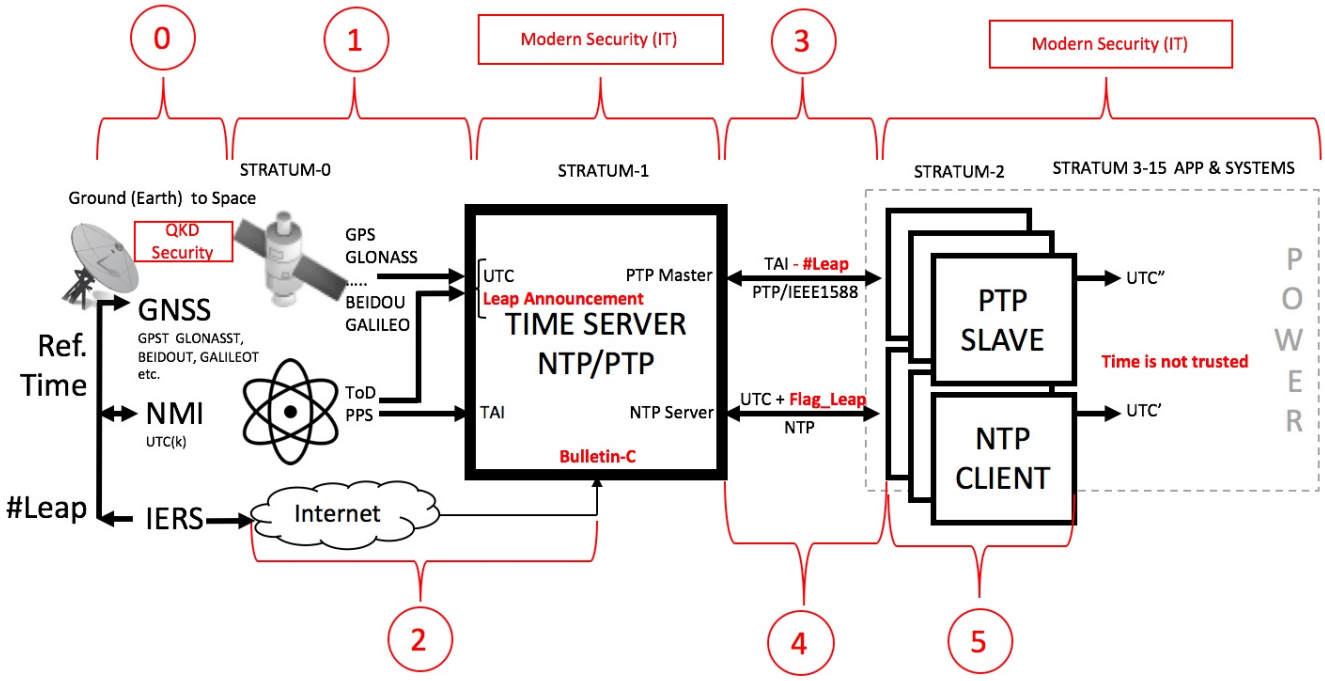
Wady synchronizacji opartej o odbiorniki GNSS i sieć Ethernet NTP/PTP

Bezpieczna i pewna synchronizacja czasu w ważnej infrastrukturze państwowej – ENERGETYKA

T. Widomski, K. Borgulski, J. Użycki, P. Olbrysz, J. Kowalski (ELPROMA)
e-mail: info@elpromatime.com web: www.elpromatime.com [1]



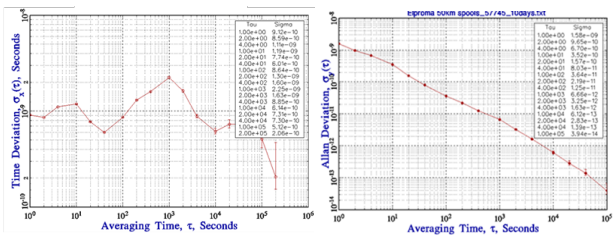
rys. 1 Pięć etapów *dystrybucji czasu UTC w energetyce obarczonych zagrożeniem błędów i utraty synchronizacji* (*ang. time gaps*)

