CYBERBEZPIECZEŃSTWO

REDEFINICJA ZAGROŻEŃ

POD REDAKCJĄ NAUKOWĄ
BOLESŁAWA SZAFRAŃSKIEGO

Wojskowa Akademia Techniczna

Cyberbezpieczeństwo – Redefinicja Zagrożeń

Rozdział 12

Niedoceniane zagrożenie – źródło i dystrybucja czasu

Wiesław Paluszyński
Polskie Towarzystwo Informatyczne

1. Wstęp

Jest znana anegdota przytaczana przez Marka Abramowicza w latach osiemdziesiątych w Paryskiej Kulturze. Mówi ona o tym jak w 1925 roku Polskie Radio rozpoczęło nadawanie programu i w południe podawało z dokładnością do pół sekundy wzorcowy sygnał czasu z obserwatorium astronomicznego w Krakowie. Tak duża dokładność robiła wielkie wrażenie w kraju i za granicą. Redakcja jednego z dzienników wysłała dziennikarza do profesora Tadeusza Banachiewicza, żeby dowiedzieć się skąd astronomowie wiedzą, kiedy jest południe z tak fantastyczną dokładnością. Profesor Banachiewicz wyjaśnił jak bardzo to jest proste mówiąc: „Reguluję swój zegarek codziennie rano w drodze do pracy, kiedy przechodzę obok witryny sklepu zegarmistrzowskiego, który oferuje szwajcarskie zegarki najlepszych marek. Używając wskazań swojego zegarka uderzam punktualnie w południe w kowadełko i sygnał ten emituje na terenie kraju Polskie Radio."

Dziennikarz udał się do sklepu zegarmistrzowskiego, aby zapytać sprzedawcę skąd ten wie, jak ustawić zegary na witrynie z tak dużą dokładnością i usłyszał odpowiedź: „Codziennie włączam radio i w południe profesor Banasiewicz podaje mi dokładnie z dokładnością do pół sekundy informacje, kiedy jest południe i ustawiam swoje zegary."

Niezależnie od tego jak śmieszna jest ta anegdota, zawiera ona bardzo głęboką prawdę, że nie ma żadnej innej metody sprawdzania zgodności czasu pokazywanego przez zegary niż porównywanie ich wskazań między sobą[1]. Synchronizacja wymaga więc zawsze zaufanego dokładnego źródła odniesienia, a jego fałszowanie będzie miało daleko idące konsekwencje dla bezpieczeństwa ludzi i maszyn.

Blisko 100 lat później, w XXI wieku znaczenie synchronizacji zaczęło odgrywać szczególną rolę, zmieniając paradygmat cyberbezpieczeństwa zbyt zależnej od GNSS silnie zautomatyzowanej rozproszonej architektury każdej infrastruktury krytycznej. Stało się to na tyle istotnym zagadnieniem stabilności systemów teleinformatycznych w erze przemysłu 4.0, że w lutym 2020 roku prezydent USA Donald Trump podpisał specjalną dyrektywę EO13905[2], rekomendującą uniezależnienie amerykańskich infrastruktur krytycznych od GPS. Okazało się, że zamiast łamać zabezpieczenia chronione

[1] Fragment wystąpienia Stanisława Bajtlika „Co to jest czas", https://youtu.be/BGE_kn1aM80.

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

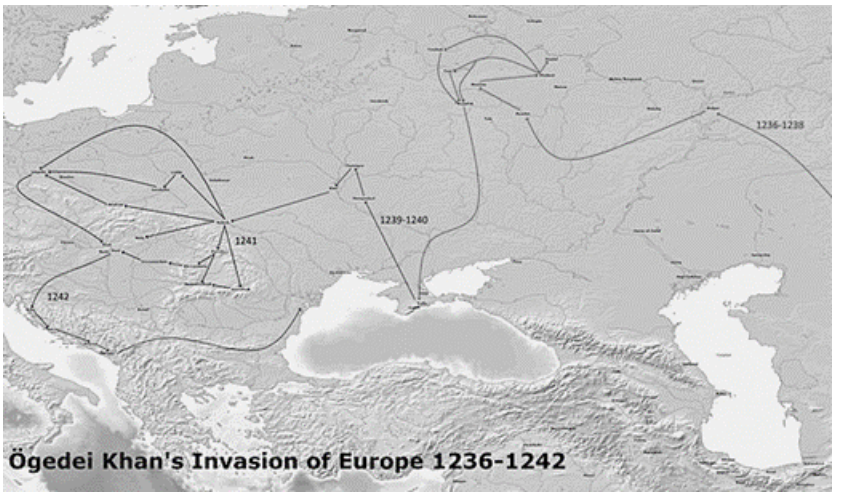
matematycznie Infrastrukturą Klucza Publicznego (PKI), znacznie prościej jest destabilizować pracę infrastruktury manipulując czasem pochodzącym z satelitów GNSS i rozsynchronizowując ją. Dyrektywa EU13905 objęła zasięgiem wszystkie gałęzie przemysłu USA, wymuszając wiele zmian i co za tym idzie inwestycji w nowe technologie w tym alternatywne satelitarne systemy PNT (np. Xona Space, Iridium itp.) oraz usługi szyfrowanych połączeń z wzorcami atomowymi czasu w NIST. Niniejszy artykuł porusza rodzaj zagrożeń związanych z rozsynchronizowaniem infrastruktur krytycznych wymienionych w tabeli 1.

Tab. 1. Rodzaje infrastruktur krytycznych omawianych w artykule

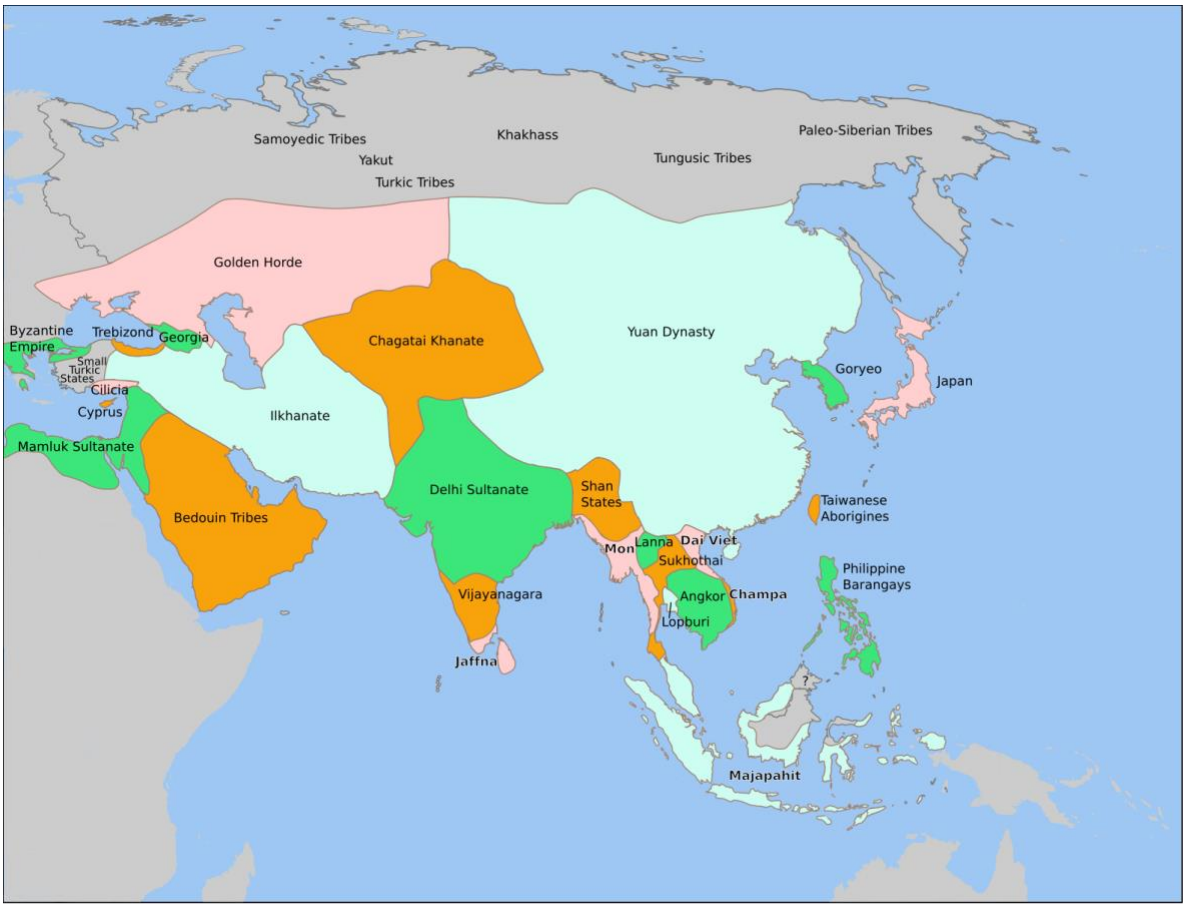
Chmura Krajowa/ Centra Danych	Inteligenta energetyka smart-grid	Telekomunikacja Lte/5G
Finanse i giełda (HFT)	Ruch lotniczy i szybkie koleje	Przemysł 4.0 (Inteligenta fabryka)
Autonomiczne pojazdy i robotyka	Inteligentne miasto	Przemysł obronny
Administracja publiczna	Zarządzanie bezpieczeństwem ISO 27000	Przemysł kosmiczny

Aby wprowadzić do problemu destabilizowania rozproszonej architektury infrastruktury teleinformatycznej przy pomocy synchronizacji, przenieśmy się na chwilę do XIII wiecznego imperium Genghis Khana. To drugie co do wielkości terytorium imperium (w historii ludzkości), zaczynało się daleko na wschodzie Azji obejmując współczesny Pekin, rozciągało się po zachodniej stronie na europejskich obszarach współczesnej Rosji, zaś na południu obejmowało Iran, Irak, Indie, wracając na wschód przez Tybet. Imperium było tak duże, że jego centralne zarządzanie, a zwłaszcza prowadzenie rozproszonych na rubieżach imperium wojen było cywilizacyjnym wyzwaniem. Czas potrzebny na pokonanie wielkich dystansów liczonych w tysiącach kilometrów, przez emisariuszy Genghis Khana rozwożących rozkazy i przywożących wieści z pola bitew, zajmował im wiele tygodni podróży i nie wszyscy docierali do mongolskiego monarchy. Coraz częściej zdarzało się, że informacje o zwycięskich bitwach docierające do cesarza były już nieaktualne, bo zdobyte ziemie były ponownie utracone. Przy tak wielkim obszarze, czas przepływu informacji wewnątrz systemu władzy nie przystawał do oczekiwań i nie pozwalał na skuteczne centralne podejmowanie decyzji cesarskich. To było początkiem klęsk i w efekcie upadku cesarstwa. Skalę problemu obrazują rysunki 1, 2 i 3.

Rys. 1. Ekspansja Imperium Mongolskiego w XII wieku
Źródło: Mongol Empire map.gif – https://en.wikipedia.org



Rys. 2. Inwazja na Europę
Źródło: 1236-1242 Mongol invasions of Europe.jpg – https://en.wikipedia.org



Rys. 3. Azja w XIV wieku
Źródło: Asia in 1335.svg – https://en.wikipedia.org

Współczesna technika musi się zmierzyć z analogicznym problem przerostu wielkości. Osiągając granice maksymalnej prędkości pracy procesorów, świat przyjął jedyny pozostały mu kierunek zwiększania wydajności przetwarzania informacji – zrównoleglanie obliczeń. Wraz z rozwojem technik komunikacji rozpoczął się trwający cały czas proces rozpraszania się infrastruktur IT, który obecnie przyjął niebezpieczny trend silnych współzależności całych systemów sterujących, również przemysłem. Zjawisko stało się szczególnie niebezpieczne w erze rozwoju przemysłu 4.0, gdzie powierzono sztucznej inteligencji (AI – ang. *Artificial Intelligence*) predykcyjne sterowanie automatyką przemysłową. Uzależnienie procesów biznesowych, przemysłowych od korelacji w czasie całych podsystemów zarządzania, eksponuje dziś technikę przetwarzania równoległego w domenie czasu (TCC – ang. *Time Coordinated Computing*) podsuwając cyberprzestępczości pomysł i narzędzie na skuteczny atak polegający na manipulacji ustawieniami zegarów. Rozsynchronizowanie czasu infrastruktur krytycznych grozi dziś awariami o nieprzewidywalnych konsekwencjach, szczególnie w energetyce, telekomunikacji, bankowości, na giełdach, w transporcie lotniczym i kolejowym. Coraz częściej mówi się o widmie wielkiej awarii, wywołującej efekt domina, awarii na skalę kontynentu. Użycie terminu „blackout" nie jest nadużyciem.

Nadmiarowa złożoność systemów teleinformatycznych i zbyt ścisła ich współzależność, w tym ta od satelitarnych systemów rodziny GNSS, uprawnia do

włączenia problematyki czasu i synchronizacji czasu jako nowego ważnego elementu współczesnego cyberbezpieczeństwa.

Ta relacja jest obszarem zainteresowania autora tej publikacji, który analizując dostępną literaturę dotyczącą omawianego tematu, a także publikacje specjalistyczne i analizy występujących przypadków tzw. „ataku na czas" dokonał syntezy głównych obszarów wiedzy dotyczącej tych zagrożeń i sposobów minimalizacji ryzyk związanych z tym obszarem cyberbezpieczeństwa.

Główną tezą jaką autor udowadnia w tym artykule, jest założenie, iż istnieje możliwość prowadzenia działań sabotażowych mogących destabilizować pracę systemów teleinformatycznych bez konieczności włamywania się do dobrze chronionych sieci wewnętrznych. To zmienia dziś cały paradygmat cyberbezpieczeństwa. Manipulując zegarami fałszuje się poprawny pomiar opóźnień sieci, to wprowadza z kolei zaburzenie, w którym prawidłowe dane mogą zostać odrzucone, a zdezaktualizowane zbyt długą podróżą informacje zostaną błędnie zaakceptowane jako prawidłowe.

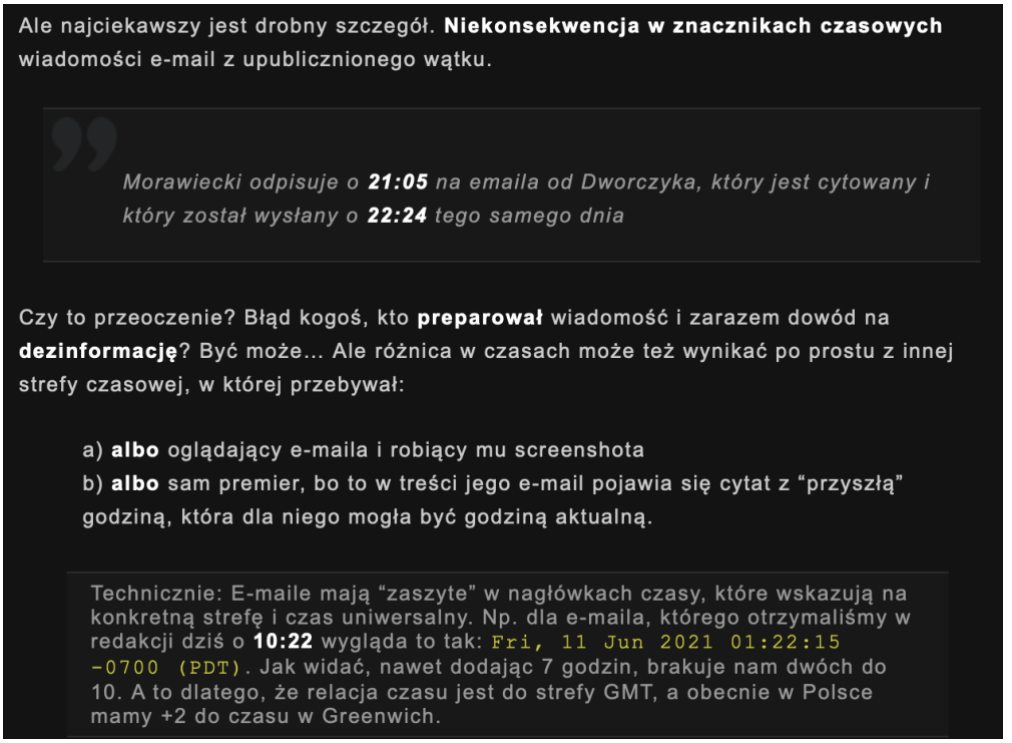
2. Opis problemu

Synchronizacja czasu to zagadnienie specjalistyczne i mało znane, a więc wygodne dla wykorzystania do ataku przez cyberprzestępców. W przypadku ataku długo pozostaje niezauważone, jest kolokwialnie mówiąc „poza podejrzeniem". Nasza intuicja podpowiada, że skoro umiemy czytać zegary, to sprawa nie może być trudna – nic bardziej mylnego. Widząc czas na pulpicie komputera czy na wyświetlaczach ulicznych, również mamy do czynienia z synchronizacją, jednak tak rozumiana synchronizacja nie stanowi zagrożenia dla systemu teleinformatycznego. Natomiast precyzyjne określanie jednoczesności zdarzeń z bardzo dużą dokładnością i małym błędem jest dzisiaj niezbędne, ponieważ jest krytyczne dla stabilności działania silnie rozproszonej infrastruktury. Również zgodność czasu w makroskali pojedynczej sekundy stanowi istotne wyzwanie rozpoczętego procesu transformacji cyfrowej administracji publicznej i przemysłu – certyfikacji, podpisu elektronicznego, uwierzytelnionego obiegu dokumentów itp.

