exist. We will also assume that space is a vacuum (no ionospheric delays), and time flows uniformly everywhere (no relativistic time dilation).

A simplified algorithm for PNT determination by any of the GPS satellite receiver:

1. **Initialization of SAT receiver.** After powering on, the GPS receiver starts operating. It tunes its radio to work in the frequency band of 1575.42 MHz. It searches for signals arriving from GPS satellites in orbit, identifies them, and assigns individual channels (GPS channels) to handle the decoded data. At this stage of operation, the receiver does not yet have information about its position in time or space (Figure 23).

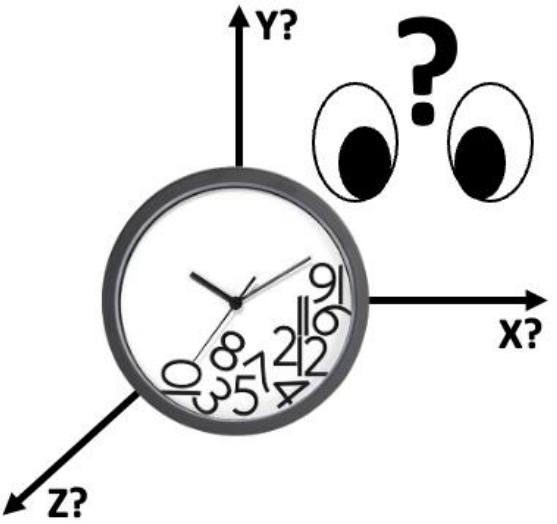


Fig. 23. The GPS receiver, after powering on (cold start) and during satellite reacquisition, has no orientation in time or space. This is the best moment to jam it with GPS jamming.
Source: *self-prepared*

2. **Time Synchronization** (T). When the receiver receives signals from GPS satellites, it decodes the information containing the timestamp. It averages the readings and synchronizes its internal clock, thus obtaining a weak millisecond-level accuracy. Jamming the GPS, particularly zeroing out the received timestamp information, effectively blocks the receiver.

[26] https://www.youtube.com/watch?v=XDbn85IBIus.

3. **Calculating the Distance from Satellites**. The synchronized clock of the GPS receiver allows it to measure the signal travel time from the satellite. This way, the distance from the receiver to the satellite can be calculated, which equals the time difference indicated by the receiver's clock, reduced by the received timestamp from the GPS satellite signal and multiplied by the speed of light *c* (the radio signal propagation speed in vacuum space).

4. **Positioning (P)**. Knowing the distance from the GPS receiver to at least 4 satellites, it can calculate its position relative to these satellites using the trilateration technique. This involves determining the position coordinates based on the lengths of the segments separating the receiver from the signal-transmitting satellites.

5. **Regular "cyclical" updating of (P) and (T)** allows the GPS receiver to regularly repeat calculations. The longer it operates, the more subsequent readings help improve the accuracy of ref. time (T) and position (P) determination, increasing the receiver's accuracy.

6. **Navigation (N)**. Real-time T&P updates enable the receiver to determine its changes in position relative to the GPS system, including the direction of its movement and, indirectly, changes in angle, speed, and acceleration. All together it brings the PNT functionality.

Timing GPS Receivers. The operation of a GPS receiver is essentially a comparison of clock readings. The accuracy of PNT parameters calculated within the GPS timing receiver depends on the TRAIM algorithm and the stability of the built-in TCXO frequency oscillator. The quality is also influenced by the sensitivity of the radio receiver, the resolution of DAC circuits, the computing power of the internal CPU, available RAM, the number of channels. A simplified general block diagram of a 6-channel GPS L1 1.575 GHz timing receiver is shown in Figure 24. Particularly, a GPS timing receiver stands out by providing high-quality UTC time consisting of the 1PPS (Pulse Per Second) frequency standard and phase information of the UTC (USNO) time scale delivered via an RS232 interface in NMEA-183 frame format or binary coded (unstandardized), which contains time and date (ToD) calendar.

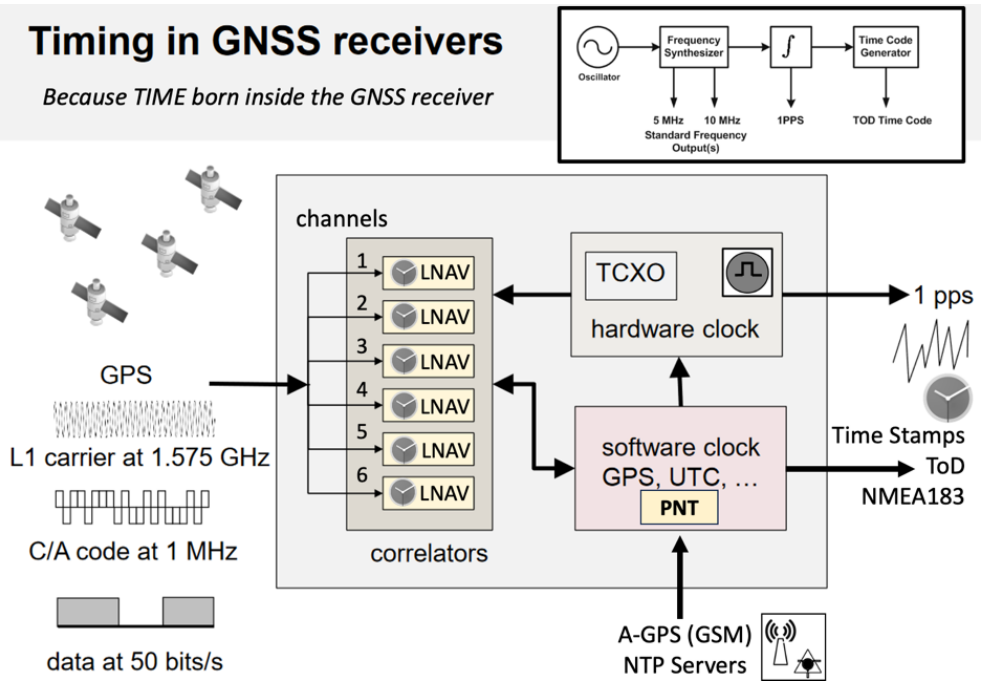


Fig. 24. Simplified block diagram of the GPS L1 timing receiver used for UTC synchronization.
Source: *self-prepared*

RTK GPS receivers. The Real-Time Kinematic (RTK) satellite receiver performs several additional steps compared to timing GPS receivers to provide high-accuracy and real-time positioning. Here are some of these steps: multi-frequency GNSS signal reception, precise carrier phase measurements from each satellite vehicle, differential corrections from ground ref. BTS. There are also numbers of scientific GPS receivers offering best accuracy. They are very expensive.