BIOGRAFIA

Tomasz Widomski (l.51), absolwent Informatyki (1990), na Wydziale Elektroniki Politechniki Warszawskiej. Ukończył w 2012r. studia podyplomowe w Głównej Szkole Handlowej (SGH) w Warszawie. Prezes Zarządu spółki ELPROMA[1] (1992-2014), później honorowy członek zarządu, obecnie wchodzi w skład Rady Nadzorczej. Współtworzył segment serwerów NTP/PTP i telemetrii M2M. Od 2017r. popularyzuje budowę systemów synchronizacji, odpornych na manipulacje czasem, określanych nazwą (ang.) *Robust Synchronization* i promowanych przez GSA[3] wraz z wdrażaniem GALILEO.

ELPROMA[1] -polski producent serwerów czasu NTP/PTP, oraz serwerów kryptograficznego znakowania czasem *rfc3161* i urządzeń bezprzewodowej komunikacji M2M. Firma brała udział w krajowych i międzynarodowych projektach B+R, w tym: CERN[2] (2009-2012 White Rabbit) i DEMETRA[3] (2014-2016) Horizon 2020. Uczestnik krajowej grupy laboratoriów ds. porównań wzorców czasu TA(PL), działającej przy Głównym Urzędzie Miar RP. Serwery czasu NTP/PTP ELPROMY, są najczęściej wybieranymi produktami w energetyce, telekomunikacji, sektorze finansowym i administracji publicznej.

ELPROMA NTS-5000 z 4 interfejsami PTP/IEEE1588 (profil dla energetyki)



Testy NPL (National Physical Laboratory UK) wykazały precyzje 50ns

[1] ELPROMA www.elpromaelectronics.com www.elpromatime.com www.teleorigin.com
[2] CERN White Rabbit PTP https://en.wikipedia.org/wiki/The_White_Rabbit_Project
[3] DEMETRA https://www.gsa.europa.eu/demonstrator-egnss-services-based-time-reference-architecture

WSTĘP

W latach 2015-2017 firma Elproma uczestniczyła w międzynarodowym projekcie DEMETRA[3] Horizon 2020. Projekt dostarczył 9 nowych usług synchronizacji[4], wspierających wdrażany przez UE system GALILEO. Aby dobrze wykonać powierzone zadania, DEMETRA[4] poprzedzona była licznymi badaniami rynku określającymi zapotrzebowanie przemysłu na usługi synchronizacji. Przeprowadzono na terenie UE liczne audyty techniczne wybranych systemów synchronizacji opartych o satelitarny system GPS i sieć Ethernet TCP/IP, a ich wyniki odsłoniły liczne niedoskonałości obecnych rozwiązań (**rys. 1**).

Elpromę zaproszono do projektu w charakterze eksperta protokołów dystrybucji czasu: NTP *(Network Time Protocol)* i PTP/IEEE1588 *(Precision Time Protocol)*. Polskiej firmie powierzono też zadanie zaprojektowania nowej metody dystrybucji czasu, jaka mogłaby np. służyć bezpiecznej dystrybucji czasu do zastosowań prawnych. Czas taki określany jest też nazwą *czasu urzędowego*, którego źródła opisuje Dz.U 56/2004 (poz. 548)[5]. Wnioski z DEMETRY stały się podstawą do kontynuacji prac B+R w innych projektach UE, takich jak *Robust Time*. Obecnie firma ELPROMA pracuje nad stworzeniem chmury znakującej czasem – projekt *Safe Time (2017-2018)*.