Dziś synchronizacja jest elementem cyberbezpieczeństwa. Zamiast włamywać się do dobrze chronionej sieci wewnętrznej TCP/IP, prościej jest destabilizować pracę systemu teleinformatycznego poprzez zdalne zaburzenie synchronizacji, np. manipulując GPS-em, od którego jesteśmy zbyt zależni[3]. Manipulując zegarami i czasem, można zaburzyć chronologię zdarzeń zapisywanych w dziennikach LOG. Traci się w takiej sytuacji bezpowrotnie szansę analizy logiki błędów i nie można ustalić prawdziwej przyczyny awarii. To temat ważny z punktu widzenia zarządzania bezpieczeństwem zgodnie z normami rodziny ISO 27000. Najlepiej pokazać ten problem na aktualnym przykładzie.

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

Gdyby w tzw. sprawie „Maili Ministra Dworczyka”[4], hakerzy zmienili adekwatnie znaczniki czasu, interpretacja zdarzenia mogła wyglądać inaczej i trudno byłoby zakładać atak hakerów. To dzięki „niezmienionym” znacznikom zapewniającym rzeczywistą chronologię, mieliśmy do czynienia z sytuacją, w której skutek wyprzedza własną przyczynę, tzn. Premier Morawiecki odpowiada na pytania zanim Minister Dworczyk je zadał (rysunek 4).



Rys. 4. Analiza maili w tzw. „Aferze ministra Dworczyka”
Źródło: https://niebezpiecznik.pl/post/mail-morawiecki-dworczyk/

Obecnie obszary ryzyka związane z bezpieczeństwem wyznaczają dwa nowe rodzaje ataków związanych z synchronizacją i czasem:

- **Atak na czas** (TSA – ang. *Time Synchronization Attack*),
- **Atak na opóźnienie** (TDA – ang. *Time Delay Attack*).

Są one jednymi z najbardziej prawdopodobnych, zarazem najniebezpieczniejszych dla zautomatyzowanej i uzależnionej od GPS[5] gospodarki. Sprawa jest na tyle poważna, że jest przedmiotem międzynarodowych prac w grupach ITU-R (WP-7A) w Genewie przy ONZ, gdzie krajowa delegacja KPRM wniosła w 2021r pierwszą Polską kontrybucje opartą na pracach polskiego producenta serwerów czasu firmę ELPROMA. Ze streszczeniem Polskiego dokumentu można się zapoznać na stronach PTI i PIIT[6]. Dlatego mówi się dziś o rosnącym znaczeniu czasu urzędowego jako alternatywy satelitarnego wzorca czasu z GNSS.

[4] Chronologia zdarzeń maili Ministra Dworczyka – https://niebezpiecznik.pl/post/mail-morawiecki-dworczyk/.

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

[6] PIIT Rekomendacja dot. wstrzymania obsługi sekundy przestępnej UTC https://www.piit.org.pl/o-nas/aktualnosci/elproma-rekomendacja-dot.-wstrzymania-obslugi-sekundy-przestepnej-utc.

W Polsce prowadzony jest przez Główny Urząd Miar RP (GUM) projekt o nazwie eCzasPL[7]. Celem głównym projektu jest dostarczenie usługi wiarygodnej i niezawodnej dystrybucji sygnałów czasu urzędowego UTC(PL), obowiązującego na obszarze Rzeczypospolitej Polskiej oraz usług monitorowania synchronizacji, tak aby skutecznie móc zapobiegać w przyszłości zdarzeniom takim jak awaria systemów PKP[8] w dniu 17 marca 2022. Z analizy tego przypadku wynika, że podobne w objawach i skutkach awarie można wywoływać atakami TSA i TDA.

Niestety, zapewnienie skutecznego monitorowania pracy zegarów systemowych w systemach teleinformatycznych pozostaje nie mniej trudnym technicznie zadaniem niż sama ich synchronizacja. Wiąże się to z ryzykiem hybrydowych działań sabotażowych jakie mogą towarzyszyć atakom radiowym na czas (TSA). Dziś, przemysł europejski powinien się liczyć z możliwością takich działań jak np. przerywanie łączności światłowodowej, a w konsekwencji przerwy komunikacji TCP/IP, z czym mierzyły się w październiku 2022 niemieckie koleje DB[9]. Doświadczenie niemieckie przywołuje z kolei retrospektywnie inne zdarzenie z Polski – pożar Mostu Łazienkowskiego w Warszawie w roku 2015. W lutym 2023 minęło właśnie 8 lat od tego pożaru[10], w którego następstwie uszkodzeniu uległy ważne komunikacyjne połączenia światłowodowe. Awaria łączy w połączeniu z awarią łączności bezprzewodowej, stawia ważne pytanie o bezpieczeństwo zapewniające stabilność pracy współczesnych infrastruktur krytycznych. Stawia pytanie czy jesteśmy przygotowani na zagłuszanie sygnałów satelitarnych (ang. *GPS jamming*) lub fałszowanie (ang. *GPS spoofing*). Z prawidłową synchronizacją wiążą się ściśle również systemy archiwizacji, o czym miało okazję przekonać się kilka tysięcy pasażerów w USA[11] w styczniu 2023.

Liczba ataków zagłuszania i spoofing GPS wzrosła po rosyjskiej aneksji Krymu w 2014 roku. Zjawisko uległo nasileniu w związku z aktywnym udziałem armii rosyjskiej w działaniach wojskowych rejonie Syrii[12,13]. Obecna agresja na Ukrainę w roku 2022 jeszcze bardziej zintensyfikowała występowanie opisywanego problemu. Skuteczność występujących destabilizacji w systemach radiowych wyjaśnia między innymi nowy rodzaj elektronicznej broni „Electronic Warfar", która znalazła się na wyposażeniu armii rosyjskiej,

[7] Główny Urząd Miar RP, Projekt eCzasPL https://www.gum.gov.pl/pl/projekty-eu/e-czaspl/3632,e-CzasPL.html.

[8] Runek Kolejowy, awaria PKP 17/03/2022, https://www.rynek-kolejowy.pl/mobile/alstom-nie-bylo-cyberataku-byl-nasz-blad-107195.html.

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

[10] Pożar mostu Łazienkowskiego w Warszawie. Nasza Warszawa, https://warszawa.naszemiasto.pl/pozar-mostu-lazienkowskiego-w-warszawie-osiem-lat-temu-po/ar/c1-9209489.

[11] Ruch lotniczy w USA wstrzymany, CNBC, styczeń 2023 "FAA system outage disrupts thousands of flights across U.S", https://www.cnbc.com/2023/01/11/faa-orders-airlines-to-pause-departures-until-9-am-et-after-system-outage.html.

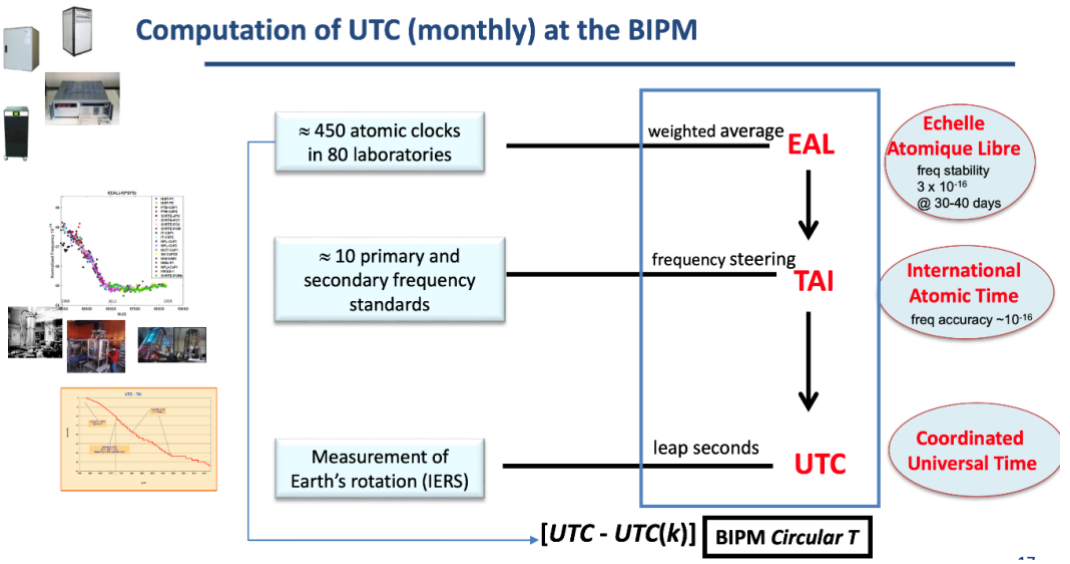
[12] Institute of Navigation Webinar, "First results from three years of GNSS interference monitoring from low Earth orbit", https://www.youtube.com/watch?v=XDbn85IBIus&t=0s.

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

a co opisuje raport szwedzki[14] z 2018 roku. W latach 2018–2021 pojawiają w mediach zachodnich (np. CNN[15]) coraz częstsze informacje dotyczące możliwości manipulacji sygnałami GNSS, w tym szczególnie amerykańskim GPS.

3. Praca w domenie czasu – nieciągłość skali UTC – sekundy przestępne

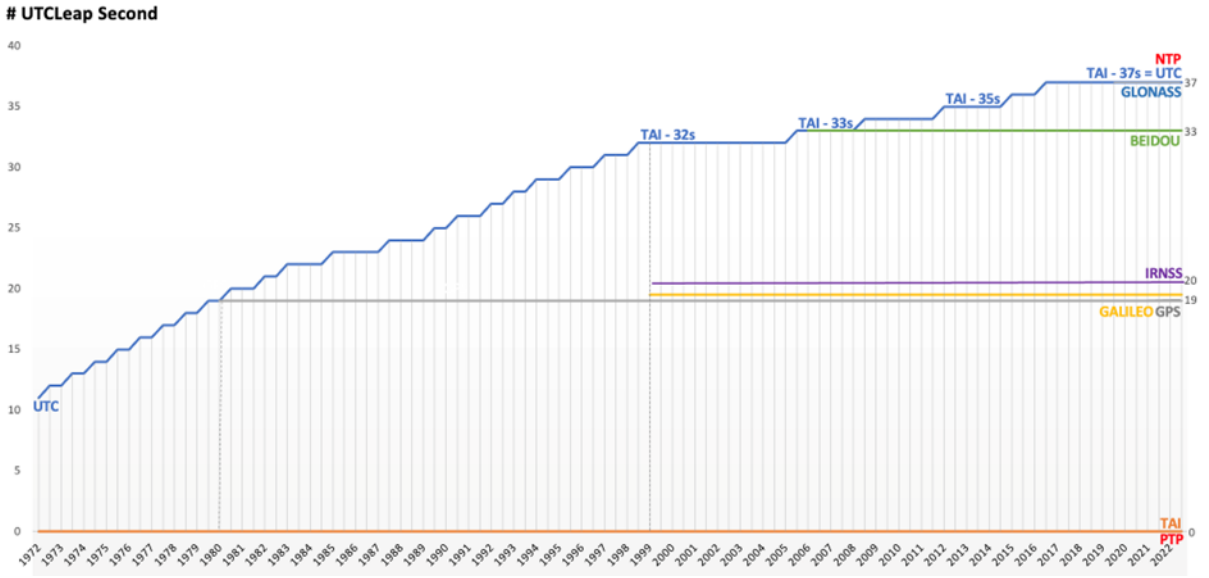
Współczesna informatyka opiera się na skali czasu UTC (ang. *Universal Coordinated Time*). Skala ta używana jest przez jądro systemów operacyjnych (OS) takich jak Windows, Linux, Unix, które różnicują wskazania zegarów na pulpicie w zależności od bieżącej strefy czasowej (ustalanej siecią komputerową lub z użyciem GNSS), ustawień językowych itp. Czas lokalny używany jest w dziennikach zdarzeń LOG, używa go system plików, bazy danych, systemy archiwizacji itp. Jednak gdzieś głęboko w systemie operacyjnym czas zawsze mierzony jest w skali UTC. Nieciągły charakter skali czasu UTC (rysunek 5) znany jest jako problem tzw. *sekundy przestępnej* (ang. *leap second*). Jest to jedna sekunda dodawana lub odejmowana bardzo nieregularnie w celu kompensacji różnicy między czasem astronomicznym takim jak historyczny GMT (ang. *Greenwich Mean Time*), a bardzo stabilnym czasem odmierzanym przez zegary atomowe współtworzące skalę czasu atomowego TAI (rysunek 5a).



Rys. 5a. Proces wytwarzania skali UTC
Źródło: BIPM, Patrizia Tavella

Ujmując prościej, UTC opiera się na zegarach atomowych i skali TAI, ale co jakiś czas koryguje niestabilność ruchu obrotowego Ziemi, która długoterminowo regularnie spowalnia (doba jest coraz dłuższa), chociaż bywa też, że okresowo przyspiesza.

[14] Jonas Kjellén, „Russian Electronic Warfare" https://www.foi.se/rest-api/report/FOI-R-4625-SE.
[15] CNN "GPS spoofing: Russia's new cyberweapon", https://edition.cnn.com/videos/cnnmoney/2017/11/03/russia-gps-spoofing-cyberweapon-lon-orig-mkd.cnn.



Rys. 5b. Wewnętrzne skale czasu poszczególnych systemów satelitarnych różnią się względem skali czasu atomowego TAI o: GPS 19s, IRNSS 20s, BEIDOU 33s, GLONASS 37s. Protokół NTP używa skali UTC zawierającej sekundy przestępne, co wymaga prawidłowej obsługi dodawania/odejmowania przestępnych sekund w sposób ciągły (nie skokowy). Z kolei protokół PTP IEEE1588 używa rozbitej skali UTC na składowe TAI i liczbę sekund przestępnych. Podmiana liczby sekund przestępnych może rozsynchronizować infrastrukturę krytyczną prowadząc do jej awarii
Źródło: własne

O korekcie sekundy decyduje organizacja IERS (*International Earth Rotation and Reference Systems Service* www.iers.org) i sygnał zmiany przekazywany jest siecią TCP/IP, systemy radiowe fal długich (np. niemiecki nadajnik DCF77 nadający wzorzec czasu na falach długich o częstotliwości 77.5 kHz i długość fali 3868.2897806 metra) i przez satelity GNSS. Niestety rozwiązanie takie jak się okazało w praktyce, ma kluczowe negatywne znaczenie dla stabilności, a w konsekwencji dla cyberbezpieczeństwa rozwijającego się w tej i kolejnych dekadach struktur przemysłu 4.0. Ma też wpływ na wszystkie infrastruktury krytyczne. Stąd pojawiają się takie problemy jak:

- rozbieżności czasowe w systemie rozproszonym, w którym ważność danych jest określana na podstawie różnicy między znacznikiem czasu zdalnego czujnika/ komputera, a znacznikiem czasu odbieranego lokalnego centralnego serwera zarządzającego. Może to prowadzić do akceptacji błędnych danych (błędnie obliczone opóźnienie podróży pakietów siecią TCP/IP), a w konsekwencji do błędów i awarii. Ryzyko wzrasta wraz z rosnącą popularnością sieci TSN (ang. *Time Sensitive Networking*), i przetwarzania rozproszonego TCC (ang. *Time Coordinated Computing*). Ma to znaczenie zwłaszcza dla telekomunikacji 5G, nowoczesnej 2-kierunkowej inteligentnej energetyki smart-grid, sieci przemysłowych *low-latency.*
- awarie oprogramowania, a tym firmware'u urządzeń IoT/IT, opartych na Windows/Linux/Unix. Należy zauważyć, że każde produkowane obecnie urządzenie sieciowe ma firmware oparty na jądrze (kernel) jednego z powyższych systemów operacyjnych (OS). Nieoczekiwane skoki czasu wprowadzone przez sekundę przestępną UTC są niebezpieczne dla stabilności pracy jądra OS i mogą wywołać

awarię krytyczną zakończoną komunikatem „*kernel panic*”. Taka awaria wynika z zaburzenia niskopoziomowej chronologii zdarzeń wewnątrz jądra OS, które odpowiada za organizację tzw. współbieżności, wielozadaniowości, wielowątkowości systemu operacyjnego. Jest to bardzo głęboki poziom systemu operacyjnego pozostający poza dostępnością dla administratorów systemowych, a więc również poza jakąkolwiek kontrolą.