In summary, we often mistakenly interpret that the time and position of the GPS receiver are being transmitted to us from space satellite vehicle, and that the satellite receiver works like a LAN network card. Consequently, we mistakenly believe in the security of our GPS-based solutions. In reality, PNT parameters are determined within the GPS receiver on Earth, and each receiver does it slightly differently. As a result, there are no two identical GPS receivers simultaneously determining the same PNT parameters. The PNT difference is a measure of the accuracy of the receiver's calculations and the fact that their operations are mutually independent – so-called, they are asynchronous. The GPS receiver has to perform a lot of calculations. These calculations take into account, among other things, signal delay corrections in the ionosphere and relativistic time dilation effects resulting from Einstein's two theories of relativity: special and general. The first daily time dilation correction is only 7 microseconds and results from the speed of 14,000 km/h at which GPS satellites orbit the Earth. The second is a system internal correction of 42 microseconds per day. This results from Einstein's general theory of relativity concerning the effect of gravity on the phenomenon of time dilation. Due to gravity impact, the time on Earth flows slower than in space, where the satellites orbit. Both of these values have opposite signs, so the daily time correction that each receiver must apply for the GPS system amounts to as much as 35 microseconds per day. This is significant, especially considering that, for example, modern 5G telecommunications allow a maximum synchronization error of just a few nanoseconds. The situation becomes more complicated when the receiver uses multiple satellite systems from the GNSS group simultaneously. It must independently recalculate the time dilation for each constellation: GPS, GALILEO, GLONASS, BEIDOU, IRNSS separately. This increases the susceptibility of the GNSS receiver to numerical overflow errors which the attacker takes advantage of.

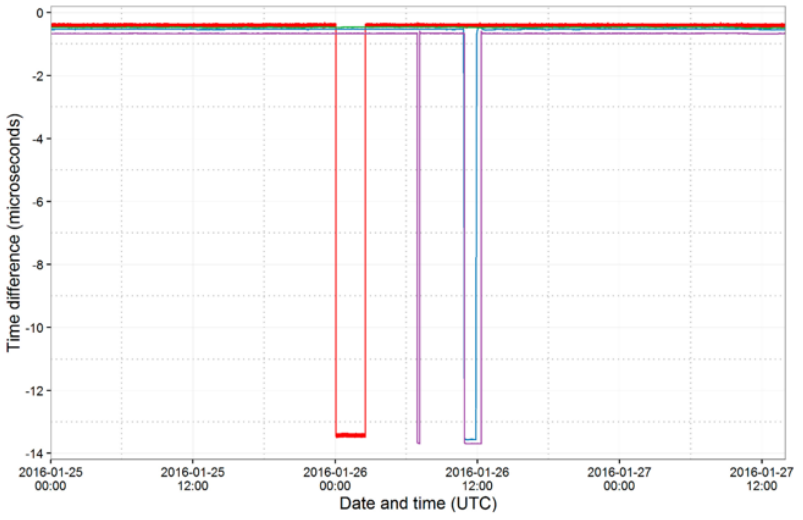


Fig. 25. Non-simultaneous reaction of 5 time servers to a 13.5 µs error of the GPS SVN23. Source: *Finnish Metrology (https://aaltodoc.aalto.fi/handle/123456789/19833).*

Today, we know that receivers from different manufacturers react differently to exceptional situations, leading to desynchronization. This was very well demonstrated by the internal error incident of the GPS system, known as the SVN23 satellite error, which occurred on January 26, 2016. It caused a desynchronization of 13.5 µs among 5 different GPS receivers tested on that day, which were used in NTP/PTP time servers (Figure 25).

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. 26. Official press release from the U.S. Armed Forces regarding the GPS SVN23 error. Source: *Finnish Metrology Appendix A at https://aaltodoc.aalto.fi/handle/123456789/19833.*

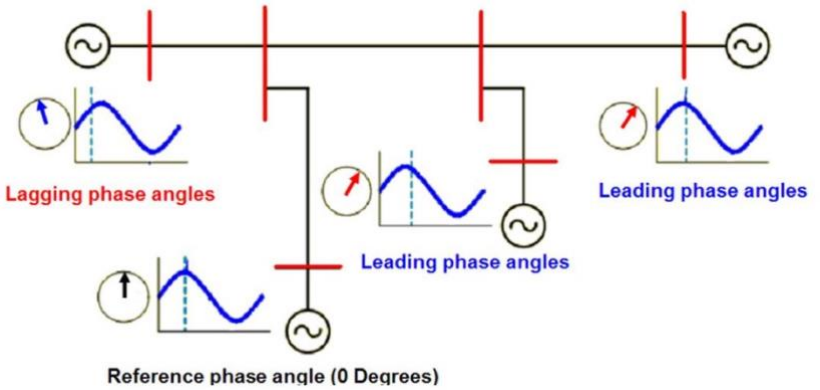


Fig. 27. The 13.5 µs GPS SVN23 error could have caused a failure in the smart grid energy sector operating according to the IEC/IEEE C37.238 standard if the red-marked synchrophasor PMU had been synchronized not to GPS like the other PMUs (blue color). The maximum allowable desynchronization error for a PMU in a smart grid according to IEC C37.238 must not exceed 1 µs. Source: *self-prepared*

Understanding the significant uncertainty that using GPS satellite receivers manufactured between year 1990 and 2020 introduces for the security of critical infrastructures in the USA and Europe, the Americans were the first to recommend risk diversification by introducing the presidential directive EO13905[27]. The executive order regulation regarding the functionality of ground-based UTC reference time supplies were described by NIST in the document[28] NIST.TN.2187. In a separate document[29] NIST.TN.2189, the dependencies of the US industry on GPS were described.

In January 2023, the European Commission published the updated NIS2 directive[30], which, following the U.S. EO13905 doctrine, advises EU member states to consider creation of A-PNT (Assured PNT) systems that supports or will be alternatives to GNSS.

So far, USA, UK and Poland performs very well compared to other EU NATO member states. The new national official time dissemination system in Poland – eCzasPL[31] (eTime) was launched on December 10, 2023, which is two weeks before the first GPS disturbances over Poland. Such GPS jamming and spoofing are now near every day in Poland[32].

The launch of the eCzasPL system at the Central Office of Measures (GUM) in Poland took place exactly on the twentieth anniversary of the publication of the official time law UTC(PL) /Journal of Laws No. 16 dated December 10, 2003[33]/. On April 22, 2024, twenty years will have passed since the entry into force of the regulation /Journal of Laws[34] No. 56 POS. 548 dated March 19, 2004/ indicating the NTP time servers named *tempus1.gum.gov.pl* and *tempus2.gum.gov.pl* as the official sources of UTC(PL) official time for the Central Office of Measures of the Republic of Poland (the Polish equivalent of the U.S. NIST).

Thus, Poland, alongside the USA, the United Kingdom, and France, has acquired its own ground-based infrastructure for distributing official state time UTC(PL), independent of military GNSS group satellite systems. Poland has surpassed other EU nations and countries like India, Japan, South Korea, and Israel. China[35] and many other countries are still working on similar ground-based UTC distribution infrastructures.

The Polish eCzasPL (eTime) system at Polish Central Office of Measures (GUM RP) has a unique and little-known functionality. It allows the NMI GUM RP to remotely control UTC on distant NTP/PTP time servers operating in the industry, including those functioning in internal infrastructure networks isolated from the Internet. This is very important because we often forget that NTP and PTP (IEEE1588) protocols do not guarantee synchronization on the receiving end. Only the audit system developed in the DEMETRA[36] Horizon 2020 project by company ELPROMA allowed remote long-distance testing and certification of time servers.

[27] https://www.govinfo.gov/app/details/DCPD-202000071.

[28] https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2187.pdf.

[29] https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2189.pdf.

[30] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en.

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

[32] https://www.reuters.com/business/aerospace-defense/poland-says-gps-disruptions-baltic-could-be-related-russia-2025-06-17/.

[33] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20040160144.

[34] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20040560548.