WORKSHOP BRUKSELA DG-ENERGY 2017

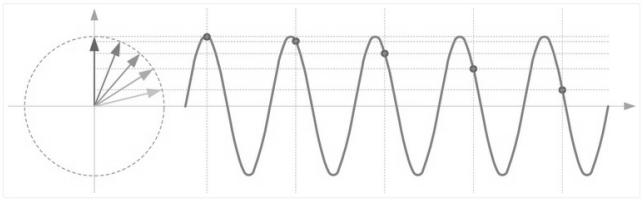
Wnioski DEMETRY zostały zaprezentowane podczas spotkania w dniu 6 lutego 2017 w DG-ENERGY[6] w Brukseli. Sformułowano tam tezę możliwego scenariusza cyber-ataku na infrastrukturę synchronizacji w sektorze energetyki (ang. *Time Synchronization Attack*), której skutkiem mógłby być np. *blackout*. Mimo, że prawdopodobieństwo skuteczności takiego ataku wydaje się nadal niewielkie, to ekspertów niepokoją sprzyjające takiemu zagrożeniu nakładające się na siebie wzajemnie okoliczności:

- *obserwowane zmiany geopolityczne tej dekady,*
- *zagrożenia terroryzmem i cyber-terroryzmem,*
- *niski stopień świadomości roli synchronizacji w strategicznych sektorach gospodarek państw UE,*
- *numeryczna reprezentacja czasu w IT stawia obok siebie tak samo prawdopodobnym błąd wielkości nanosekundy, sekund, godzin, miesięcy i lat; zwiększa to ryzyko dotkliwszych skutków skutecznego cyber-ataku w energetyce,*
- *rosnąca złożoność i współzależność systemów IT mogąca wywołać efekt domina o dużej skali,*
- *niszowa natura synchronizacji powoduje, że segment ten liczy niewielkie grono ekspertów; ogranicza to możliwości wymiany informacji na dużą skalę z gronem ekspertów bezpieczeństwa,*
- *brak rozwiązań alternatywnych, w tym procedur postępowania w przypadku wystąpienia cyber-ataku na infrastrukturę synchronizacji energetyki*

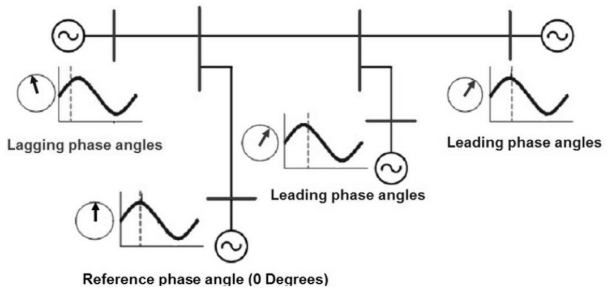
Zgodnie z wymaganiami opisanymi w dokumentach IEEE [29] [30] , synchronizacja powinna zapewniać:

1) zgodny czas, tzn. pracę we wspólnej domenie czasowej (ang. *Time Domain*) skali *UTC,*
2) zapewnienie dokładności 1 mikrosekundy [µs] przy założeniu maksymalnej liczby 16 przejść (ang. *hop)* przez przełączniki i routery sieci Ethernet. Każde przejście wnosi średnio 50 ns opóźnienia, co definiuje konieczność zapewnienia przez serwer czasu co najmniej precyzji lepszej niż 200 ns (200x 10^{-9} sekundy). Wymóg ten spełniają nieliczne serwery czasu z tzw. sprzętowym znakowaniem czasu w warstwie fizycznej PHY Ethernet (np. ELPROMA model NTS-5000 PTPv2 IEEE1588:2008 z profilem „Energy" oferujący precyzję synchronizacji 25ns)
3) dokładność 500 ns do nadzoru stanu linii i precyzyjnej lokalizacji uszkodzeń techniką fali bieżącej (ang. *travelling wave).*

Dokładność 1 µs jest niezbędna do zarządzania dystrybucją energii. Kontrola odbywa się poprzez pomiar kąta fazowego (rys. 2) i jest realizowane przy pomocy urządzeń PMU (ang. *Phasor Measurement Unit)* określonych w standardzie *IEEE C37.118 (*rys. 3*)*



rys. 2 *Reprezentacja kąta fazowego w PMU /Synchrophazors IEEE C37.118/*



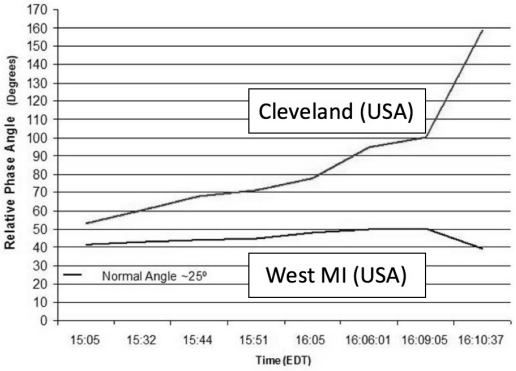
rys. 3 *Rozproszony system monitorujący kąt fazowy dystrybuowanej energii*