Dokument ITU-R TF.460-6 (link) wskazuje jako możliwość wprowadzenia lub usunięcia sekundy przestępnej, koniec każdego miesiąca o północy UTC. Preferuje priorytet scenariusza „A” 30 czerwca i/lub 31 grudnia; a następnie scenariusz „B” 31 marca i/lub 30 września o czym decyduje organizacja IERS i informuje co najmniej na 8 tygodni przed wdrożeniem *leap second UTC*. Obsługa tworzy skokową zmianę o jedną sekundę skali UTC powodując nieciągłość skali czasu uniwersalnego. Skok należy traktować jak swoistą „dziurę w czasie”, która tworzy utratę korelacji między światem komputerów, a upływem czasu jakiego doświadczamy w rzeczywistym newtonowskim świecie, w którym żyjemy.

Obsługa, zawsze wywołuje negatywne skutki w IT, ale ich wielkość jest trudno przewidywalna. Wiele urządzeń, wymaga twardego restartu. Firma CISCO rekomendowała swoim klientom CATALYST wyłączenie urządzeń na kilka godzin przed dodaniem 37 sekundy przestępnej w grudniu 2016. Również IBM Redhat Linux z powodu wykrycia błędu jądra ostrzegał o możliwości wywołania paniki jądra (kernel).

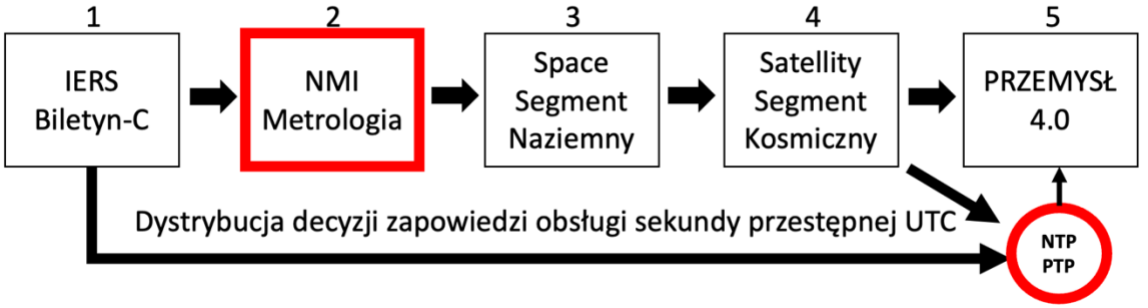
Wcześniej odczuwalność negatywnych efektów nie była aż tak bardzo dotkliwa. Dopiero z czasem wzrastająca ilość współzależności zaczęła zwiększać ryzyko dla systemów teleinformatycznych. Wprawdzie przyjęty harmonogram zmian A i B minimalizuje ryzyko dla biznesu i sektora finansowego, ale pozostaje ono nadal wysokie dla telekomunikacji, energetyki i kierowania ruchem lotniczym. Szczególny problem tworzy tu wspomniane zróżnicowanie obsługi tej trudnej sekundy. Podczas gdy stare wersje OS obsługują sekundę niebezpiecznie skokowo, nowsze najczęściej kompensują sekundę na wzór relatywistycznego zjawiska dylatacji czasu, tzn. rozciągając lub kurcząc czas mierzony we wnętrzu jądra OS. Wykonuje to się poprzez okresową redefinicję interwału jednej sekundy na poziomie liczników. W ten sposób zachowuje się ciągłość czasu w jądrze OS, podczas gdy użytkownik widzi na pulpicie ekranu scenariusz skokowy wstawiania sekundy jak pokazuje rysunek 6.

Rys. 6. Wprowadzenie sekundy przestępnej widziane na wyświetlaczach czasowych oraz na pulpicie ekranu komputera
Źródło: własne

Efekty uboczne rozbieżności czasowych jakie tworzą nowe generacje Windows/Unix/Linux wynikają z różnic podejścia w stosowanej technice „rozciągania” i „kurczenia” czasu. Niektóre systemy Linux rozpoczynają proces „wytracania” (lub adekwatnie „przyspieszania”) już na wiele godzin przed północą UTC, stosując

zaproponowaną w 2015 roku technikę Google Smear[16]. Z kolei Microsoft Windows ma podejście gwałtowne i wykonuje całą pracę w ciągu kilku minut przed i po północy UTC.

Mechanizm manipulacji dystrybucją harmonogramu zmian sekund przestępnych UTC nie został dotychczas dobrze opisany, ale eksperci polskiej ELPROMY wskazują na słabość systemu rozgłaszania oficjalnej informacji publikowanej w Bulletin-C[17] na stronach www.IERS.org. Dane podawane są z wielomiesięcznym wyprzedzeniem i jest wysoce prawdopodobne, że wiele systemów pobiera je w sposób zautomatyzowany, tak jak pokazuje rysunek 7. Zmiana tej informacji może skutkować wywołaniem skoku w czasie i rozsynchronizowaniem ważnych dla gospodarki infrastruktur krytycznych.



Rys. 7. Prawdopodobny scenariusz (dataflow) zautomatyzowanej dystrybucji zapowiedzi wprowadzenia sekundy przestępnej

Z danych tych korzysta część laboratoriów metrologii, w tym te odpowiedzialne za obsługę czasu dla naziemnej infrastruktury systemów satelitarnych. Zapowiedź sekund przestępnych jest też udostępniona przez IERS publicznie w formacie zgodnym z protokołem NTP (rysunek 8). Z danych IERS korzystają najczęściej serwery NTP/PTP bezpośrednio sprzężone z wzorcowymi zegarami atomowymi. Są to urządzenia jakie posiadają ośrodki metrologii dostarczające wzorce czasu do systemów satelitarnych oraz infrastruktury krytyczne, których praca musi pozostawać niezależna od satelitarnego systemu GNSS z powodów bezpieczeństwa. Integralność danych w pliku chroni jedynie funkcja HASH, co w przypadku skutecznego cyberataku na publiczne serwery IERS i podmianę przedmiotowego pliku, może wywołać trudne do przewidzenia sutki rozsynchronizowania w skali globalnej. Już sam fakt, wywołania zapowiedzi fałszywej sekundy przestępnej może wywołać nieprzewidziane testami symulacji zachowanie odbiorników GNSS. Dlatego ryzyko skutecznego ataku na serwery IERS stanowi dzisiaj ważny element ryzyka. Na przykład w przypadku naziemnej telewizji DVB-T/DVB-T2 utrata synchronizacji nadawczych masztów radowych BTS wywołuje ich automatyczne wyłączenie, co skutkuje wstrzymaniem emisji programu telewizyjnego w regionie.

Na koniec tego akapitu dodajmy, że dyskusja nad wzniesieniem sekundy przestępnej trwa od ponad dwudziestu lat i zawsze skutecznie blokowało je jedno państwo. Przeciwnymi wzniesienia są też przedstawiciele wszystkich trzech monoteistycznych religii świata, ponieważ religie to obok wspólnego Boga łączy fakt, że ważne dla nich święta odwołują się do historycznych wydarzeń i wyznaczane są w oparciu o obserwacyjny czas astronomiczny.