[35] https://www-thepaper-cn.translate.goog/newsDetail_forward_23171179?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp&_x_tr_hist=true.

[36] ION PTTI conference, https://doi.org/10.33012/2017.14982.

4. How to Prevent Desynchronization of Critical Infrastructures

Recognizing synchronization as an area of modern cybersecurity necessitates updating operational procedures (OT – Operational Technology) both at the state level and in local work environments. A key element is public education, which raises awareness of the importance of maintaining a stable UTC domain during peacetime as well as in the event of armed conflict. Proper UTC synchronization is essential to the efficient operation of all modern information technology IT and OT. In the event of a kinetic conflict (armed conflict), the importance of synchronization remains unchanged, but the rigor of accuracy is lowered, and the method of technical realization of UTC time distribution changes, resulting from shifting priorities between the utility of IT and OT data. Understanding the above is important given the ongoing GPS signal jamming over wide area of EU member country (Figure 28). During the kinetic conflict or serious crisis, the IT priority 1,2,3 (Confidentiality, Integrity, Availability) changes to OT with opposite priority (Availability, Integrity, Confidentiality).

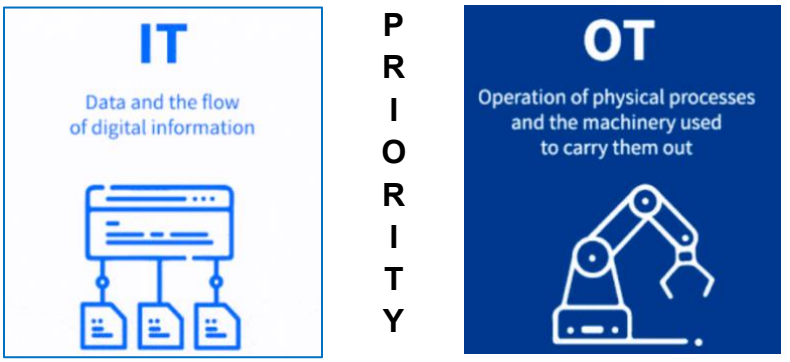


Fig. 28. Change of IT and OT priorities resulting from a shift in data utility.
Source: *General M. Chmielewski (MBA Cybersecurity at Military University of Technology)*

One should start with assessing the current situation (status quo). The IT/OT security auditor should, for example, use drones or conduct a personal inspection to check the volumes and the condition of the GPS RF-antennas installed on the roof, and then ask the building and IT system administrators the following questions:

- *Is time and date important for the IT / OT systems in the organization?*
- *Can desynchronization of IT / OT affect the operational capability of the enterprise?*
- *Does the enterprise use systems with a distributed IT or OT architecture?*
- *Does the organization use multi-server solutions or modular IT or OT architectures?*

A positive answer to any of the above questions indicates that synchronization is important for the organization. An additional preliminary inquiry during the conversation can provide the auditor with an answer to the question of whether the organization is prepared for the GPS being turned off or unavailable.

Fig. 29. View of GNSS antennas mounted on the roof of a critical infrastructure building. The inspection provides information on the number of systems dependent on GPS and the quality of the installation, as well as an insight into the period of origin of the individual GPS-dependent solutions. Source: own

Moust of GPS receivers manufactured before 2022 are not resistant to GPS jamming and spoofing. In Poland, as in other countries, there is an unknown large number of devices using satellite GNSS receivers supplied as components of large IT and OT systems. Despite the manufacturer's claims, these devices may use GLONASS or BEIDOU instead of, for example GPS and GALILEO that are crucial for EU security. Owners of synchronization devices, especially older than 5 years the NTP/PTP servers using GPS (GNSS) regardless of brand, should consider replacing their devices with newer models manufactured after 2022. A good candidate to choose is domestic European manufactures ELPROMA and PIK Time Systems. Their product NTP/PTP servers with NATO codification and metrological certification from the Central Office of Measures (GUM) of the Republic of Poland. They are mostly chosen by NMI all over the world. Polish products are security and performance highly valued worldwide today, as the world begins to recognize the security benefits of synchronization (Figure 30).

Fig. 30. Polish NTP/PTP synchronization devices used in NATO and in the eCzasPL project. Source: Elproma, PIK Time Systems

The national polish industry and users should consider the transition to and integration of their existing IT structures with the eCzasPL (eTimePL) GUM RP (NMI) synchronization system, which is independent of GPS and GNSS at all. Other countries should consider relying on either local ground UTC dissemination such as the US NIST (NIST Time) or the UK NPL (NTL Time). Possibly there will be more similar local solutions deployed in each of EU country due to polish eCzasPL (basis on DEMETRA Horizon 2020) is available commercially for exporting inside the EU members and for selected countries outside of EU.

Application notes with configuration diagrams for connecting isolated internal infrastructure networks to atomic official time standards UTC(PL) have been extensively discussed on pages 210-212 in literature [1]. Here we focus on short summarizing the synchronization technique that is resistant for time manipulations including GPS (GNSS) jamming and spoofing (Figure 31).

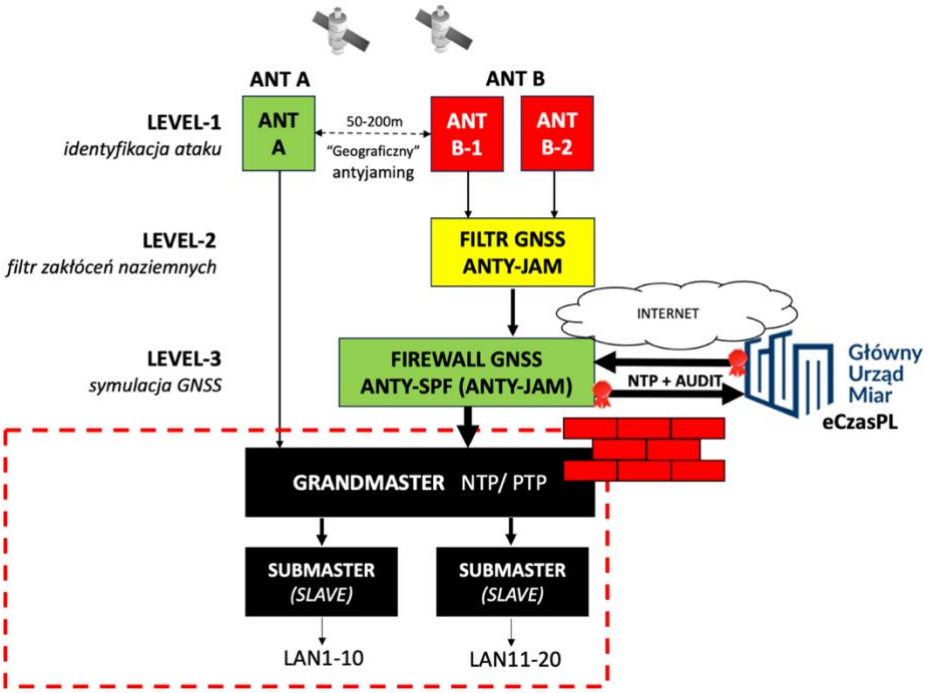


Fig. 31. Model of secure synchronization eCzasPL/eTimePL, 100% resistant to GNSS jam/spf. Source: Elproma

The key security elements of the structure presented in Figure 31 are:

1. **Multiple Sources of UTC** ref. Reference UTC time is sourced from multiple sources simultaneously, such as satellite GNSS (GALILEO+GPS for EU), remote atomic clocks of the NMI (e.g. Central Office of Measures eCzasPL), local Rubidium and OCXO holdover oscillator built into the NTP/PTP server for time keeping in case of the network links from NMI are down or there is unavailability of GNSS signal (jamming and spoofing of GNSS).