Tak precyzyjna synchronizacja w energetyce formuje krytyczne parametry przesyłu energii, tutaj fazę, ale i częstotliwość wytwarzanego napięcia. Aktualny stan sieci energetycznej opiera się na estymacji, opartej o bieżący odczyt danych z układów pomiarowych. Dlatego dane muszą być przekazywane do systemów sterowania z możliwie jak najmniejszym opóźnieniem (*delay*).

Nieskorelowane w czasie informacje mogą dostarczyć nieprawdziwych lub nieaktualnych danych. Może to spowodować podjęcie błędnej decyzji przekierowania sterowania mocą i przepływem dystrybuowanej energii. W szczególności odchylenie kąta fazowego o wartość ponad 25^0 stwarza ryzyko poważnej awarii energetycznej, a

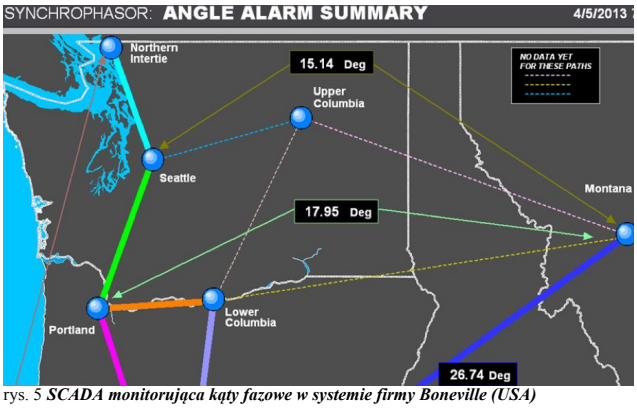
[4] Oficjalna strona www.demetratime.eu INRIM: http://rime.inrim.it/H2020-Demetra/
[5] Dz.U poz. 548 z 2004r: http://isap.sejm.gov.pl/DetailsServlet?id=WDU20040560548
[6] DG ENERGY http://ec.europa.eu/energy/ (patrz również bibliografia [42])

nawet *blackoutu*. Rozsynchronizowanie PMU było najprawdopodobniej przyczyną blackoutu na wschodnim wybrzeżu USA w sierpniu 2003 roku (rys. 4).



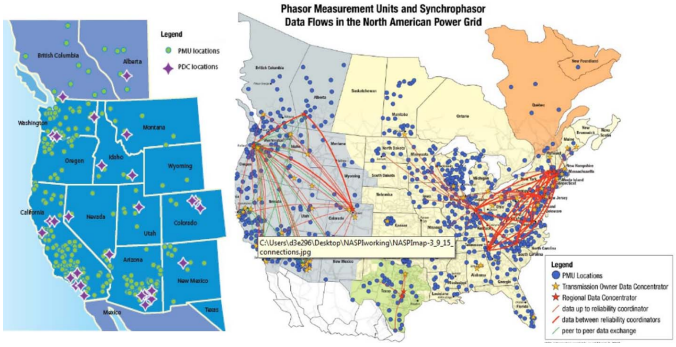
rys. 4 *Rejestrowany blackout na wschodnim wybrzeżu USA (sierpień 2003)*

Monitorowanie dystrybucji energii odbywa się przy pomocy systemów SCADA (rys. 5) generujących stosowne alarmy, w tym zwłaszcza informujące o zbyt dużych zmianach kątów fazowych. Nie mniej ważne jest przekazywanie tych danych ze znanym opóźnieniem, tak aby reakcja operatora możliwa była bez ryzyka awarii mogącej wywołać efekt domina (*blackout*). Rygor utrzymania parametrów synchronizacji w energetyce w Europie reguluje standard *IEC61850-9-2 Bus & Station*.