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

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

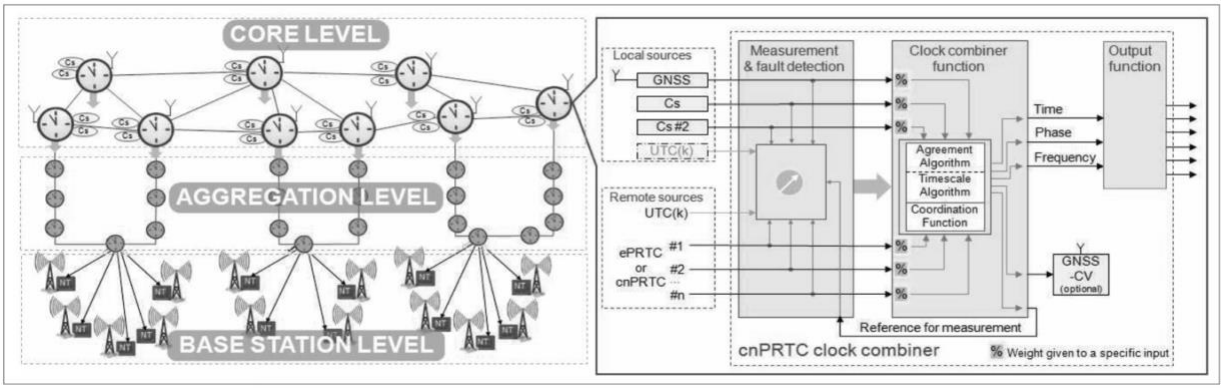
```
#
#       The following line shows the last update of this file in NTP timestamp:
#
#$      3882249427
#
#       2) Expiration date of the file given on a semi-annual basis: last June or last December
#
#       File expires on 28 December 2023
#
#       Expire date in NTP timestamp:
#
#@      3912710400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

Rys. 8. Informacja o sekundach przestępnych.

W ostatniej linii znajduje się wynik funkcji skrótu SHA zapewniający integralność danych w pliku. Brak uwierzytelnienia (podpisu kluczem publicznym infrastruktury PKI) pozwala na podmianę tego pliku i upublicznienie fałszywych danych zmian – zdarzenie, które z pewnością wywołałoby wiele awarii IT/OT na całym świecie.

Źródło: *strona IERS, https://hpiers.obspm.fr/iers/bul/bulc/ntp/leap-seconds.list*

W przypadku telekomunikacji, rozsynchronizowanie ma znaczenie zarówno dla stacji bazowych BTS jak i infrastruktury szkieletowej sieci LTE/5G. Z czasem wrażliwość telekomunikacji na rozsynchronizowanie będzie większa wraz z zakończeniem prac nad definicją standardu 6G, który będzie wymagać kontroli nad opóźnieniami, tzw. *low-latency networking,* a to z kolei wymusza bardzo dokładną synchronizację i monitorowanie wszystkich zegarów w sieci telekomunikacyjnej (rysunek 9).



Rys. 9. Model synchronizacji infrastruktury telekomunikacji 5G
Źródło: P. Krehlik, H. Imlau i inni *„Fiber-Based UTC Dissemination Supporting 5G Telecommunications Networks."*

Rola synchronizacji czasu jest bardzo ważna dla najnowszej inteligentnej dwukierunkowej energetyki smart-grid. Należy wprawdzie rozróżniać smart-grid od dotychczasowej jednokierunkowej klasycznej energetyki, ale z natury energetyka zawsze wiąże się z czasem i częstotliwością w każdym przypadku. Pozycje[18,19] wskazują realne zagrożenia atakiem Time Synchronization Attack (TSA). Teza taka znajduje potwierdzenie również w publikacjach branżowych[20], pracach naukowych[21] z obszaru cyber-bezpieczeństwa energetyki smart-grid. Podkreśla się, że w energetyce smart-grid nadrzędna rola obecnych elektrowni jest ograniczona. Prąd może wytwarzać wiele równoważnych sobie miejsc jednocześnie, w tym OZE, a ta sytuacja stwarza problem ustalenia zgodnej częstotliwości napięcia 50Hz. Zauważmy, że parametr częstotliwość zabezpiecza sieć energetyczną oddolnie podczas gdy odgórnie sieć zabezpieczana jest przed przeciążeniem i przepięciami. Rozsynchronizowanie smart-grid grozi poważnymi konsekwencjami,

[18] BrandsIT, „Czy przeszła energetyka będzie bezpieczna", https://brandsit.pl/czas-i-synchronizacja-czy-przyszla-energetyka-bedzie-bezpieczna/.

[19] BrandsIT, „Pilnie Potrzebujemy Smart-Grid", https://magazyn.brandsit.pl/pilnie-potrzebujemy-smart-grid-o-przyszlosci-polskiej-energetyki-rozmowa-z-tomaszem-widomskim-elproma/.

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

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

a nawet blackoutem. Na początku stycznia 2021 doszło w Europie do zagadkowego spadku[22] częstotliwości poniżej 50Hz na połączeniach sieci elektroenergetycznych, synchronizowanych ze sobą, w tym również w Polsce. Incydent nie spowodował awarii połączeń w Europie, ale wystawił je na bardzo poważną próbę. Odnotowane zostały jedynie przerwy dostaw energii na Bałkanach, a źródło awarii prowadziło do Rumunii, co o niczym nie przesądza. Problem pokazuje natomiast, że awaria energetyczna w jednym państwie może niebezpiecznie obniżyć częstotliwość i wywołać awarię w innym państwie, a za to odpowiadają Synchrofazory PMU (ang. Phaser Measurement Unit) wymagające stabilnej synchronizacji. W przypadku smart-grid PMU wymagają dokładności 1μs, podczas gdy w klasycznej energetyce jednokierunkowej wystarcza jedynie dokładność rzędu milisekund.

Reasumując, problem synchronizacji związany z obsługą sekundy przestępnej związany jest najczęściej z odbiornikiem GNSS używanym dziś popularnie do synchronizacji. Odpowiednia manipulacja sekundą (np. poprzez spoofing GNSS) stwarza realne zagrożenie dla nowoczesnych rozproszonych infrastruktur krytycznych i może wywołać efekt domina awarii powiązanych systemów. Opisane awarie odbiorników wskazują możliwość pojawienia się niewspółmiernie wysokich błędów czasu i skutki takich awarii są trudne do przewidzenia. Manipulacja sekundą przestępną UTC jest możliwa, ponieważ brakuje wyznaczonych standardów jej obsługi, która wymaga zaawansowanych technik płynnej korekcji czasu. Z kolei jej likwidacja jest przedmiotem prac ITU-R przy ONZ. Dotychczasowe uzgodnienia wskazują rok 2035 jako datę likwidacji poprzez zamrożenie. Według publikacji Nature[23] w listopadzie 2022 protest w sprawie złożyła Rosja.

4. Problem odbiorników GNSS – łatwa podatność na przepełnienia – błędy wewnętrzne GNSS

Chociaż *sekunda przestępna UTC* jest podstawowym ryzykiem, to nie jest jedynym. Odkąd w latach 90. pojawił się pierwszy komercyjny odbiornik GPS, wdrożono na globalnym rynku kilkaset milionów komercyjnych odbiorników satelitarnych GNSS używanych do dziś jako źródło odniesienia do skali UTC. Wszystkie one obliczają UTC ułamek sekundy inaczej, ze względu na różnice w wewnętrznych algorytmach i w zależności od używanej konstelacji GNSS. Dokładność wyznaczanego UTC zależy również od warunków pogodowych, jakości instalacji anteny, zakłóceń i wspomnianego wcześniej zagłuszania/fałszowania sygnałów satelitarnych GNSS.

Powszechnie przyjmuje się, że zasadniczym problemem amerykańskiego GPS i innych z grupy GNSS jest ich wojskowa natura. Z wyjątkiem europejskiego Galileo wszystkie pozostałe systemy nie mogą zapewnić źródła UTC w sytuacjach kryzysowych i mogą być użyte do manipulacji. Specjalną dyrektywę w tej sprawie wydał już

[22] Biznes Alert, „Bałkany mogły być przyczyną zagadkowego incydentu niestabilności", https://biznesalert.pl/energia-elektryczna-przesyl-energii-spadek-czestotliwosci-sieci-przesylowej-entso-e-pse-balkany-rumunia-energia-elektryczna-energetyka.

[23] Nature, https://www.nature.com/articles/d41586-022-03783-5.

w 2004 roku prezydent USA G.W. Bush[24]. Ale dopiero cytowana w tym artykule dyrektywa prezydenta USA Donalda Trumpa o numerze EO13905 zaczyna zmieniać podejście rynku. Rekomenduje ona uniezależnienie się amerykańskich infrastruktur rozproszonych od rodzimego GPS. Istnieją też inne stosowne dyrektywy rządowe zezwalające na ograniczanie sygnałów satelitarnych bez uprzedzenia opinii publicznej. Zdarzają się też zwykłe awarie tych systemów, błędy transmisji telemetrii Ziemia–kosmos jak np. ta znana jako SVN23[25] [26] wprowadzająca błąd 13.5μs do systemu GPS w dniu 26 stycznia 2016 roku (rysunek 10).

Efekt błędu ilustruje rysunek 10, na którym widać rozbieżność 13.5μs między pięcioma różnymi urządzeniami synchronizacyjnymi (w tym serwerami NTP/PTP IEEE1588), różnych producentów, synchronizowanych względem tego samego systemu GPS. Urządzenia reagują o różnych porach, niepokrywających się, ponieważ ich odbiorniki różnią się algorytmami liczącymi UTC. Widoczną bezwładność (zróżnicowanie reakcji urządzeń), należy tłumaczyć zróżnicowaniem obsługi awaryjnej pracy z oscylatora holdover. Wszystkie one wykażą rozbieżność UTC względem liniowej (bez skoku) charakterystyki innych urządzeń, które w trakcie awarii używały inne niż GPS podsystemy np. GALILEO, GLONASS, BEIDOU lub IRNSS.

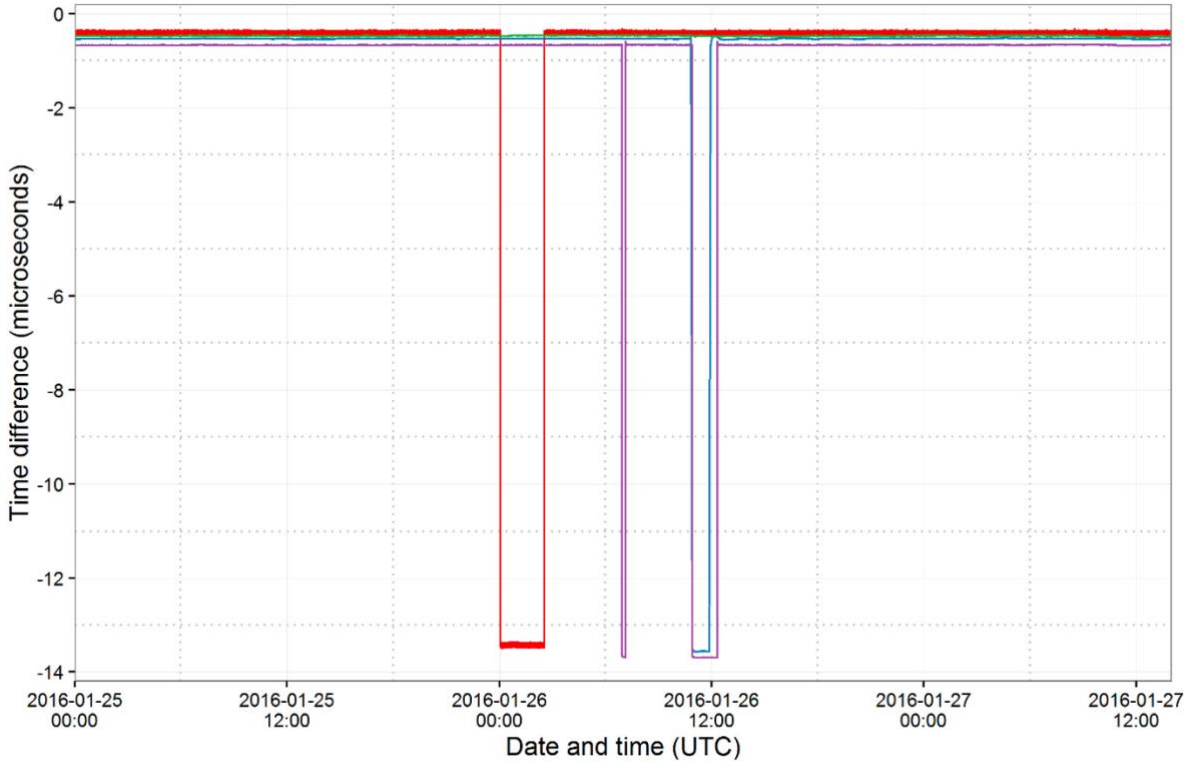
WAŻNY WNIOSEK

Z powyższych przyczyn do synchronizacji IT i OT infrastruktury krytycznej, należy używać rozwiązań sprzętowych synchronizacji pochodzących od jednego sprawdzonego, zaufanego producenta. Powinien to być dostawca krajowy, zweryfikowany przez krajową metrologię (Główny Urząd Miar RP). Urządzenia powinny być skonfigurowane tak aby używały pojedynczy system satelitarny, a ich odbiorniki powinny uwzględniać nawet zgodność wersji oprogramowania systemowego (frimware). Serwery powinny być skonfigurowane zapewniając konwergencję synchronizacji do urzędowych wzorców Głównego Urzędu Miar RP, a w przypadku braku dostępu do wzorca krajowego UTC(PL) synchronizacja powinna się odbywać do GALILEO przy wsparciu amerykańskiego GPS. Nie należy korzystać, GLONASS ani z BEIDOU. Wszystkie serwery czasu NTP/PTP używane do synchronizacji powinny być ponadto wyposażone w we własny oscylator holdower. Najlepiej, jeżeli będzie to oscylator Rubidowy i OCXO.

[24] G.W Bush, dyrektywa 2004, https://insidegnss.com/wp-content/uploads/2018/01/novdec08-coverstory.pdf.

[25] The effects of the January 2016 UTC offset anomaly on GPS-controlled clocks monitored at NIST, https://tf.nist.gov/general/pdf/2886.pdf.

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



Rys. 10. Rozbieżności czasu 13.5µs systemu GPS w dniu 26.01.2016 r.
Źródło: ISBN 978-952-60-6703-2 (pdf)

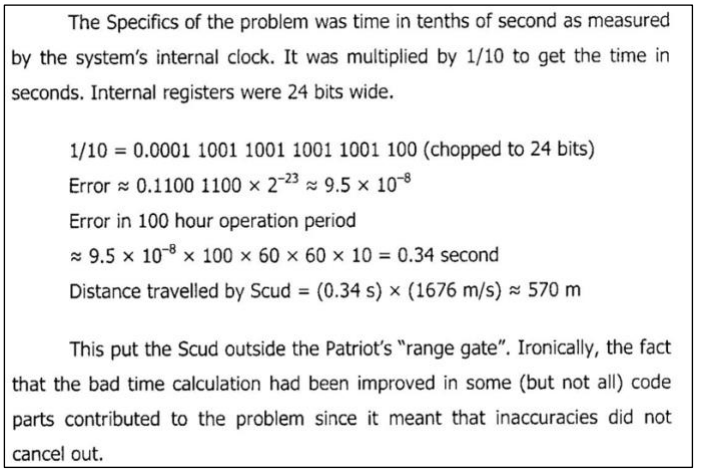
W przypadku Polski powinien to być europejski system GALILEO wspierany pracą amerykańskiego GPS, jednak ze względu na możliwość wprowadzania ograniczeń emisji sygnału wojskowego sygnału GPS (dyrektywa G.W. Bush – 2004, dyrektywa D. Trump EO13905 – 2020) ważne jest wspieranie synchronizacji dystrybucją czasu z Głównego Urzędu Miar RP (projekt eCzasPL[27]). Używane do synchronizacji odbiorniki satelitarne powinny mieć zgodność sprzętową, w tym zgodną wersje firmware. Rekomendowana jest też zgodność obsługi awaryjnego trybu działania bez GNSS, tzw. synchronizacji holdover, a więc pracy z wewnętrznych oscylatorów kwarcowych OCXO, Rubidowych i cezowych Cs.

Największy problem utrzymania zgodności synchronizacji na dużym obszarze kraju stanowią komercyjne odbiorniki GNSS. Są one najczęściej wbudowane w urządzenia takie jak serwery czasu NTP/PTP. Okazuje się, że w synchronizacji opartej na GNSS błąd jednego roku jest tak samo prawdopodobny jak skok o jedną milisekundę. Dzieje się tak, ponieważ czas wewnątrz odbiornika GNSS reprezentowany jest numerycznie i podlega procesowi przetwarzania, wykazując znaczną podatność na błędy przepełnień. Ma to miejsce, zwłaszcza gdy producent „upchnie" w jednym bajcie obok czasu również datę. Łatwo w takim przypadku przenieść bit przepełnienia milisekundy na pole kodujące datę co skutkuje dużymi skokami w czasie. Przymusowa kompresja danych związana jest z optymalizacją rozwiązania, które musi być małe gabarytem i oszczędne energetycznie.