2. **GNSS Geopolitics**. Poland and other EU members should focus on the leading role of the European GALILEO system as a source of UTC time, supported by the US GPS system. The roles of military systems such as the Russian GLONASS, Chinese BEIDOU, and Indian IRNSS should be limited to comparisons and analyses only. Using exclusive GNSS constellation settings for specific smart RF antenna (e.g. the antenna ANT-A path should be set exclusively for GALILEO, and ANT-B can be setup to exclusive GPS). Products that do not support smart antennas, should consider using separate external GNSS receiver connected to NTP/PTP server (Figure 31).

3. **UTC Redundancy with Asymmetry Link.** The classical symmetry of redundancy A/B structure, once A or B is hacked, both A and B are not useful longer. Considering asymmetry for redundancy A and B lines is recommended. At the time ANT-A (exclusive Galileo e.g. w/ PRN anti-spoofing) goes directly to NTP/PTP server, the ANT-B signal goes intermediately via additional LEVEL-1, LEVEL-2, LEVEL-3 GPS filter and GPS firewall. Hacking, jamming, or spoofing of the ANT-A antenna path does not affect the security of the ANT-B path, which has additional LEVEL-2 active jamming filtering protections and LEVEL-3 GPS FIREWALL that base on satellite signal simulation. It is good practice to use two independent GNSS receivers from different manufacturers for the ANT-A and ANT-B paths. In case of ELPROMA product, customers can extra choose GNSS receivers to be sure what their synchronization is dependent on. This is important security geopolitical factor.
4. **Resistance to Mobile Non-military GPS Interferences**. To limit the impact of local sabotage or diversionary actions, the minimum distance between ANT-A and B should be 50-200 meters. This is a "natural geographic anti-jamming" technique, highly effective against mobile GNSS signal jamming devices. This technique cannot counter strong military GPS jammers.
5. **Security Model with Functional Convergence Features**. It allows central synchronization to the eCzasPL (eTimePL) land-based official time system, independent of GNSS. If the TCP/IP connection with NMI (GUM RP in Poland or NPL in UK) is lost, synchronization automatically decentralizes, continuing to work using GALILEO (ANT-A) and GPS (ANT-B), and vice-versa. In case of ground TCP/IP links are down and the GNSS signals are not available the NTP/PTP server should survive operationally by automatic switching to oscillator holdover mode (see below).
6. **UTC Autonomy (OSC Holdover Mode)**. It ensures continued operation even in the absence of GNSS signals or loss of the TCP/IP link to the ground time dissemination system from NMI (e.g. eCzasPL/eTimePL Central Office of Measures, NPL-Time in UK, NIST-Time in USA). The solution sources time from aggregated Rubidium (Rb), CSAC atomic clocks and TCXO/OCXO built into the NTP/PTP time server equipment operating within NIS2 critical infrastructure. Every critical infrastructure should be equipped with local NTP/PTP server equipped with holdover oscillator.
7. **LEVEL 1-2-3** Security Management Hierarchy at antenna ANT-B path (Figure 31):
   LEVEL-1. The RF antenna and GNSS receiver follows the specific exclusive constellation configuration (Galileo and GPS for EU) reflects the cybersecurity objectives related to geopolitics. For example, the national critical infrastructures of the EU and USA should not depend on the Russian military GLONASS and Chinese military BEIDOU, and vice-versa, it is hard to imagine that Russian or Chinese critical infrastructures will depend on the US military GPS. Another highlight of LEVEL-1 security is the minimum antenna distance of 50-200 meters in ANT-A and ANT-B paths. It decreases vulnerability to amateur low-power GPS mobile jammers.
   LEVEL-2. Active Filtering of GNSS Jamming and Spoofing Interference. Devices at this level use *null steering* techniques to recognize and reject false signals emitted from the ground. They perform differential measurements and therefore must be equipped with multiple antennas, typically three. Solutions with two and six antennas also exist. This level is responsible for retrieving from jamming the original signals.
   LEVEL-3. Physical Isolation of Internal Infrastructure from GNSS. Often referred to as a GPS firewall. Devices at this level have the functionality to simulate GPS L1 1575.42 MHz signals or generate a ready-to-use decoded GPS frame in NMEA183 format. The simulated GNSS system (GALILEO supported by GPS for Poland) is

"bridged" directly to the GRANDMASTER time server input, bypassing the network firewall and operating within the isolated infrastructure network NIS2. This connection is secure because it does not use the TCP/IP network protocol, but an rs232 electrical or L1 1575.42 MHz radio transmission, secured by a one-way information transmission "diode." In the event of a jamming or spoofing radio attack, LEVEL-3 cuts off access to the physical GNSS satellites from the infrastructure network, but remains in monitoring mode (sandbox) until the end of the radio attack. The same LEVEL-3 device can remotely control and report for certification the compliance of the used UTC with official UTC(PL) time.

Poland has recently been experiencing more intense GPS jamming attacks. Therefore, an important support for the proposed eCzasPL secure synchronization structure is a GPS interference monitoring system that notifies about event occurrences and assesses the end of radio attacks on our country. Such a system is ARGOS by ELPROMA

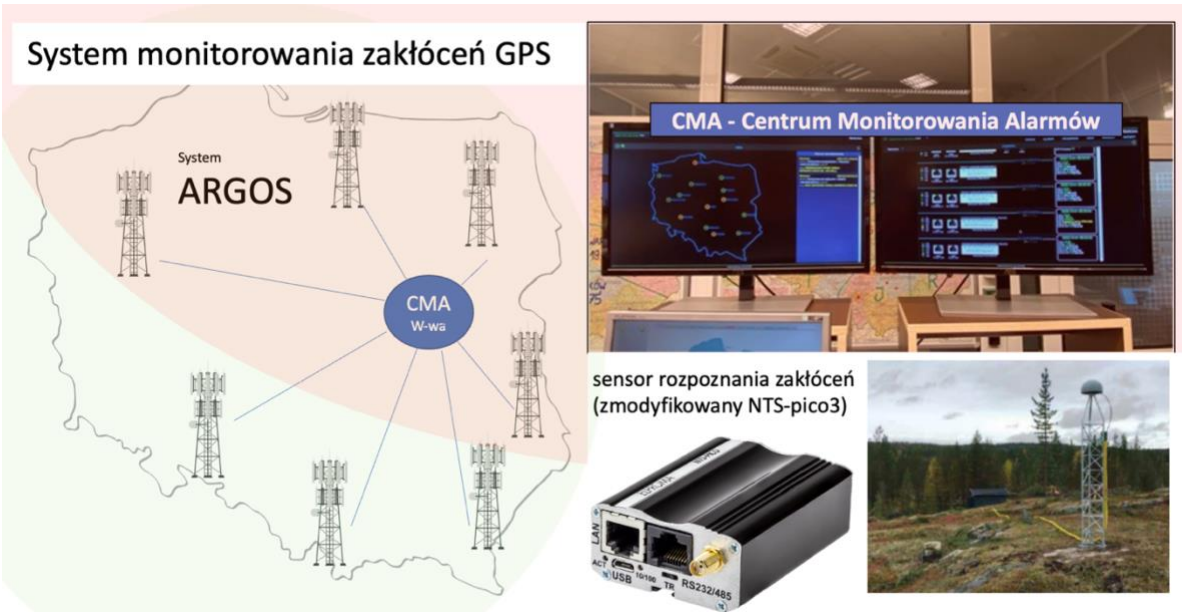


Fig. 32. The stationary ARGOS system with dense sensor mapping detects GPS interference. Source: own

ARGOS is a Polish stationary system for monitoring GNSS signals with so-called dense mapping of telemetry sensors that examine the quality of received satellite signals in individual subgroups. It is based on the miniaturized Elproma NTS-pico3 time server produced domestically since 2017, which has been actively tested by companies in Israel, the USA, and Germany as a candidate for coordinating the synchronization of sensor fusion and their data in autonomous vehicles and robots.