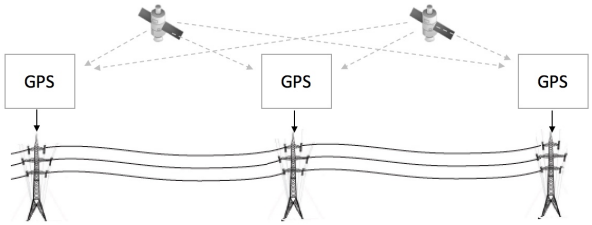
rys. 5 ***SCADA monitorująca kąty fazowe w systemie firmy Boneville (USA)***

Zdaniem profesora Vaccarro [42] (ekspert DEMETRA), to właśnie obawy przed skutecznym cyberatakiem na infrastrukturę synchronizacji opartą o GPS sprawiają, że do dnia dzisiejszego największy amerykański system zarządzania Smart Grid *WAMPAC (Wide Area Monitoring, Protection, and Control Systems)* pozostaje w trybie nadzoru danych, tzn. bez aktywnej automatyki sterowania przekierowaniem mocy dystrybuowanej energii. Sterowanie to pozostaje nadal pod kontrolą operatora i opiera się o dane z równoległych systemów.

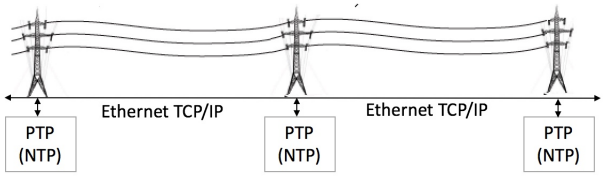


rys. 6 *WISP (lewa strona)) – obszar zachodniego wybrzeża objęty programem połączenia PMU. Na prawo widok całej infrastruktury energii w USA*

Dlatego tak ważne jest stworzenie niezawodnego, pewnego mechanizmu dystrybucji czasu gwarantującego utrzymanie rygoru 1 µs precyzji synchronizacji względem skali UTC. Wymóg ten opisuje standard IEEE C37.238. Dystrybucja czasu UTC zapewniającego wspólną domenę czasową może odbywać się na dwa sposoby przedstawione na rysunku rys. 7 i rys. **8**.



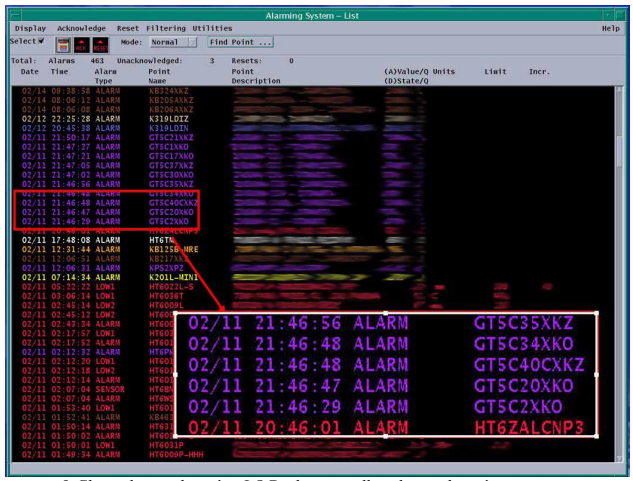
rys. 7 Zdecentralizowany system odbiorników GPS



rys. 8 Scentralizowany system dystrybucji czasu siecią Ethernet TCP/IP wykorzystujący PTP/IEEE1588 (wcześniej protokół NTP)

Do dystrybucji UTC można też, wykorzystać mieszany model hybrydowy będący dowolną kombinacją schematów z rysunków rys. 7 i rys. **8**.