[27] eCzasPL GUM, https://www.gum.gov.pl/pl/projekty-eu/e-czaspl/3632,e-CzasPL.html.

Sam odbiornik GNSS ma sporo do policzenia i ma sporo okazji do popełniania błędów. Błędnie często domniemajmy, że czas i pozycja wysyłane są do nas z kosmosu. Czas i pozycja wyznaczane są tu na Ziemi w odbiorniku GNSS. Każdy odbiornik robi to inaczej, ale każdy musi uwzględniać poprawkę wynikającą ze szczególnej teorii względności Einsteina, która wynosi 7μs/24h, co wiąże się z prędkością 14 tys. km/h z jaką poruszają się satelity np. GPS po średnich orbitach względem Ziemi. Druga ważna poprawka to 42μs/24h wynikająca z ogólnej teorii względności Einsteina i wpływu grawitacji na zjawisko dylatacji czasu. Na Ziemi czas płynie wolniej niż w kosmosie. Obie wielkości są przeciwstawne znakiem wiec dzienna korekta czasu, jaką odbiorniku dla systemu GPS musi policzyć po odebraniu telemetrii z satelitów to aż 35μs/dobę. To bardzo dużo, zważywszy, że np. współczesna telekomunikacja 5G dopuszcza maks. błąd 10ns, a od źródeł dla smart-grid wymaga się dokładności sieci Ethernet poniżej 1μs (200ns dla źródła jak serwery czasu NTP/PTP wg normy IEEE C37.238). Wszystko to zwiększa jeszcze podatność odbiornika GNSS na przepełnienia numeryczne.

Najbardziej znanym skutkiem błędu przepełnienia rejestru zegara jest awaria systemu baterii rakiet Patriot, który zawiódł podczas pierwszej wojny w Zatoce Perskiej w 1991 roku. Z powodu niedokładnych obliczeń pozycji bateria rakiet Patriot w Dhahran, w Arabii Saudyjskiej, nie zdołała przechwycić nadlatującego irackiego pocisku SCUD, który uderzył w koszary zabijając 28 osób. Zgodnie z raportem GAO/IMTEC-92-26[28,29] błąd związany był z czasem zegara zapisanym w 24-bitowym rejestrze systemowym, w którym pojawił się błąd zaokrąglenia (rysunek 11).



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

1/10 = 0.0001 1001 1001 1001 1001 100 (chopped to 24 bits)
Error ≈ $0.1100\ 1100 \times 2^{-23} \approx 9.5 \times 10^{-8}$
Error in 100 hour operation period
$\approx 9.5 \times 10^{-8} \times 100 \times 60 \times 60 \times 10 = 0.34$ second
Distance travelled by Scud = (0.34 s) × (1676 m/s) ≈ 570 m

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

Rys. 11. Wyjaśnienie błędu zegara baterii rakiet Patriot z Dhahran w Arabii Saudyjskiej w 1991 roku

[28] Raport awarii systemu rakiet Patriot GAO/IMTEC-92-26, https://www.gao.gov/assets/imtec-92-26.pdf.

[29] Link US GAO dotyczący raportu awarii systemu rakiet Patriot, https://www.gao.gov/products/imtec-92-26.

5. Chipy GNSS, które nie działają zgodnie z deklaracją producenta

Globalizacja doprowadziła do rozproszenia światowej produkcji elektroniki. Poszukując optymalizacji kosztów produkcji, wielu renomowanych producentów układów scalonych i odbiorników GNSS przeniosło swoją produkcję do Chin, z których dziś w pośpiechu powraca z produkcją do swoich macierzystych krajów. Wielu producentów oparło też swoje projekty na obcym kapitale intelektualnym inżynierii Indii, Chin i Rosji, gdzie dostęp do taniej, bardzo dobrze wykształconej kadry inżynierskiej, przeważał w procesach podejmowania decyzji przez menadżerów i inwestorów.

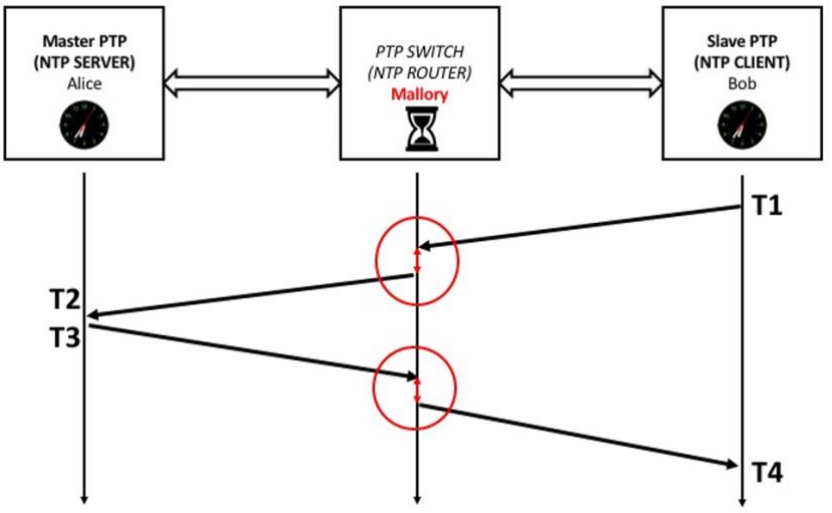
Również wielu producentów odbiorników GNSS, w tym szczególnie firmy z Rosji chcąc wyrównać swoje komercyjne szanse z zaufanym i bogatym biznesem zachodu, utworzyło celowe spółki zagraniczne utrudniając identyfikację pochodzenia i know-how wytwarzanego produktu. Zachęcani niską ceną i bardzo dobrą jakością, producenci, między innymi serwerów czasu, stosowali latami układy rosyjskie w swoich urządzeniach. Dziś nadal bez trudu odnaleźć można w produktach jednego z bardzo renomowanych niemieckich producentów serwerów czasu podzespoły zarówno rosyjskich oscylatorów OCXO jak i rosyjskie odbiorniki GNSS. Jak wiele firm branży, Niemcy mimo wstrzymania eksportu do Rosji i na Białoruś, nie wstrzymali importu i używania rosyjskich komponentów, mimo że problem występujących ryzyk został wskazany przez liczne międzynarodowe laboratoria USA, Japonii oraz został potwierdzony przez polską firmę Elproma, która do wybuchu wojny w Ukrainie w roku 2022, podobnie jak Niemcy używała rosyjskich komponentów, zamieniając je obecnie, w wyniku uwzględnienia występujących ryzyk, na amerykańskie i japońskie.

Rys. 12. Rosyjski odbiornik NVS ANAI 469635.002 oparty na systemie GLONASS jako wiodącym oraz jego wewnętrzny chipset NV08C-CSM sprzedawany komercyjnie pod szyldem szwajcarskiej firmy NVS i eksportowany globalnie

Podpisana w 2020 roku dyrektywa prezydenta USA EO13905 była najprawdopodobniej spowodowana niemożliwością identyfikacji i wycofania z rynku urządzeń, opartych o rosyjskie i chińskie odbiorniki GNSS oraz oscylatory kwarcowe OCXO holdover, chipy jakie wyprodukowano w minionej dekadzie w ilościach milionów sztuk i wdrożono do licznych systemów IT infrastruktur krytycznych. W tym samym czasie, gdy firmy amerykańskie rozwijały swoje produkty dbając o obsługę możliwie jak największej liczby dostępnych konstelacji GNSS, przemysł rosyjski dbał, aby wyizolować z lokalnego rynku rosyjskiego układy zależne od amerykańskiego systemu GPS. Rosyjski przemysł pozostawał tym samym zależny wyłącznie od systemu naziemnego „Czajka" wspierany pracą satelitarnego systemu GLONASS. Pojawiły się rekomendacje nazw producentów jakie infrastruktury krytyczne mogą używać w Rosji i wyprzedziły one amerykańską dyrektywę EO13905 o wiele lat. Takim rekomendowanym na rynku wewnętrznym w Rosji producentem jest firma NVS, posiadająca rejestrację zarówno w Szwajcarii jak i w Rosji. Generowany przez odbiorniki tej firmy czas UTC wykazuje cechy silnej koherencji względem skali czasu systemu satelitarnego GLONASS, nawet po programowym wyłączeniu GLONASS i pozostawieniu samego GPS (rysunek 12). Mimo widniejącej na etykiecie nazwy GALILEO układ NV-08 nie obsługuje europejskiego systemu satelitarnego.

6. TDA Atak na opóźnienie – karty i urządzenia sieciowe

Wydawać by się mogło, że skoro urządzenie sieciowe pracuje wewnątrz dobrze strzeżonej sieci wewnętrznej, to nie może być skutecznym narzędziem w rękach cyberprzestępców. Nic bardziej mylnego. Rysunek 13 ilustruje działanie ataku na opóźnienie wewnątrz sieci Ethernet. Sieciowe urządzenie pośredniczące, takie jak przełączniki i routery Ethernet mogą wprowadzać losowe zmienne opóźnienie. Zaburza ono proces synchronizacji między klientem a serwerem protokołów NTP i PTP (IEEE1588) w miejscach zaznaczonych kolorem czerwonym na rysunku.

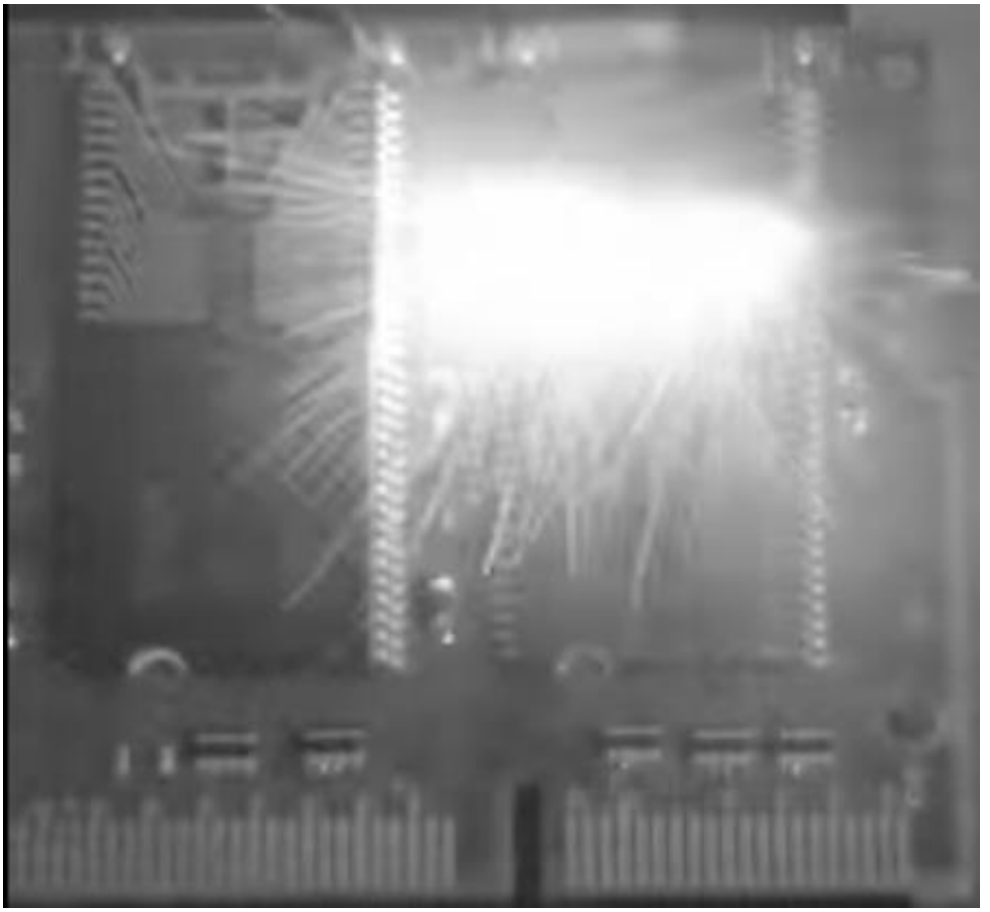


Rys. 13. Ilustracja tzw. round-trip pakietu synchronizacyjnego
(ta sama zasada dotyczy też synchronicznego rozgłaszania IEEE1588)

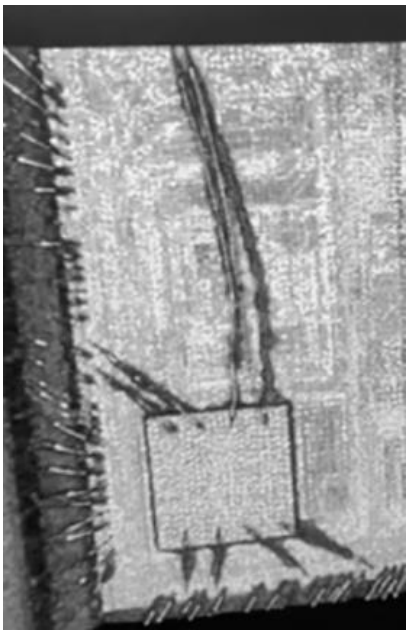
Źródło: prezentacje firmy Elproma www.elpromaelectronics.com
podczas konferencji TA/PL/ Głównego Urzędu Miar RP

Atak na opóźnienie TDA w sieci możliwy jest najczęściej dzięki podrzuconym „intruzom" dodawanym do urządzeń w trakcie produkcji układów scalonych (rysunek14a i rysunek 14b) lub montażu obwodów drukowanych PCB (rysunek 15). Intruz w postaci dodatkowego układu może być ulokowany wewnątrz prawidłowego układu scalonego (rysunek 14a) jak i dodany ręcznie do PCB karty sieciowej (rysunek 15).

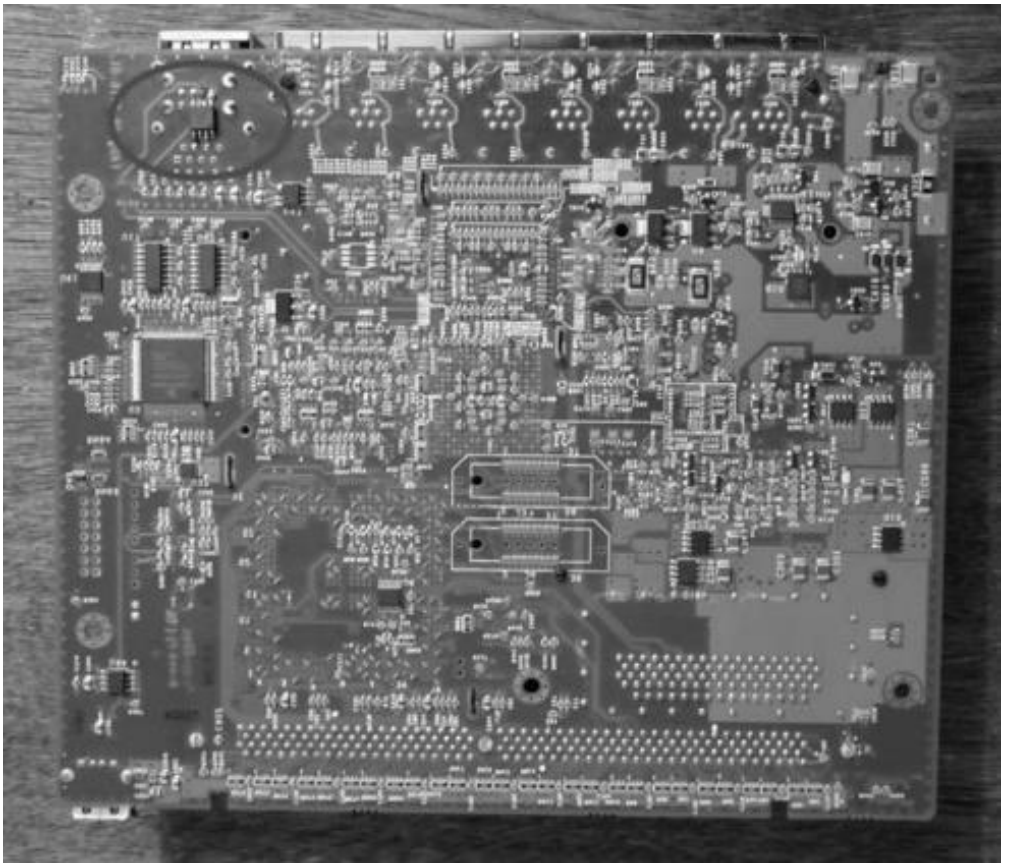
Identyfikacja intruzów biorących udział w TDA odbywa się na skutek obserwacji anomalii procesu synchronizacji takich jak nieoczekiwane nadmiarowe asymetrie łącza wewnętrznego, nadmiarowe szumy synchronizacji, zmienne opóźnienia obserwowane w ustabilizowanych termicznie warunkach pracy. W takim przypadku niezbędne jest znalezienie przyczyny, co w inspekcji wzrokowej wymaga często laserowego otwarcia i obejrzenia w mikroskopowym powiększeniu układu scalonego (rysunek 14b). Analizę taką mogą wykonywać specjalistyczne ośrodki diagnostyki Cyberbezpieczeństwa, jednak najczęściej układy bada producent urządzeń.



Rys.14a. Efekt otwierania chipa za pomocą lasera w celu inspekcji wnętrza. Tak poszukuje się „podrzucone" podukłady, które w przypadki synchronizacji wprowadzają szum i losowe opóźnienia.



Rys. 14b. Widoczny po otwarciu laserem chip „Intruz" generujący szum i losowe opóźnienie transmisji w specjalnej wersji kart sieciowych używanych do synchronizacji w rozproszonej infrastrukturze chmury.



Rys.15. Efekt umieszczenia chipa „intruza" w obwodzie drukowanym – widoczny po lewej stronie w owalu chip „Intruz" dodany do PCB [30]

[30] Źródło: Monta Elsins SANS Institute.

7. Spoofing czasu UTC przez Internet – Projekt NTPPOOL.ORG

Atak spoofingiem na system synchronizacji obejmuje swoim zasięgiem nawet systemy IT nieużywające odbiorników GNSS. Zagrożenie to obejmuje dużą liczbą urządzeń sieciowych opartych na oprogramowaniu Open Source, w tym na systemach rodziny Linux. System operacyjny Linux używany jest zarówno do organizacji platform serwerowych IT jak stanowi większość oprogramowania systemowego firmware, na którym opierają się urządzenia IoT i routery sieciowe. Standardowym referencyjnym źródłem czasu UTC dla systemów rodziny Linux/Unix jest grupa publicznych serwerów NTP zgromadzona w projekcie NTPPOOL[31].

Tab. 2. Lokalizacja serwerów NTP

Active Servers

Africa	87
Asia	349
Europe	3042
North America	1023
Oceania	154
South America	71
Global	4458
All Pool Servers	4704

As of 2023-05-21