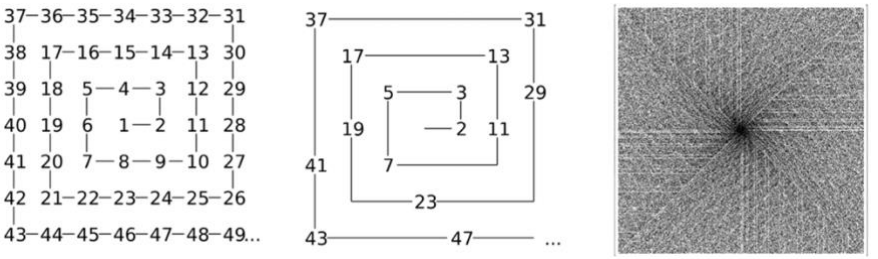


Fig. 33. The first 49 numbers of the Ulam spiral. Prime numbers highlighted. View of a large population of prime numbers. This allegory should be regarded as illustrative rather than literal. Source: Wikipedia

The ARGOS version of the NTS-pico3 sensor is significantly expanded compared to the standard version of the product available for regular sale. The details are not known, but the manufacturer claims that the sensor can be equipped with a dual-band GNSS satellite receiver, allowing individual and group tracking of all available constellations (GPS, GALILEO, GLONASS, BEIDOU, IRNSS) and, most importantly, can optionally have a built-in frequency spectrum analyzer. Dense mapping using ARGOS sensors allows for a broader exploration of GNSS satellite signal interference issues. Data can be presented in a simple format, such as a monochrome bitmap (1 - interference, 0 - no interf,) or using colors.

Emphasizing the unique approach of using dense mapping techniques, the Polish manufacturer of the ARGOS system refers to the allegory of searching for prime numbers based on the so-called Ulam spiral (a Polish mathematician from the pre-war Lwów School, participant in the Manhattan Project in the USA). Looking at the Ulam spiral for large statistics of prime numbers (Figure 33), it is hard not to agree that we observe a certain graphical regularity in their positions in the set of natural numbers. Meanwhile, the problem of searching for prime numbers remains an unsolved millennium problem, known as the Riemann Hypothesis. This allegory aims to encourage cooperation with other entities as well.

By assigning a color palette to intermediate states 0-1, representing the varying levels of interference, the ARGOS system opens up new research possibilities, important for assessing the impact of other factors on GPS interference. Weather conditions, severe atmospheric pollution from industry, electromagnetic fields generated by the energy sector, and even the overloading of the source signal are interesting to understand the phenomena that are an emerging field of civil cybersecurity.

This type of research directly references the American concept discussed earlier in this chapter (Figure 22), concerning the graphical visualization based on statistical hypothesis testing, using both machine learning and artificial intelligence to determine the location and identify the type of GPS interference.

It may turn out in the future that in justified cases, it will be necessary to counteract hostile GPS jamming by enhancing it with our own stronger jamming (Figure 34), just to ensure that domestic industrial systems react correctly in an "immunological" manner by rejecting GPS as a UTC time source and replacing it with the alternative land-based system eCzasPL from GUM RP. This is because current research indicates that in many cases, weak GPS jamming can behave similarly to GPS spoofing, and it may be necessary to provide "artificial assistance" in enforcing a stable level of GPS jamming to trigger automatic system switching procedures.

Fig. 34. Chinese-made mobile GPS jammer (on the left). Polish-made PIAP and iTTi/Łukasiewicz professional programmable jammer (right side), model ZKR-1 with 150W power and a frequency range of 25-5800 MHz, capable of generating continuous and responsive jamming. Source: iTTi / Łukasiewicz

The “bitmap “of ARGOS interference indications is significant because it allows for the identification of single attacks caused by diversionary or sabotage actions using portable GPS jammers (Fig. 34, left side).

The Elproma-ARGOS system reacts in real-time to any type of interference. It generates alarms at the start of a radio attack, monitors the level of interference during the event, and sends notifications of its end. The system itself is resistant to GPS jamming and spoofing. It protects itself through a distributed sensor structure centrally managed by the Elproma-EDMS program supported by AI. Incorporated into the national synchronization system with official UTC(PL) time, the ARGOS system receives an effective startup tool through eCzasPL in case a restart is needed during severe GNSS disruption over Poland.

Information (alarms) from ARGOS should be directly communicated to the country's key critical infrastructures. Early warning of GPS jamming is a crucial security element today. It allows for a reaction to the attack at its early stage. Simply turning off the GPS receiver can protect IT / OT systems from the effects of non-deterministic behavior, but only using alternative land-based PNT solutions like eCzasPL offers 100% resilience and security.

Current GPS disturbances over Poland exhibit characteristics of a DoS attack that blocks PNT receiver functions in specific cases, such as startup (cold-start) and reacquisition of satellite signals. It's possible that the intent of the current action is to acclimate Poland to the problem and neglect this important security issue.

Therefore, alongside the statistical quantitative assessment, a thorough qualitative investigation of GNSS interference using various independent measurement methods is necessary. The Institute of Telecommunications is also conducting such research. With well-equipped mobile laboratory units, it can both assess the quality of received GNSS signals and perform GNSS jamming in the region (Fig. 35). Among civilian manufacturers of radio signal jamming systems, the iTTi / Łukasiewicz (PIAP) solution is noteworthy. The ZKR-1 device is a professional programmable jammer with 150W power operating in the frequency range of 25-5800 MHz. It can generate continuous and responsive jamming (Fig. 34)

Fig. 35. Mobile measurement station for testing the quality and jamming of GNSS signals Source: Institute of Telecommunications