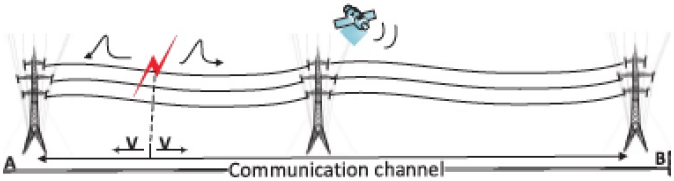
Każde wydarzenie w sieci generujące alarm jest rejestrowane w systemowych dziennikach zdarzeń LOG wraz z datą i godziną wystąpienia. Zachowanie chronologii tych zdarzeń wymaga synchronizacji wszystkich elementów systemu, włączając główne serwery, kontrolery (czujniki, w tym PMU) a nawet systemy baz danych (DB). W przypadku wystąpienia awarii, uporządkowane zapisy LOG dostarczają informacji niezbędnych do identyfikacji problemu. Jest to możliwe wyłącznie wtedy, gdy system IT pozostaje zsynchronizowany. Zachowanie relacji przyczynowo skutkowych pozwala odtworzyć dokładny przebieg wydarzeń i ustalić przyczynę awarii. Nieautoryzowane zmiany zawartości dzienników LOG lub niewystarczająca synchronizacja uniemożliwiają identyfikację przyczyny wystąpienia awarii. Obecnie dzienniki LOG chronione są uprawnieniami administratora i włamanie do systemu z takimi prawami pozwala zmienić zapisy (rys. 9).



rys. 9 *Chronologia zdarzeń w LOG odzwierciedla relacje zdarzeń i zapewnia ciąg przyczynowo skutkowy niezbędny do identyfikacji awarii.*

Synchronizacja jest też wykorzystywana w rozliczeniach energii (*ang. metering*), w wirtualnym handlu energią, bilingu i fakturowaniu. Błędy synchronizacji nie wnoszą tu wprawdzie bezpośredniego ryzyka paraliżu, ale mogą być powodem strat finansowych w różnej skali.

Warto jeszcze wspomnieć o pewnej poddziedzinie synchronizacji w energetyce, wymagającej dużych precyzji rzędu co najmniej 500 ns. Tak precyzyjny czas używany jest do pomiaru fali bieżącej (ang. *travelling wave*) – reakcji na wzorzec, używanej do diagnozowania stanu linii przesyłowych i wskazywania miejsca uszkodzeń. Im większa precyzja, tym dokładniej można ustalić miejsce uszkodzenia linii przesyłowej. Ma to zastosowania zarówno dla linii napowietrznych jak i podziemnych (rys. 10)



rys. 10 *Fala bieżąca lokalizuje uszkodzenia w linii przesyłowej*

Awarie w sektorze energetyki mają wpływ na inne gałęzie przemysłu, a w szczególności na: bieżącą produkcję, telekomunikację (TV/radio/Internet), sektor finansowy, administrację publiczną, a w miastach na wodociągi i kanalizację, kierowanie ruchem ulicznym, ruch kolei, kontrolę lotów itp. Każda większa awaria w energetyce niesie ryzyko okresowej destabilizacji jakiegoś regionu. Odwoływane są planowe zabiegi operacyjne w szpitalach, licznym utrudnieniom ulega praca służb publicznych. Niepokój społeczny stymuluje dezinformacja spowodowana brakiem łączności i wzmacniana panującą po zachodzie słońca ciemnością. Brak perspektywy dostępu do posiadanych środków pieniężnych zdeponowanych w bankach wzmacnia jedynie i tak panującą niepewność.

Z tych powodów sektor energetyki pozostaje w zasięgu zainteresowania grup hakerów i jest narażony na ataki. Nowym wyzwaniem staje się ochrona infrastruktury energetycznej wrażliwej na skutki rozsynchronizowania.