Projekt NTPPOOL zgromadził w ciągu kilkunastu lat ponad 4.5 tysiąca serwerów NTP rozproszonych po całym świecie (tabela 2). Są to serwery publiczne. Ich używanie jest nieodpłatne. Należą one do firm, organizacji, do rządów państw i osób prywatnych. Są wśród nich publiczne serwery wysokiej jakości jakie udostępnia NIST w USA, NPL w Wielkiej Brytanii, PTB w Niemczech, a w Polsce Główny Urząd Miar RP. Jednak większość zgromadzonych w NTPPOOL serwerów NTP jest miernej jakości i ich pochodzenie oraz konfiguracja źródeł UTC pozostają nieznane. Każdy właściciel serwera NTP, który posiada statyczny publiczny adres IPv4 może zgłosić swój serwer do projektu NTPPOOL i udostępnić swój serwer. Wśród 4.5 tyś serwerów znajdują również te oparte na zwykłych laptopach, na komputerach Raspberry Pi, Arduino itp. Niektóre, mają ewidentnie czas ustawiany przypadkowo. System NTPPOOL bada routing ustalając automatycznie lokalizacje serwera i przypisuje automatycznie do grup kontynentalnych i narodowych. Serwery NTP, których fizyczny publiczny adres IPv4 zostanie skojarzony z urządzeniami pracującymi w Polsce zostaną zaliczone do grupy domeny europejskiej

[31] www.ntppool.org

`europe.pool.ntp.org` i polskiej `pl.pool.ntp.org`. System NTPPOOL nie rozróżnia serwerów fizycznych NTP od serwerów programowych uruchomionych w środowisku wirtualnym VM.

Fizyczny przydział serwera NTPPOOL odbywa się automatycznie na zasadzie zbliżonej do obsługi nazw symbolicznych DNS. Użytkownicy Linux/Unix/Windows nie mają tu żadnego wpływu na wybór serwera NTP z puli dostępnych NTPPOOL, ponieważ plik konfiguracyjny ntp.conf zawiera jedynie ogólną symboliczną nazwę, pod którą system podstawia losowo najbliżej położony geograficznie serwer z dostępnej puli: tabela 3 i tabela 4.

Tab. 3 Przykładowa zawartość pliku *ntp.conf* w przypadku serwerów europejskich (max 4 linie)

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

Tab. 4 Przykładowa zawartość pliku *ntp.conf* w przypadku serwerów z lokalizacją w Polsce

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

Proces przydziału i wywłaszczanie publicznego serwera NTP z komputera Linux odbywa się bez wiedzy właściciela. Mimo, że NTPPOOL monitoruje zdalnie dokładności posiadanych serwerów NTP względem skali UTC, to robi to bardzo rzadko i nie może w porę zablokować ataku TAS. Szczególny niepokój budzą raporty opisujące udział w NTPPOOL serwerów NTP pracujących w DARKNET ponieważ serwery takie mogą w sposób utajniony podstawiać fałszywy czas i zmieniać ustawienia lokalnego zegara w serwerze lub routerze.

Opisane zjawisko, to sieciowy substytut spoofingu GNSS wykonywany z poziomu sieci Internet. Serwery DARKENT uzyskują poprzez NTPPOOL i protokół NTP styczność z synchronizowanym PC/serwerem bez wiedzy jego właściciela. Jeżeli w Polskiej puli publicznych serwerów NTP zostanie podstawione 6-8 fałszywych serwerów, to prawdopodobieństwo kontaktu wynosi 10%, ponieważ łączna liczba publicznych serwerów w Polsce waha się w przedziale od 60 do 80. Podejście takie chociaż wydaje się mało skuteczne, to zważywszy na niejawne funkcje NTPPOOL automatycznej zmian serwerów daje w skali długoterminowej instrument skutecznego ataku. Zdalny serwer NTP hakera potrafi zidentyfikować fizycznie zasoby klienta NTP. Znając luki bezpieczeństwa systemu operacyjnego Linux i firmwaru opartego na tym systemie, haker może wykorzystać to do bezpośredniego ataku. Styczność maszyny hakera (serwer NTP) i użytkownika (klient NTP) stwarza duże ryzyko skutecznych ataków DDoS.

Do najgroźniejszych i zarazem najtrudniej wykrywanych ataków należą te oparte na wprowadzaniu do NTP fałszywej zapowiedzi tzw. sekundy przestępnej UTC[32] (ang. Leap Second[33]). Mogą one wywołać powstanie rozbieżności 1 sekundy. W latach 2021-2023 delegacja KPRM do ITU (obraduje przy ONZ w Genewie) wprowadziła pierwszą w 100 letniej historii kontrybucję Polski. Praca Polaków została opisana[34] w ITU-News[35] 02/2023.

Grupa polska NTPPOOL zawiera zmienną ilość w przedziale 60-80 serwerów NTP, co stanowi jedynie 1.5% puli europejskiej zawierającej ponad 2700 serwerów.[36] W roku 2023 osiągnęła ona poziom 100 i utrzymuje się w roku 2024, co stanowi 100% wzrost. Pozostaje niejasnym komu zawdzięczamy taki wzrost w tak krótkim czasie, i czy aby nie jest to działanie ofensywne obcego państwa podrzucające nam zmanipulowane serwery.

Światowym liderem jest USA posiadające blisko 1000 serwerów publicznych NTP. Za nimi klasyfikują się: Niemcy (rząd wielkości) 900 serwerów, Francja 300, Wielka Brytania 300, Holandia 230. Polska nadal posiada niebezpiecznie niską liczbę serwerów publicznych PL.POOL.NTP.ORG w porównaniu do wymienionych państw. Tak małą liczbę 60-100 polskich publicznych serwerów NTP łatwo jest statystycznie zaburzyć podstawiając tylko 6-10 wrogich serwerów destabilizujących czas UTC co stanowi 10% krajowej populacji serwerów i nadal pozostaje nie jasnym, czy 100% wzrost polskiej puli w 2023 r. nie jest wrogim działaniem podstawiającym do Polski zmanipulowane serwery.

Dla zmniejszenia w/w ryzyka celowe jest zatem statystyczne działanie, zwiększające liczbę polskich serwerów publicznych NTP do min. 400szt. (rekomendowane jest 800szt. serwerów publicznych NTP w Polsce - na wzór Niemiec). Polskie serwery powinny być włączone do projektu eCzasPL i synchronizowane do czasu urzędowego UTC(PL) wzorców jakie utrzymuje Główny Urząd Miar RP. Zwiększenie puli ma na celu zapewnić statystyczną neutralizację potencjalnej możliwości wpływu „wrogich" podstawionych publicznych serwerów NTP ukrywających się w krajowej i europejskiej puli *pl.pool.ntp.org* (POOLNTP). Tym samym stanowi to jedyne i zarazem bezpośrednie wzmocnienie polskiej publicznej strefy synchronizacji NTP Linux, która dostarczy do NTPPOOL sygnał czasu urzędowego zgodny z rozporządzeniem Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 19 marca 2004 r. w sprawie sposobów rozpowszechniania sygnałów czasu urzędowego i uniwersalnego czasu koordynowanego UTC(PL) (Dz. U. Nr 56, poz. 548), co realizuje projekt eCzasPL[37]. Firma Elproma opracowała techniczne rozwiązanie w ramach PWCyber. Jak wynika z nieoficjalnych informacji w ostatnim czasie kraje UE, np. Niemcy dokonały już podobnego zwiększenia puli serwerów NTP, o czym świadczy liczba aż 900 serwerów.

[32] Coordinated Universal Time https://en.wikipedia.org/wiki/Coordinated_Universal_Time
[33] Sekunda przestępna - UTC Leap Second https://en.wikipedia.org/wiki/Leap_second
[34] Blokada sekund przestępnych. Streszczenie Polskiej kontrybucji do ITU-R grupa WP-7A (str. 28). https://www.itu.int/en/itunews/Documents/2023/2023-02/2023_ITUNews02-en.pdf
[35] ITU-News 02/2023 "The future of UTC" https://www.itu.int/en/itunews/Pages/default.aspx
[36] https://www.ntppool.org/zone/europe).
[37] Projekt eCzasPL Głównego Urzędu Miar RP - system dystrybucji czasu urzędowego UTC(PL) https://www.gum.gov.pl/pl/projekty-eu/e-czaspl/3632,e-CzasPL.html

8. Zestawienie – 5 grup ryzyka destabilizacji systemów IT teleinformatycznych z wykorzystaniem ataku TAS na system synchronizacji czasu, lub błędy synchronizacji czasu

1. **Ziemia.** Proces wytwarzania czasu – Laboratoria metrologii czasu i segment naziemny GNSS:
   a) **Możliwość manipulacji danymi Biuletynu-C IERS** zmiany liczby sekund przestępnych skali UTC;
   b) **Nieciągłość skali UTC** i wielosekundowa rozbieżność czasu między wewnętrznymi skalami satelitarnymi GPST, GALILEOT, GLONASST, BEIDOUT, IRNSST (suffix „T" za nazwą konstelacji oznacza skalę czasu danego systemu satelitarnego rodziny GNSS);
   c) **Błędy proceduralne obsługi aktualizacji satelitów GNSS** – np. utrata łączności GALILEO z 2019[38].

2. **Ziemia-kosmos.** System satelitarny - Transfer telemetrii czasu do systemu satelitarnego GNSS:
   a) **błędy danych telemetrii przesyłanej do satelitów GNSS** – np. problem SVN#23 26/01/2016r[39] . Nawet chwilowy błąd w jednym systemie implikuje duży skok czasu w systemie teleinformatycznym zależnym od innych systemów dystrybucji czasu.

3. **Kosmos-Ziemia**, odbiór danych z satelitów GNSS przez odbiorniki w urządzeniach takich jak zegary GrandMaster i serwery czasu NTP i PTP IEEE1588:
   a) **luki bezpieczeństwa** w układach odbiorczych GNSS, niebezpieczne w szczególności są backdoor;
   b) **błędy przepełnień** w odbiorniku np. GPS WNRO 7/04/2019, do dziś tworzy skoki czasu o 19.7 lat;
   c) **zagłuszanie sygnałów** satelitarnych (ang. GNSS Jamming) – zaliczane do „Atak na czas"
   d) **symulacja naziemna** sygnałów (ang. *GNSS Spoofing*) – określane jako „Atak na czas";
   e) **przechwytywanie i opóźnianie** (ang. GNSS Meaconing) – określane jako „Atak na opóźnienie";
   f) **brak lub sztuczne dodanie/odjęcie obsługi sekundy przestępnej** (ang. *UTC Leap Second*);
   g) **niepewność synchronizacji względem wewnętrznych skal czasu** GPS(T), GALLEO(T), GLONASS(T), BEIDOU(T), IRNSS(T)
   h) **nieprawidłowa zapowiedź lub brak zapowiedzi sekundy przestpnej**

[38] https://focalpointpositioning.com/insights/that-time-galileo-was-stuck-in-the-past.
[39] https://tf.nist.gov/general/pdf/2886.pdf; https://www.bbc.com/news/technology-35491962.

4. **Transfer siecią komputerową t i Internetem** (protokoły NTP i PTP IEEE1588):
   a) **brak zapowiedzi i obsługi sekundy przestępnej** (Leap Second), wywołuje skoki sekundowe i minutowe;
   b) **wpływ asymetrii łącz** na dokładność synchronizacji, szumy wywołane tzw. random traffic i DDoS;
   c) **celowe wprowadzanie opóźnień** z poziomu urządzeń sieciowych (TAD – ang. *Time Delay Attack*);
   d) **niestosowanie uwierzytelnień wzorca i brak zdalnego audytu czasu** (serwery DARKNET w NTPPOOL). Fałszowanie nieuwierzytelnionych źródeł NTP i PTP, brak audytu strony klienta czy ustawił czasu.
   e) **błędy mylenia skali czasu UTC z atomową skalą TAI oraz z czasem lokalnym**;
   f) **wpływ asymetrii łącz** na dokładność synchronizacji.

5. Urządzenia klienckie końcowe (ang. Submaster NTP/PTP – wcześniej nazywany zegarem Slave), aplikacje, w tym również same serwery czasu NTP/PTP mające obok trybu Grandmaster również w/w funkcje Submaster i konwersji standardów:
   a) **wpływ ruchu** (random traffic, ataki DDoS) na proces synchronizacji po stronie klienta NTP i PTP;
   b) **problem kompatybilności wersji rewizyjnych protokołów NTP i PTP**, wywołuje nieplanowane rozbieżności;
   c) **zróżnicowanie obsługi sekundy przestępnej (ang. leap-second)** generuje błędy wielosekundowe. Manipulując flagą zapowiedzi sekundy przestępnej można wywoływać przepełnienia numeryczne firmwaru odbiorników GNSS jak i kart sieciowych co prowadzi do rozsynchronizowania liczonego nawet w latach!