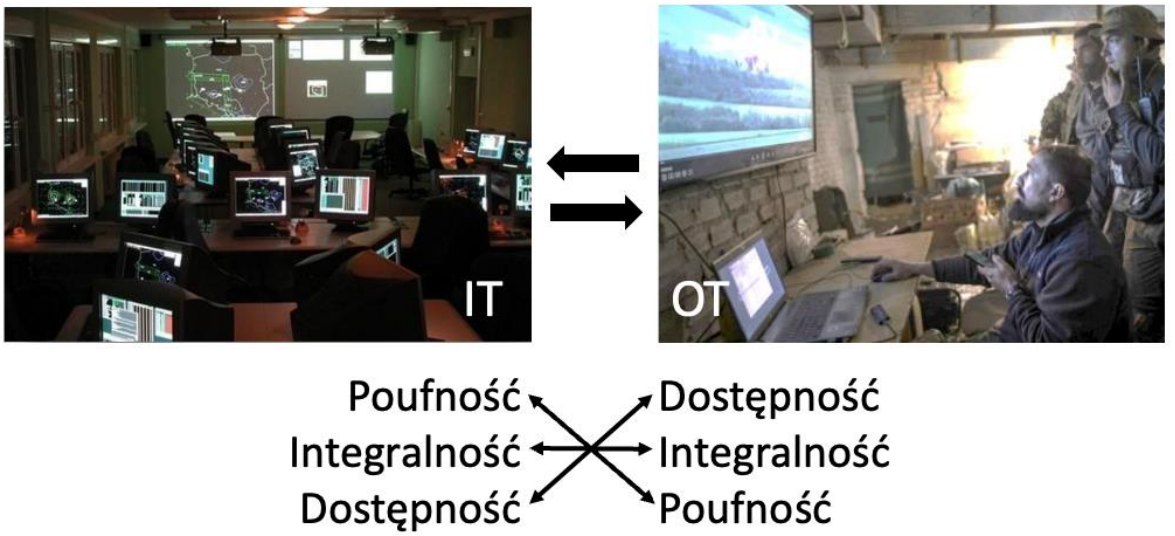


Fig. 36. Changing IT to OT and their priorities in the face of the threat of kinetic conflict. NATO command system (left side), operational command post in Ukraine (right side).
Source: Brigadier General M. Chmielewski for MBA Cybersecurity WAT

At the moment of the threat of military kinetic conflict, priorities change. Some functionalities of stationary IT systems are transferred to field mobile OT systems, which increases the ability to move and disperse, important for the modern theater of war. The IT/OT transformation does not reduce the need for synchronization but shifts the priority of using PTP and the NTP protocols. It minimizes the need for the newest, non-routable but precise synchronization protocol PTP (IEEE1588) and increases the significance of the older, routable on the Internet – the NTP protocol. The transformation involves a multi-level market participation structure (Fig. 37). Listed on the Figure 37 hardware reminds in use inside of critical infrastructure IT/OT. It is also important to note the NTP protocol reminds basically in use by the NATO Link 22 distributed architecture.

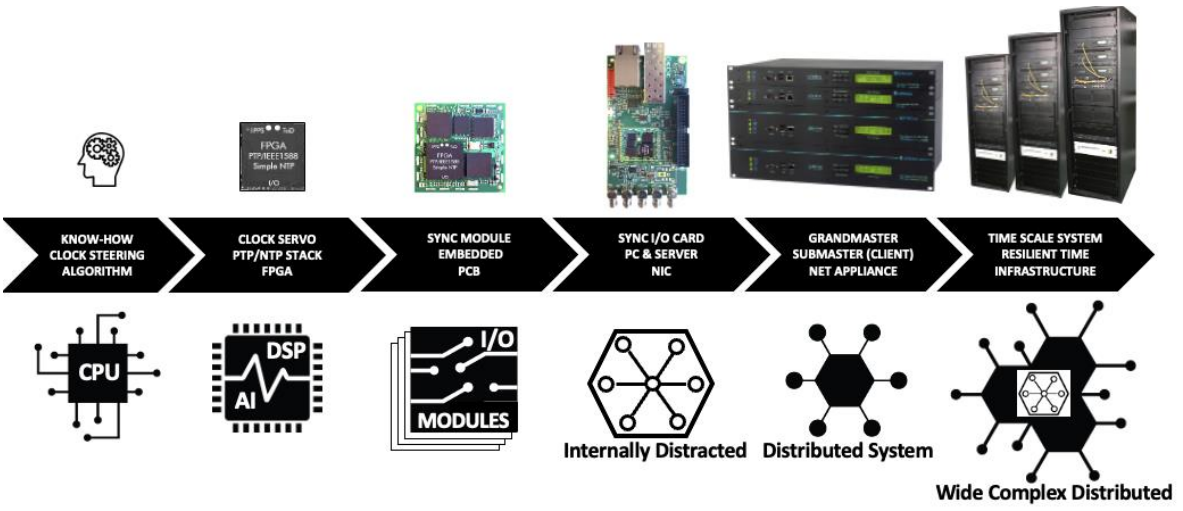


Fig. 37. Evolution (groups) of synchronization components used in IT/OT, from smallest to largest. Each element to the right contains the previous one.
Source: own

As long as distributed IT systems have access to the Internet, their resources can use the central synchronization system eCzasPL/eTimePL[31] [32], providing the UTC(k) time[33] [34] broadcasted from the NMI (Central Office of Measures of Poland - Figure 10). It should be considered that in the event of a cyber threat, the centralized structure of GUM may face availability limitations due to DoS-type cyberattacks. Therefore, it is crucial to plan for convergence and skillfully combine the features of the current centralization (eCzasPL/eTimePL, resistant to GPS jamming and spoofing) with simultaneous decentralization of synchronization sources. In such a case, the role of trusted, publicly available NTP time servers on the Internet from the NTP POOL[37] group increases (Figure 10). Unfortunately, using NTP POOL carries risks because it is not always known who manages them and the source of the UTC time. The public pool of NTP servers may also contain "rogue" servers that can deliberately behave unstably and provide incorrect UTC during a crisis. Such rogue NTP servers at POOL can be “poisoned” –prepared to serve false reference time to specific targets.

Building trust in public NTP servers requires a special quantitative statistical approach within the isolated and fully controlled national NTP POOL group. The more numerous the group of public NTP servers in a country (those whose time remains under the control of, for example, the national metrology institute NMI), the lower the external influence on desynchronizing IT/OT systems due to the use of such a national pool.

Since the outbreak of the war in Ukraine, the number of public NTP POOL servers in Russia[38] has increased from 150pcs by approximately 200%, reaching a max. amount of 450pcs. on the end of year 2024 – all, just in a short period of 6 months (since June 2024). Moreover, there is the technical possibility of remote maintaining NTP servers operating at POOL outside the borders of one's own country. This technique is so-called *poisoning* NTP POOL at specific region. For comparison, since the outbreak of the war in Ukraine in 2022, Sweden, aspiring to join NATO, has doubled its own population of public NTP servers. Two years earlier, Finland recorded a significant increase in servers. In 2012, during EURO financial crisis, Germany and France have increased the number of their public NTP servers over 100% (Figure 39).

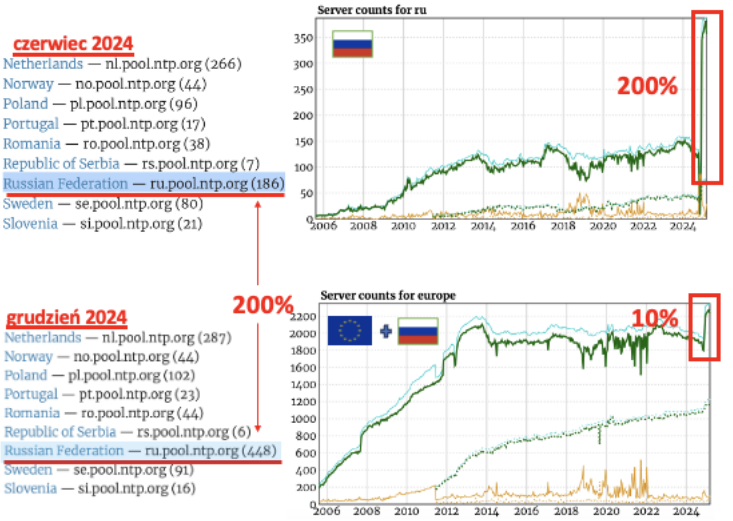


Fig. 38. Since the outbreak of the war, Russia has significantly increased the number of public NTP servers. In December 2024, this number exceeded 450 pcs. In June 2024 number was only 190 pcs. Source: https://www.ntppool.org/zone/ru

[37] https://www.ntppool.org.