   d) **błędy ludzkie** (ustawień konfiguracji, mylenie UTC z TAI vs. Czas lokalny);
   e) **błędy reprezentacji skal czasu** - reprezentacja: UTC vs. TAI, skale POSIX, problem GPSd itp., ale również rozbieżności struktur danych. Na przykład system satelitarny BEIDOU numeruje dni tygodnia w przedziale 0-6 podczas gdy pozostałe systemy numerują 1-7. Przełączenie systemu w układzie scalonym podczas obliczeń może wywołać błąd 1 dnia. Przełączanie firmwaru między systemami ma miejsce najczęściej przy słabej jakości odbieranych sygnałów satelitarnych. W związku z tym do dobrych zwyczajów realizacji systemów należy skonfigurowanie odbiorników tak aby odbierały tylko jeden system satelitarny, co z pozoru wydaje się sprzecznym z logiką i zasadą *„im więcej tym lepiej”*.
   f) **Niechlujnie wykonane instalacje anten GNSS dachach** wywołują interferencje między antenami, skupione w grupie ułatwiają atak i zwiększają jego skuteczność.

Wielkości błędu (skok) w czasie mogą być różne w zależności od przyczyny i może się to wahać w przedziale od nanosekund, aż po całe sekundy, a nawet dni i lata. Dobrze ilustruje to problem wyzerowania licznika dni tygodni tzw. GPS WNRO jaki trwa od dnia 07.04.2019 i w zależności od użytego sprzętu, oraz wersji firmwaru objawia się losowo, wprowadzając błąd max. do 19.7 lat.

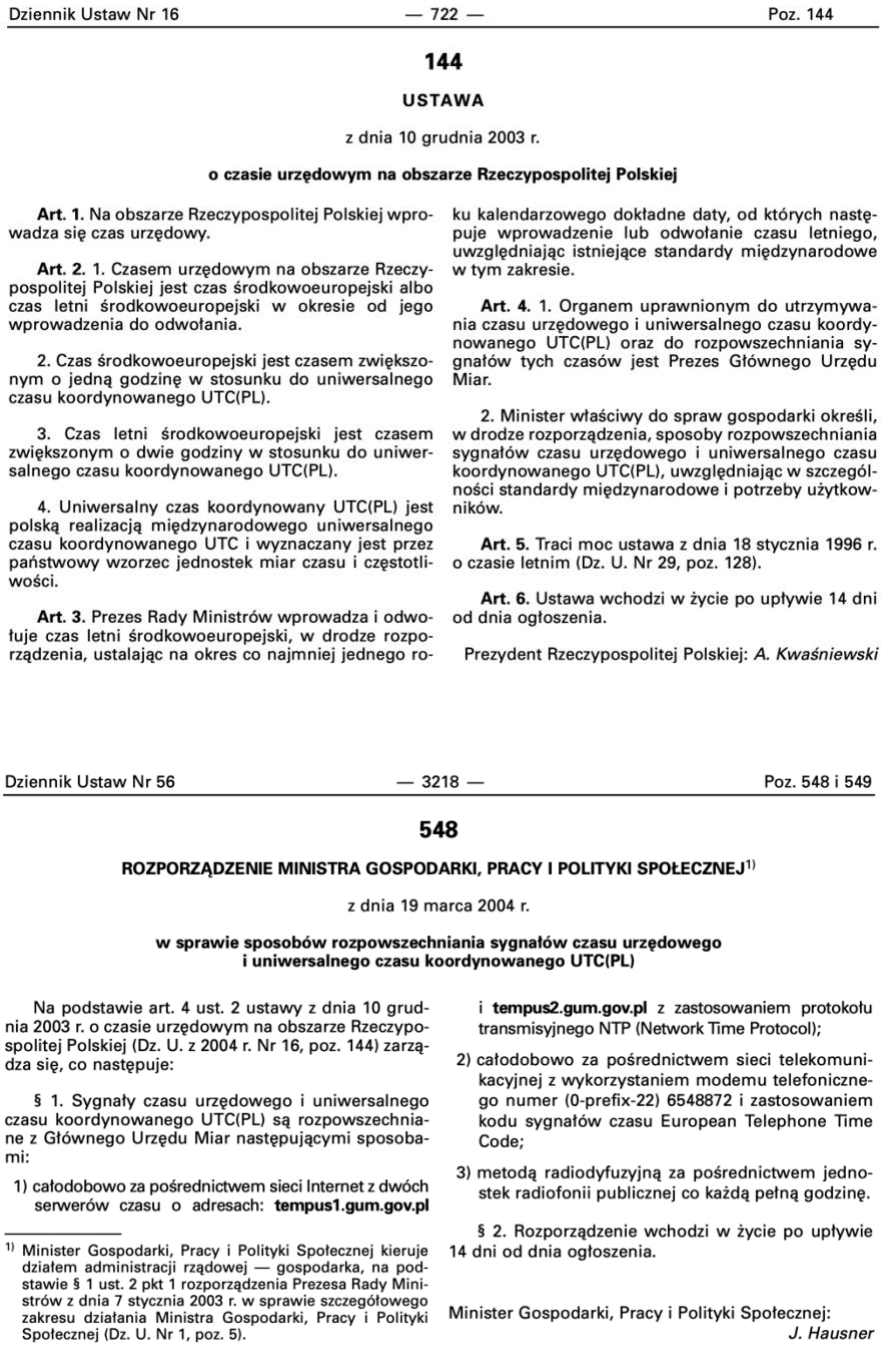
Rys. 16. Widok dachu zakładu przemysłowego na przełomie drugiej i trzeciej dekady XXI wieku. Ilość anten odzwierciedla charakterystyczny dla Przemysłu 3.0 proces relacji jeden PC steruje jedną linią produkcyjną (lata 1980-2020). Zbyt blisko położone anteny GNNS interferują i są łatwym celem ataku TAS. Duża liczba zróżnicowanych odbiorników zwiększa ryzyko przepełnień

Rys. 17. (Źródło: własne) Błąd wyzerowania licznika dni tygodni GPS z 2019

Rys. 18. (Źródło: własne) Błąd wyzerowania licznika dni tygodni GPS z 2019 - skok o 19.7 lat. (górny rysunek) w żyroskopie samolotów Boeing; dolny rysunek w systemach fiskalnych w Pradze.

9. Wnioski i krajowe rekomendacje budowy systemów czasu do bezpiecznej synchronizacji UTC(PL) odpornej na wady GNSS

Polska znacznie wcześniej od USA i Wielkiej Brytanii zwróciła uwagę na znaczenie oficjalnych krajowych wzorców czasu. Krajowym odpowiednikiem NIST (USA) i NPL (UK) jest Główny Urząd Miar RP (PL). Oficjalny polski czas definiuje ustawa o czasie urzędowym z 10.12.2003 r Dz.U. Nr 16, a metody dystrybucji określono w Dz.U. Nr 56 z 2004, poz. 548 (rysunek 19).



Dziennik Ustaw Nr 16 — 722 — Poz. 144

144

USTAWA

z dnia 10 grudnia 2003 r.

o czasie urzędowym na obszarze Rzeczypospolitej Polskiej

Art. 1. Na obszarze Rzeczypospolitej Polskiej wprowadza się czas urzędowy.

Art. 2. 1. Czasem urzędowym na obszarze Rzeczypospolitej Polskiej jest czas środkowoeuropejski albo czas letni środkowoeuropejski w okresie od jego wprowadzenia do odwołania.

2. Czas środkowoeuropejski jest czasem zwiększonym o jedną godzinę w stosunku do uniwersalnego czasu koordynowanego UTC(PL).

3. Czas letni środkowoeuropejski jest czasem zwiększonym o dwie godziny w stosunku do uniwersalnego czasu koordynowanego UTC(PL).

4. Uniwersalny czas koordynowany UTC(PL) jest polską realizacją międzynarodowego uniwersalnego czasu koordynowanego UTC i wyznaczany jest przez państwowy wzorzec jednostek miar czasu i częstotliwości.

Art. 3. Prezes Rady Ministrów wprowadza i odwołuje czas letni środkowoeuropejski, w drodze rozporządzenia, ustalając na okres co najmniej jednego roku kalendarzowego dokładne daty, od których następuje wprowadzenie lub odwołanie czasu letniego, uwzględniając istniejące standardy międzynarodowe w tym zakresie.

Art. 4. 1. Organem uprawnionym do utrzymywania czasu urzędowego i uniwersalnego czasu koordynowanego UTC(PL) oraz do rozpowszechniania sygnałów tych czasów jest Prezes Głównego Urzędu Miar.

2. Minister właściwy do spraw gospodarki określi, w drodze rozporządzenia, sposoby rozpowszechniania sygnałów czasu urzędowego i uniwersalnego czasu koordynowanego UTC(PL), uwzględniając w szczególności standardy międzynarodowe i potrzeby użytkowników.

Art. 5. Traci moc ustawa z dnia 18 stycznia 1996 r. o czasie letnim (Dz. U. Nr 29, poz. 128).

Art. 6. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Prezydent Rzeczypospolitej Polskiej: *A. Kwaśniewski*

Dziennik Ustaw Nr 56 — 3218 — Poz. 548 i 549

548

ROZPORZĄDZENIE MINISTRA GOSPODARKI, PRACY I POLITYKI SPOŁECZNEJ[1)]

z dnia 19 marca 2004 r.

w sprawie sposobów rozpowszechniania sygnałów czasu urzędowego i uniwersalnego czasu koordynowanego UTC(PL)

Na podstawie art. 4 ust. 2 ustawy z dnia 10 grudnia 2003 r. o czasie urzędowym na obszarze Rzeczypospolitej Polskiej (Dz. U. z 2004 r. Nr 16, poz. 144) zarządza się, co następuje:

§ 1. Sygnały czasu urzędowego i uniwersalnego czasu koordynowanego UTC(PL) są rozpowszechniane z Głównego Urzędu Miar następującymi sposobami:

1) całodobowo za pośrednictwem sieci Internet z dwóch serwerów czasu o adresach: **tempus1.gum.gov.pl** i **tempus2.gum.gov.pl** z zastosowaniem protokołu transmisyjnego NTP (Network Time Protocol);

2) całodobowo za pośrednictwem sieci telekomunikacyjnej z wykorzystaniem modemu telefonicznego numer (0-prefix-22) 6548872 i zastosowaniem kodu sygnałów czasu European Telephone Time Code;

3) metodą radiodyfuzyjną za pośrednictwem jednostek radiofonii publicznej co każdą pełną godzinę.

§ 2. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Minister Gospodarki, Pracy i Polityki Społecznej:
J. Hausner

[1)] Minister Gospodarki, Pracy i Polityki Społecznej kieruje działem administracji rządowej — gospodarka, na podstawie § 1 ust. 2 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 7 stycznia 2003 r. w sprawie szczegółowego zakresu działania Ministra Gospodarki, Pracy i Polityki Społecznej (Dz. U. Nr 1, poz. 5).

Rys. 19. Fragment Dz.U. Nr 16 z 2003 poza 144 i Nr 56 z 2004, poz. 548 określający sposoby dystrybucji czasu urzędowego UTC(PL) w Polsce

Tym samym od ponad 20 lat czas w Polsce jest chroniony prawnie i może on wywoływać skutki prawne. Dlatego krajowy przemysł i administracja powinny bazować na polskim czasie urzędowym. W roku 2023 uruchomiony został w Głównym Urzędzie Miar RP system eCzasPL[40], który może niezależnie od GNSS dostarczać uwierzytelniony kryptograficznie polski czas urzędowy UTC(PL) siecią Internet i dedykowanymi łączami Ethernet. Projekt eCzasPL rozszerza ustawę o mechanizm zdalnego audytowania wskazań czasu odległych serwerów NTP i PTP (IEEE1588). Technologia ta została opracowana w latach 2015-2016 przez inżynierów polskiej Elpromy[41] uczestniczących w europejskim projekcie Horizon 2020 o nazwie DEMETRA[42].

Jedną z bardzo ważnych cech systemu e-CzasPL, szczególnie ważnych dla budowy systemów czasu odpornych na manipulacje i fałszowanie, jest możliwość stworzenia konwergetnego modelu bezpieczeństwa synchronizacji, gdzie czas pobierany jest jednocześnie:

- **siecią komputerową** z uwierzytelnieniem do serwerów NTP wymienionych w Dz.U. Nr 56 z 2004, poz. 548 i ciągłym audytem (monitorowaniem) ustawień czasu na synchronizowanych tak serwerach NTP/PTP (IEEE1588).
- **z europejskiego systemu satelitarnego GALILEO** wspieranego zapasowym systemem GPS, oba objęte **funkcją zdalnego audytowania** wskazań czasu UTC po stronie odbiorcy końcowego (audyt serwerów NTP/PTP użytkownika) z raportowaniem do Głównego Urzędu Miar RP dla celów certyfikacji czasu urzędowego zgodnie z ustawą.

Powyższy model pozwala na tworzenie bezpiecznych systemów dostaw czasu urzędowego UTC odpornych na manipulacje. W zależności od zdefiniowanych wektorów zagrożeń system synchronizacji powinien dynamicznie adoptować swoją konfigurację tak aby pracować w sposób scentralizowany (brak zagrożeń) i stopniowo w miarę pojawiania się ataków decentralizować konfigurację na obszarach objętych jammingiem lub spoofingiem.

Kolejną bardzo ważną cechą niezawodnego systemu czasu, szczególnie istotną dla jego pracy w trybie decentralizacji (podczas ataku) jest utrzymywanie autonomii rozproszonych zegarów składowych. Osiąga się to poprzez stosowanie oscylatorów holdover podtrzymujących czas. Do najbardziej popularnych należą oscylatory (w kolejności od najgorszych parametrycznie ale najtańszych do najlepszych i najdroższych): TCXO, OCXO, rubidowe, cezowe, masery wodorowe, zegary optyczne i fontanny cezowe. Proces autonomii pracy podsystemów synchronizacji systemu niezawodnej synchronizacji wymaga wsparcia techniki agregowania zegarów, co polega na wzajemnym łączeniu wielu zegarów szeregowo w grupy tworząc większą inercję utrzymania stabilnego upływu czasu.

Autonomicznie pracujące podsystemy synchronizacji coraz częściej wspiera sztuczna inteligencja (AI) i uczenie maszynowe (ML). Już obecnie telekomunikacja 5G stosuje zegary

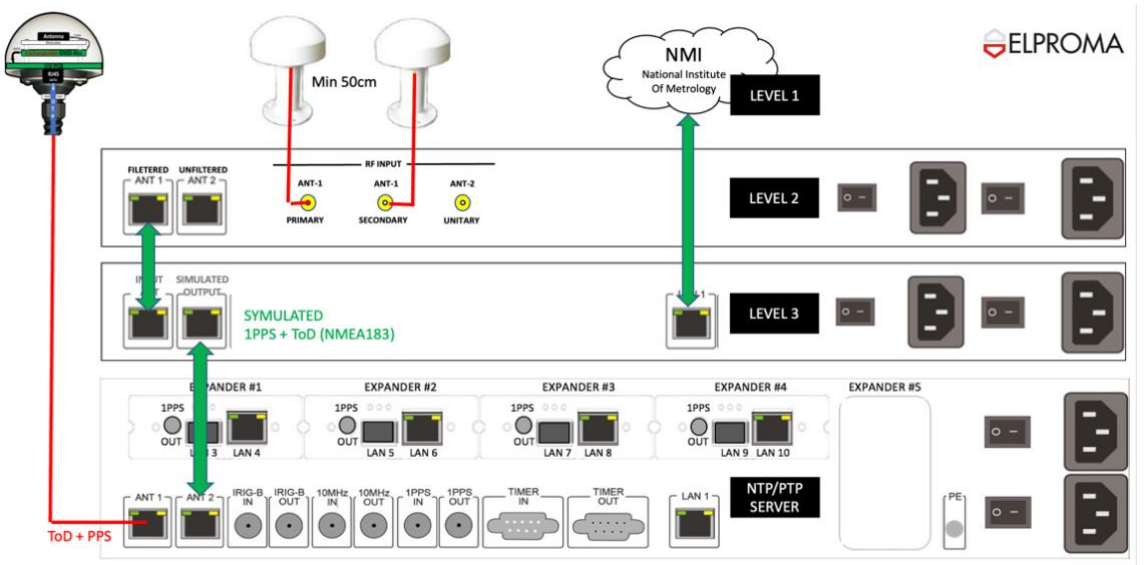
[40] Główny Urząd Miar RP, Projekt eCzasPL, https://www.gum.gov.pl/pl/projekty-eu/e-czaspl/3632,e-CzasPL.html.

[41] www.elpromaelectronics.com

[42] Projekt DEMETRA Horizon 2020 (EUSPA)
https://www.ion.org/publications/abstract.cfm?articleID=14982

klasy ePRTC, które mając wbudowane statystyki stabilności zegarów atomowych i ucząc się na bieżąco mogą się zachowywać, w trybie holdover, jak zegary cezowe. Agregacja takich zegarów pozwala tworzyć całe podsystemy autonomicznych korporacyjnych skal czasu UTC określanych jako sieciowe zegary koherentne (cnPRTC). Nie wymagają one częstej kalibracji do GNSS. Ich wadą pozostaje wysoka cena, dlatego mogą być brane pod uwagę jedynie do potrzeb wspierania stabilności pracy infrastruktury krytycznej IT w jej części szkieletowej. Dobrym przykładem zastosowania sieci zegarów cnPRTC jest jej użycie do budowy alternatywnych względem GNSS naziemnych systemów PNT (Positioning Navigation Timing). Rozwiązania takie odegrają ważną rolę w automatyzacji smart-city, inteligentnej sieci smart-grid, autonomicznych pojazdach, portach – to ważny składowy element telekomunikacji 5G i 6G low-latency.