[38] https://www.ntppool.org/zone/ru.

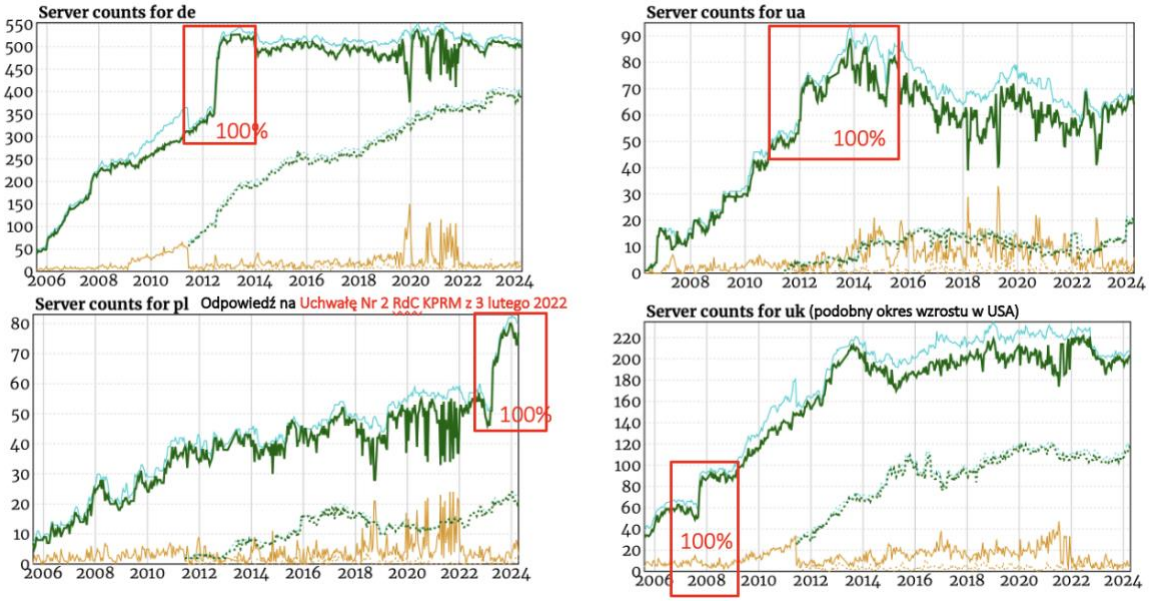


Fig. 39. Increases in the number of servers correlate with years of economic and political crisis.
Source: https://www.ntppool.org/zone/europe

A precise analysis of characteristics available via NTP POOL will likely indicate many interesting relationships between the number of a country's public NTP servers and economic, political and military events in the region. Incidentally the characteristics of the USA and UK (Figure 39) suggest an association of a 100% increase in the number of public NTP servers with the real estate financial crisis of 2008. Is it a coincidence that the two leading countries in the financial sector are increasing the number of their public servers so significantly at the same time? It seems that the national NTP POOL group is a serious candidate for a synchronization source in case of economic crises that may cause social unrest or when there is a risk of kinetic conflict in the country.

An interesting description is found in the justification of Polish Resolution[39] No. 2 of the Council for Digitization at the Ministry of Digital Affairs dated February 3, 2022. It recommends that the Office of the Prime Minister (KPRM) increase the number of Polish public NTP servers in the national pool. This action is preventive in nature. On one hand, it aims to reduce the statistical weakening effect of *poisoned (false ticking)* NTP servers intentionally inserted into the *pl.poo.ntp.org* domain that introduce incorrect UTC time patterns. On the other hand, it will statistically ensure more probable access to these *healthy (true ticking)* trusted NTP servers. On the May the 5th 2025, another Recommendation[40] was released recommending usage of eCzasPL/eTimePL trusted time.

For the prevention to be effective, a special NTP configuration is necessary. If we decide to use the NTPPOOL group, we should only use the source NTP software available for download at www.ntp.org. This software can be compiled from C/C++ sources into a binary version that runs as a service on all versions of the Microsoft Windows operating system. In that case, multiple NTP sources should always be applied and listed in the ntp.conf file:

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

[39] https://www.gov.pl/attachment/a748fde4-8912-4412-b8b2-0718e4e27e0b.
[40] https://www.gov.pl/attachment/179f2961-2278-4f9f-a328-14b462920e07.

and then complete eCzasPL/eTimePL ref. clocks:

server tempus1.gum.gov.pl
server tempus2.gum.gov.pl
server tempus3.gum.gov.pl

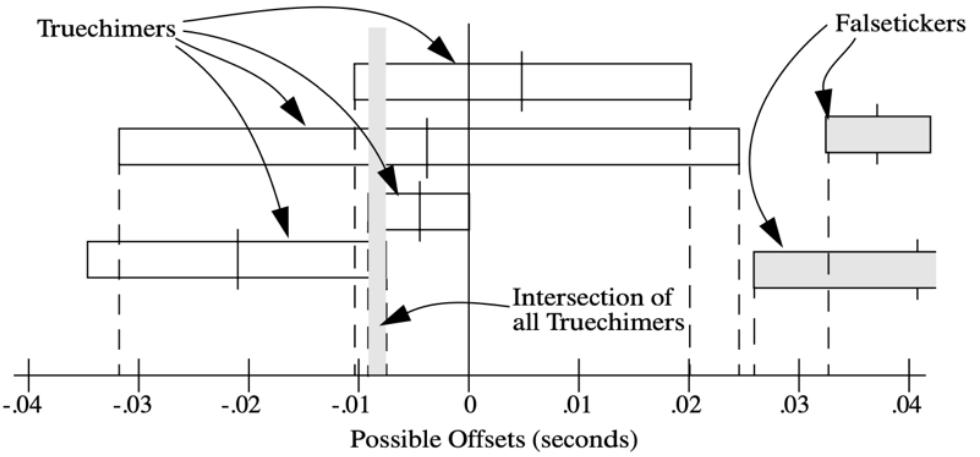


Fig. 40. Ref. UTC is the smallest common interval of the largest group of 'truechimers.'
Source: D. Deeths, G. Brunette (Sun Microsystems Blueprints 2001)

Using multiple UTC sources simultaneously activates the anti-spoofing mechanism built into NTP, which protects against desynchronization. In other words, by using multiple NTP servers simultaneously, the NTP protocol itself can select the 'good' ones (truechimers) and reject the 'bad' ones (falsetickers). The mechanism is based on Marzullo's algorithm[41]. It was designed in the early 1980s to protect against desynchronization of US military defense systems. It is an experimentally proven decision-making algorithm for selecting the best available time sources. The middle part of the rectangle represents the UTC indication on a remote NTP server. The right and left sides of the rectangle (the size of the area) represent the maximum UTC error seen by NTP client. Each client sees this error differently because it depends on network location, traffic intensity, routing paths, link asymmetry, etc. Like in Einsteinian relativity, time is different for each observer, the ref. time and sync error will be different for each NTP client too.

In places where distributed military OT systems do not have access to the Internet and cannot utilize eCzasPL/eTimePL or NTP POOL, and wherever system operations require external synchronization in GNSS restricted environments, mobile synchronization devices like Time Loaders can be helpful. They are used to transfer the UTC standard between a reference laboratory station and the target synchronized defense system. These devices are equipped with very high-quality oscillators for maintaining time (OCXO or Rubidium) and battery power. They support the operation of military autonomous systems such as UAVs, radars/EO, missile defense systems, and any other ground, naval, or airborne systems that require external UTC synchronization (Figure 40).

[41] https://en.wikipedia.org/wiki/Marzullo%27s_algorithm.

Fig. 41. Polish portable UTC "defibrillator" ELPROMA, on the right Israeli "Time Loader." The size of the device determines the UTC support time and depends on the battery capacity. Source: Elproma

Fig. 41a. Advertisement for the Israeli mobile Time Loader (defibrillator). source: Focus Telecom, Israel

5. Evolution to Autonomous UTC Time Scale Systems

The risk of effective disruption of GNSS group satellite systems has led technology to the only remaining direction to solve the problem – the development of autonomous UTC time scales. These are ePRTC clocks controlled by new-generation AI, which aggregated into groups, create coherent cnPRTC clock networks. Full autonomy of the time source requires, as a first step, the elimination of UTC leap seconds. Therefore, ITU[42] urgently strives to eliminate this dangerous single 1 second for computer technology (source [6]). The Polish delegation[43] has made a significant contribution to breaking the 20-year negotiation impasse with Russia. It turns out that without a continuous UTC time scale, large-scale autonomy of devices, robots, or cars cannot exist.

Autonomous UTC time scale systems are network solutions. They are equipped with software clocks that, with the help of AI, learn the characteristics of atomic clocks. After several weeks of learning using machine learning, ePRTC clocks gain the ability to make short- and medium-term predictions of the UTC time scale. When appropriately combined into groups (clock aggregation), they form cnPRTC networks that can better predict the future and maintain long-term consistency with the BIPM UTC scale.

Of course, even the most intelligent autonomous UTC time scale system requires periodic calibration to ensure the accuracy of time and frequency standards generated. The Common View (CV) technique is used for this purpose, involving the observation of commonly visible satellites (Figure 42). The advantage of this method is the indirect use of satellite C for the direct comparison of the indications of clocks A and B with each other

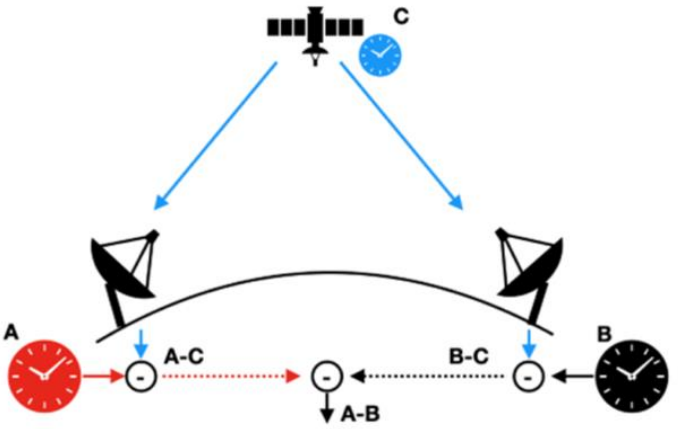


Fig. 42. The Common View method is used for the comparison of the indications of clocks A and B
Source: NIST

The future of autonomous UTC time scales goes significantly beyond applications on Earth. Currently, advanced work on a lunar time scale is already underway at BIPM[44], and Mars is next in line. Space is changing before our eyes and is becoming a place for the search for valuable natural resources that we want to import to Earth. It is also a place of competition for influence among powers such as the USA, China, the EU, Russia, and India.

[42] https://www.itu.int/en/itunews/Documents/2023/2023-02/2023_ITUNews02-en.pdf.
[43] https://www.gov.pl/web/instytut-lacznosci/polski-sukces-na-konferencji-itu.
[44] https://www.bipm.org/en/-/2023-05-22-moon-time.

.

The author thanks Waldemar Sielski, Adam Widomski, Leszek Widomski, Krzysztof Borgulski, and Mikołaj Wojciechowski for their comments

Literature

[1] B. Szafrański, collective work "Cybersecurity redefinition of threats", Chapter XII, W. Paluszyński "Underestimated threat – the source and distribution of time", pp. 177-214, Military University of Technology (2023).

[2] C4ADS Innovation for Peace "Above us only stars – Exposing GPS spoofing in Russia and Syria" (2019).

[3] M. J. Murrian, L. Narula, P.A. Iannucci, S. Budzien, B.W. O'Hanlon, M. Psiaki "First results from 3 years of GNSS Interference Monitoring from Low Earth Orbit" Aerospace and Ocean Engineering, Virginia Tech, ION, Researchgate (2021).

[4] W. Lewandowski, M. Marszalec "A Brief History of UTC Leap Second", JTIT Journal of Telecommunications and Information Technology, No 4 (2023).

[5] 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).

[6] P. Tavella, T. Widomski (Elproma) "The impact of UTC on Industry 4.0" "The Future of Coordinated Universal Time" ITU-News No 02 page 28 (2023)

[7] T. Widomski "Synchronization security at Smart Gird", DG-Energy (2017).

[8] P. Tavella, J.X. Mitrovica "Melting ice solves a leap-second problem – for now", Nature "News & Views Forum", No March 27th (2024).

[9] Doctoral thesis "Security of Time Synchronization for PMU-based Power System State Estimation: Vulnerabilities and Countermeasures", E. Shereen's Doctoral Thesis in Electrical Engineering, KTH Sweden Royal Institute of Technology (2021).

[10] Collective work M. Han, P.A. Crossley, "Vulnerability of IEEE 1588 under Time Synchronization Attacks", IEEE Power & Energy Society General Meeting (2019).

[11] Collective work W. Alghamdi, M. Schukat and others, "Precision time protocol attack strategies and their resistance to existing security", Cybersecurity, No 4 (2021).

[12] Collective work W. Gao, Hong Li, J. Li, M. Lu, "GNSS Time Synchronization Attack Detection and Discrimination Based on Correlations of Calculated Clock Drift Time Differences", in: Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), September 2020.

[13] Collective work T. Widomski, J. Użycki, K. Borgulski and others, "Trusted Time Distribution with Auditing and Verification Facilities Project TSI#2", Conference Precise Time and Time Interval Meeting, ION/PTTI Monterey, California (2016).

[14] Collective work Z. Guo, Y. Ni and others W. S. Wong, L. Shi, “Time Synchronization Attack
and Countermeasure for Multi-System Scheduling in Remote Estimation”,
Cornell University (2019).
[14] Collective work A. Mujunen, J. Atrokoski, M. Tornikoski, J. Tammi “GPS Time
Disruptions on 26-Jan-2016” Metsähovin Metsähovi Radio Observatory (2016).
[15] T. Widomski, “Analysis of time desynchronization phenomenon as a new cyber-weapon
destabilizing the critical infrastructure of the state” MBA Cybersecurity Master's Thesis
WAT (June 2024)."