W zdecydowanej większości przypadków budowa systemu synchronizacji odpornego na ataki i manipulacji odbywać się może skutecznie o trzy poziomowy model ochrony jaki proponuje Polska firma Elproma wspierana produktami firmy PIK Time[43]. Obie firmy ściśle współpracują od ponad dekady.



Rys. 20. Trzy poziomowy autorski system synchronizacji polskieg producenta ELPROMA z synchronizacją do Głównego Urzędu Miar RP

.

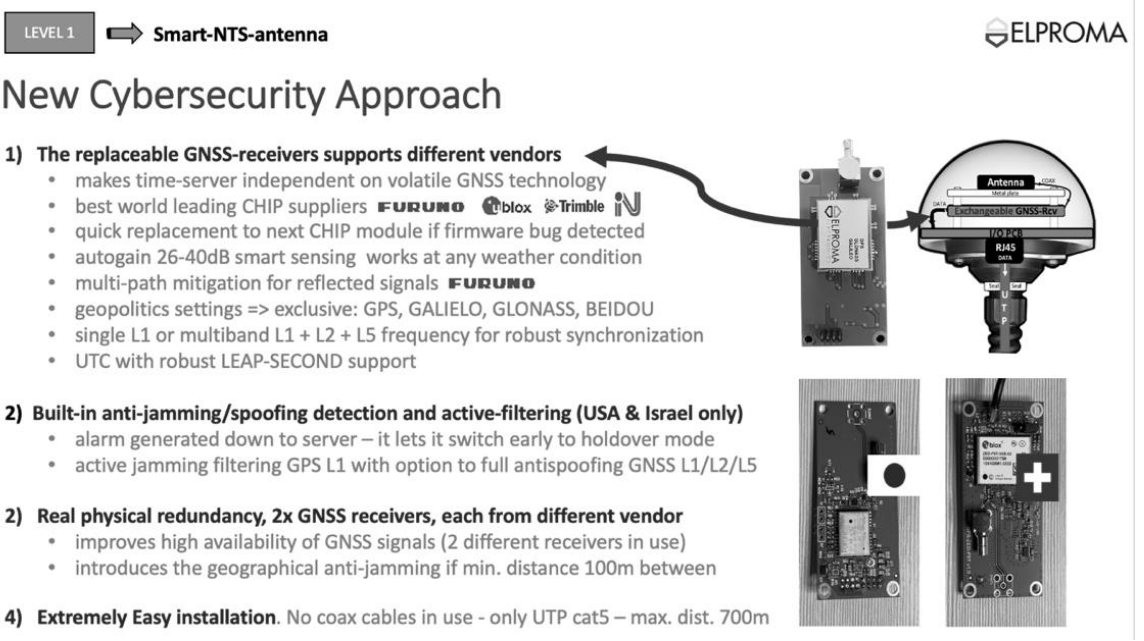
Firma ELPROMA stworzyła autorski system synchronizacji z 3-stopniowym zabezpieczeniem (rysunek 20) bezpieczeństwa:

LEVEL-1 (poziom 1), to inteligenta antena zawierająca wymienny moduł odbiorników GNSS. Firma proponuje specjalne dopasowanie odbiorników do uwarunkowań geopolitycznych w regionie lub na kontynencie. W Europie rekomendowany jest do użycia system GALILEO wspierany GPS. Ameryka, Australia i Nowa Zelandia używają anteny wyposażone w odbiorniki synchronizowane do GPS i wspierane GALILEO. Gospodarki państw powiązane z Rosją wybierają konfiguracje anten z odbiornikami synchronizowanymi do systemu GLONASS. Chińczycy używać będą system BEIDOU, a Indie IRNSS. Pozostałe

[43] www.piktime.com

państwa dobierać będą odbiorniki w zależności od preferencji i uwarunkowań gospodarczych i geopolitycznych dla swojego regionu. Dobór producenta układów odbiorczych GNSS odbywa się w takim przypadku zawsze we współpracy z działem cyberbezpieczeństwa infrastruktury krytycznej klienta.

Ważną cechą rozwiązania jakie proponuje polska Elproma jest możliwość korekty odbiornika GNSS w antenie w dowolnym momencie eksploatacji systemu. Wykrycie choćby najmniejszej ulotności bezpieczeństwa wymusza uruchomienie procedury wymiany modułu bez konieczności ingerencji w zaawansowany technicznie serwer czasu NTP IEEE1588.



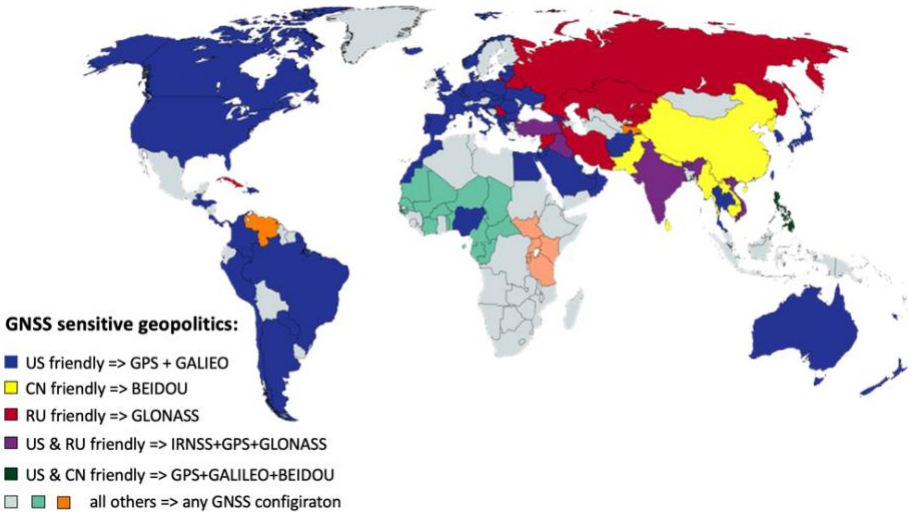
Rys. 21.Rysunek z prezentacji polskiej firmy ELPROMA [44]
prezentujący wymienność modułów GNSS w odbiorniku (antenie) z propozycją wyboru układu produkcji japońskiej i szwajcarskiej. Podobnych wymiennych układów firma Elproma ma kilkanaście w ofercie.

Polska firma oferuje kilka testowanych laboratoryjnie odbiorników GNSS do anten, w tym również bardziej zaawansowane z wbudowaną funkcją anty-jammingu, anty-spoofingu, filtrowania odbić (ang. Mutipath Mitigation) sygnału GNSS. Na specjalne zamówienie i za dodatkową opłatą Elproma jest w stanie zastosować w swoich urządzeniach dowolnie wybrany przez klienta odbiornik satelitarny również od operatorów satelitarnych systemów niskich orbit takich jak Xona Space i IRIDIUM.

Zaletą takiej architektury jest jej konfiguracja „pod klucz" i odejście od stereotypu statycznych konfiguracji, łatwych w rozpoznaniu i w konsekwencji w hakowaniu z użyciem jammingu i spoofingu GNSS, a to szczególnie zwiększa walor cyberbezpieczeństwa polskiego rozwiązania doceniany dziś w agendach NATO w Europie (rysunek 20).

[44] www.elpromatime.com

LEVEL-2 (poziom 2), to urządzenie do aktywnej filtracji zakłóceń GPS L1 w tzw. technice null-steering. Opcja ta jest adresowana do klientów używających amerykańskiego systemu GPS wiązka L1 o częstotliwości 1575.42 MHz jako referencyjne źródło czasu (np. kraje Ameryki Łacińskiej, wybrane kraje Azji, w tym Izrael – patrz rysunek 22) skutecznie filtruje zakłócenia tej wiązki emitowane na Ziemi. Odfiltrowany sygnał GPS jest w pełni wartościowym sygnałem wzorcowym czasu. Filtr wprowadza nieznaczne kilkunanosekundowe opóźnienie, które projektanci systemów synchronizacji mogą uwzględnić w kolejnym poziomie (LEVEL-3) lub z poziomu serwera czasu NTP IEEE1588.



Rys. 22. Mapa geopolityczna widziana jako BIOS zaufania do systemów satelitarnych GPS+GALILEO, GLONASS, BEIDO (bez IRNSS)

LEVEL-3 (poziom 3), to urządzenie klasy GNSS-firewall. Obejmuje warstwę symulacji sygnału satelitarnego GNSS oddzielającą serwer czasu NTP/PTP (IEEE1588) od fizycznego dostępu do satelitów GNSS. Symulacja sygnału GNSS na wyjściu odbywa się w oparciu o czas przechowywany w wewnętrznych oscylatorach lub może być dostarczany siecią komputerową z oddalonych serwerów NTP. Ocena z którego źródła czasu ma skorzystać LEVEL-3 należy do zaawansowanych technicznie rozwiązań i stanowi unikatowe know-how polskiej firmy ELPROMA. Polskie urządzenie poziomu 3 identyfikowane jest nazwą **SafeTime GNSS Guard LEVEL3** i może pobierać niezależnie siecią uwierzytelniony kryptograficznie wzorcowy czas z Głównego Urzędu Miar RP (Projekt e-Czas.PL), oraz z lokalnych zegarów atomowych rozlokowanych na terenie kraju w tzw. zapasowych centrach czasu. Firma Elproma dysponuje unikatową technologią pobierania i rozgłaszania skali UTC bezpośrednio z atomowych zegarów cezowych Microchip 5071A (wcześniej HP/Agilent 5071A) oraz z poziomu mikrostepera HROG-10 firmy Spectra Dynamics (USA).

TIME-SERVER, to główne urządzenie odpowiedzialne za synchronizacje wszystkich elementów pracujących w sieci komputerowej. Jest komponentem składowym systemu bezawaryjnej synchronizacji, gdzie jako zegar podlega zwielokrotnieniu w wyniku agregacji. W przypadku polskiej firmy Elproma rolę tę znakomicie pełni serwer czasu NTS-5000Rb. Ważną zasadą stosowaną przy projektowaniu systemów synchronizacji odpornych na

manipulacje i cyberataki jest filozoficzna zasada używania wielu źródeł czasu jednocześnie i składająca się co najmniej z grup:

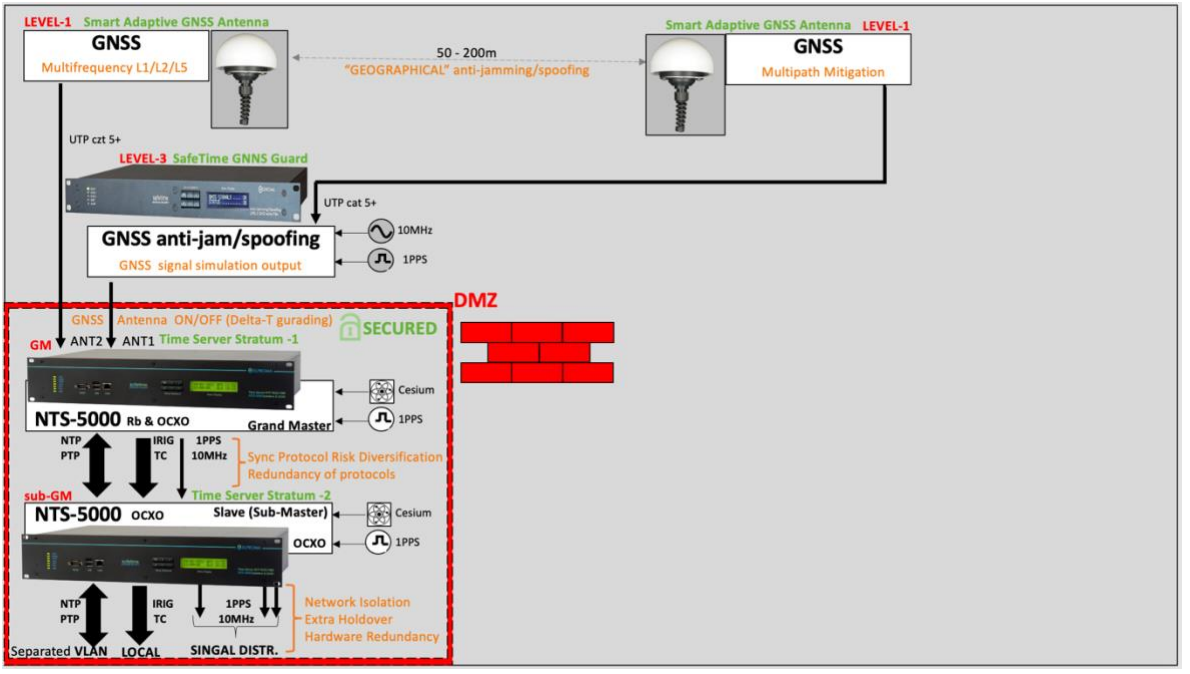
- wzorzec z konstelacji GNSS (np. GALILEO wspierany amerykańskim GPS)
- Wbudowane oscylatory podtrzymujące czas (Rubidowy, OCXO)
- Zewnętrzne źródło czasu urzędowego dostarczane siecią (np. e-Czas.PL GUM RP)

Całość w konfiguracji wspieranej poziomami ochrony LEVEL 1-3 opisanymi wyżej.

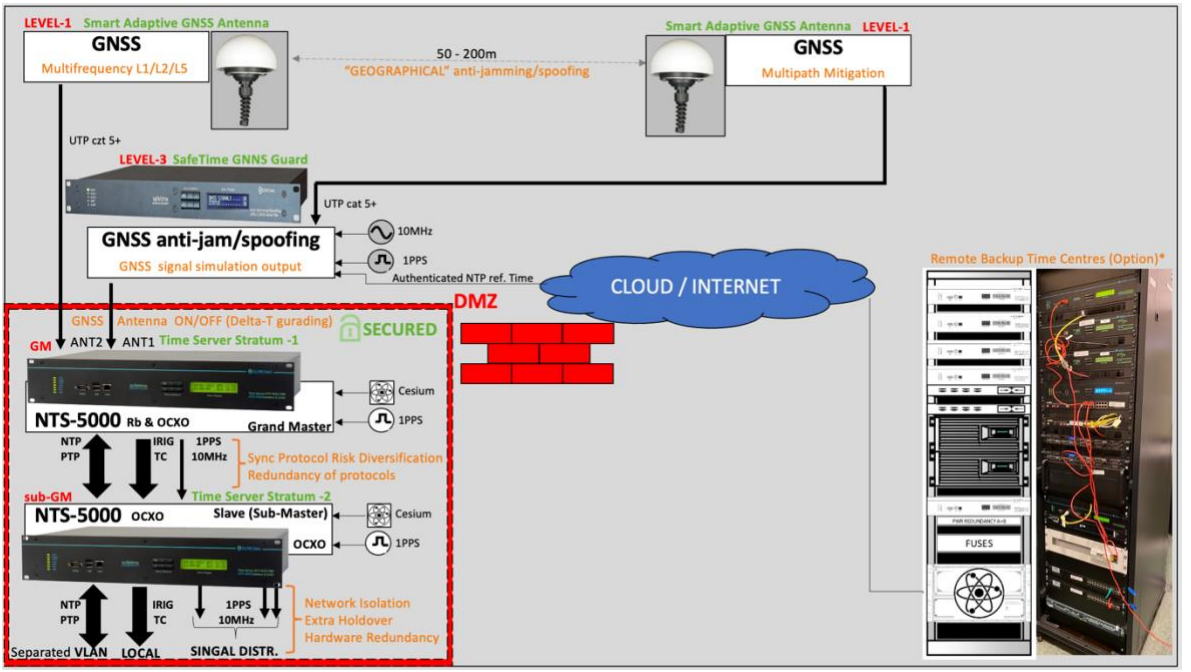
Na zakończenie warto powiedzieć o izolacji „galwanicznej informacyjnej" pomiędzy poziomem serwera czasu NTP/PTP a synchronizowanymi urządzeniami sieciowymi pracujących w wewnętrznej odizolowanej od Internetu sieci infrastrukturalnej. Izolację taką wprowadza się w przypadku, gdy wiele podsieci LAN korzysta ze wspólnego zasobu pojedynczego serwera czasu. W przypadku takim należy najpierw dodać i synchronizować kolejny poziom serwera SUBMASTER (wcześniej określany jako slave).

Przykładowe schematy aplikacyjne systemów synchronizacji odpornych na ataki.

W najprostszym modelu ochrony (Rysunek 23), obie fizyczne anteny z odbiornikami GNSS oddalone są od siebie fizycznie o dystans min 200 metrów co zapewnia skuteczną ochronę przed amatorskimi urządzeniami zakłócającymi (jamming GNSS). Należy zadbać, aby wymienne wkłady odbiorników GNSS w antenach pochodziły od różnych kwalifikowanych dostawców. Zwraca się uwagę, na asymetrię toru anten. Jedna z anten wprowadzana jest bezpośrednio do serwera czasu, podczas gdy druga przechodzi poprzez symulator LEVEL3, który w przypadku ataku TAS wyłączy odbiornik (antenę) i sam przejdzie w tryb pracy holdover dostarczając czas pochodzący z wewnętrznych oscylatorów. Urządzenie LEVEL-3 symuluje sygnał czasu GNSS do właściwego serwera tworząc agregacje 2-ch zegarów. Serwer NTS-5000 Grandmaster synchronizuje pośrednio urządzenia sieciowe poprzez taki sam serwer ale skonfigurowany jako SUBMASTER. Takie połączenie zapewnia izolacje „galwaniczną informacyjną" oraz tworzy kolejny poziom agregacji zegarów jednego z wielu rozproszonych węzłów synchronizacji

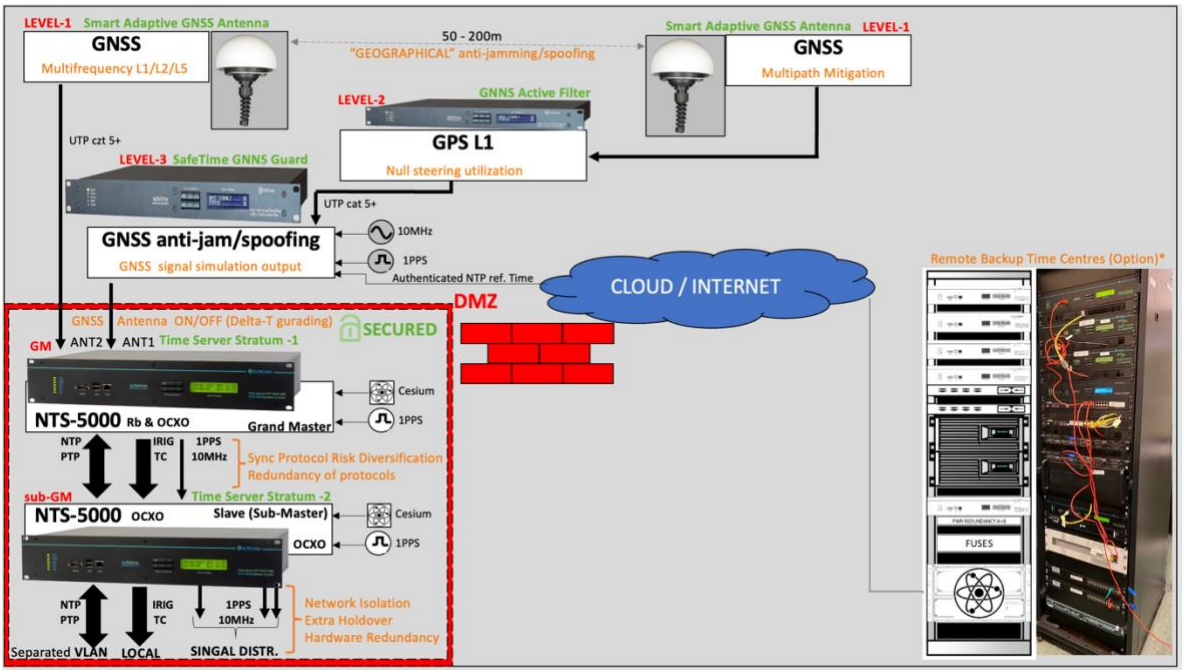


Rys. 23. Model prosty synchronizacji z użyciem 2szt. odbiorników GNSS (LEVEL-1)



Rys. 24. Model średniej klasy bezpieczeństwa synchronizacji. Rozwiązanie używa odbiorniki GNSS (LEVEL-1) szt. 2 praz symulator satelitarny LEVEL-3 zasilany z GUM (e-CzasPL)

W najbardziej złożonym modelu ochrony (Rysunek 25) dodaje się filtr aktywny LEVEL-2 pracujący w torze z symulatorem LEVEL-3. Zwraca się uwagę, że nadal zachowana jest zasada asymetrii konfiguracji torów antenowych (ilość i rodzaj użytych urządzeń w każdym z torów antenowych).



Rys. 25. Rozbudowany model bezpieczeństwa synchronizacji.
Rozwiązanie używa 2szt. odbiorników GNSS (LEVEL-1), aktywne filtry GPS L1 LEVEL-2 i symulator LEVEL-3 zasilany z zapasowego centrum czasu GUM (Projekt e-CzasPL)

Priorytetem w budowaniu systemu zarządzania czasem jest podstawowe stwierdzenie, że bezpieczna synchronizacja nie może się odbywać w oparciu o pojedynczy serwer czasu. Jako

niezbędne minimum przy budowie takich systemów uważa się użycie w pojedynczym węźle kilku serwerów czasu skonfigurowanych do pracy w układzie redundancji i zapewniających również agregację zegarów.

Rys. 26. Węzeł systemu synchronizacji „Klepsydra" w Polskiej Agencji Żeglugi Powietrznej, cześć rozproszonej architektury synchronizacji jaką dysponuje PAŻP w układzie konwergencji międzymiejskiej. Prezentowany węzeł zawiera 5 serwerów klasy NTS-5000, w tym jeden atomowy.

Rys. 26.a Widok panelu przedniego aktywnego filtru LEVEL-2 Elproma. Urządzenie filtruje zakłócenia GPS L1 klasy jamming/spoofing techniką nul-steering

Rys. 26.b Widok panelu przedniego symulatora GNSS poziomu LEVEL-3 Elproma. To sieciowy symulator GNSS odbierający z odległych serwerów NTP/PTP GUM RP (eCzasPL) informacje i zamieniający na symulowany sygnał antenowy do serwera czasu NTS-5000

Rys. 26.c Widok panelu serwera czasu NTP/PTP model NTS-5000 używanego w systemie eCzasPL

Podziękowanie

Autor dziękuję Panu **Tomaszowi Widomskiemu** z firmy ELPROMA[45], akredytowanemu krajowemu konsultantowi ds. czasu i częstotliwości ITU-R WP-7A w Genewie, za udostępnienie materiałów wykorzystanych w opracowaniu i udzielone konsultacje.

LITERATURA

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

[45] www.elpromaelectronics.com

DEMETRA project", poster presented at the 30th European Frequency and Time Forum, April 2016.

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

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

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

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

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

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

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

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

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

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