PIĘĆ GRUP RYZYKA POWSTAWANIA BŁĘDÓW

W procesie transferu czasu ryzyko powstawania błędów synchronizacji występuje w następujących 5 etapach, wskazanych na rysunku **rys. 1**:

etap 0 – transfer ziemia-kosmos
- ***błędy wewnętrzne GNSS*** *(GPS, GLONASS, BEIDOU)*
- ***wojskowa natura*** *systemów GPS, GLONASS, BEIDOU*

etap 1 – transfer kosmos-odbiornik GNSS na Ziemi
- ***zagłuszanie sygnałów*** *GPS (ang. GPS Jamming)*
- ***symulacja naziemna*** *sygnałów GPS (ang. GPS Spoofing)*
- ***brak obsługi sekundy przestępnej*** *(ang. Leap Second)*
- ***błędy wewnętrzne odbiorników*** *satelitarnych GNSS*
- ***wielosekundowe różnice skal czasu*** *GPST, GLONASST, BEIDOUT, GALILEOT*

[7] http://www.gps.pl/artykul-jamming.html

etap 2 – transfer publiczną siecią Internet
- ***brak kryptograficznej ochrony pliku*** *(IERS biuletyn-C) (możliwość manipulacji czasem oparta o podmianę pliku)*

etap 3 – transfer siecią Ethernet (protokół NTP)
- ***brak zapowiedzi sekundy przestępnej*** *(Leap Second)*
- ***wpływ asymetrii łącz*** *na dokładność synchronizacji*
- ***celowe wprowadzanie opóźnień*** *(np. Time Delay Attack)*

etap 4 – transfer siecią Ethernet (protokół PTP/IEEE1588)
- ***brak autentykacji*** *przesyłanych protokołem danych*
- ***reprezentacja UTC w postaci składowych*** *(TAI, #Leap)*
- ***wpływ asymetrii łącz*** *na dokładność synchronizacji*
- ***wpływ asymetrii łącz*** *na dokładność synchronizacji*
- ***celowe wprowadzanie opóźnień*** *(np. Time Delay Attack)*

etap 5 – transfer wewnętrzny na poziomie sprzętu
- ***zróżnicowanie systemowe OS/firmware*** *(obsługa czasu UTC, różnice w sposobie obsługi sekund przestępnych)*
- ***błędy i opóźnienia asymetrii*** *OS API (firmware)*
- ***błędy ludzkie*** *(ustawień konfiguracji, profili PTP itp.)*
- ***błędy niezgodności*** *(kompatybilności) PTP/IEEE1588*
- ***błędy skal czasu*** *(reprezentacja: UTC, POSIX, TAI)*

Sama wielkość błędu synchronizacji może się wahać w przedziale od nanosekund, aż po całe sekundy, a nawet dni i lata. Wiąże się to z numeryczną reprezentacją czasu (różne wagi poszczególnych bitów reprezentujących czas), podczas gdy powszechnie znane czynniki, takie jak temperatura czy propagacja informacji dają z reguły niewielkie błędy.

ŹRÓDŁA BŁĘDÓW SYNCHRONIZACJI

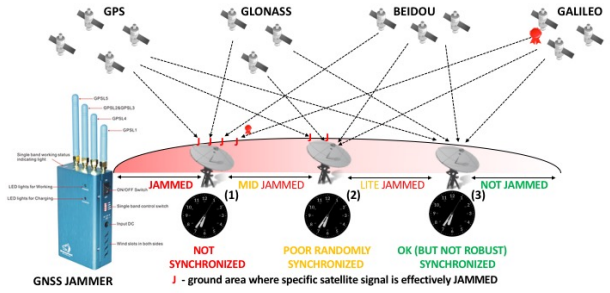
1. Jamming & Spoofing GNSS[7]

rys. 11 *Urządzenia do zagłuszania sygnałów GNSS są obecnie precyzyjnie dopasowane częstotliwością i pasmem do typu wiązki, a nawet sposobu jej kodowania.*

Jamming, to możliwość lokalnego zagłuszania sygnałów GNSS przy pomocy niedrogich, ale bardzo skutecznych urządzeń dostępnych, np. w sprzedaży internetowej. Skuteczność działania systemów zagłuszających i symulatorów GPS zależy od mocy użytego nadajnika. Współczesne urządzenia zagłuszające są perfekcyjnie dopasowane do częstotliwości wiązki satelitarnej i emitowany przez nie sygnał zagłuszający coraz częściej uwzględnia zaawansowane właściwości kodowania wiązki GPS L1-L5 (rys. 11). Skuteczność zagłuszania zależy od ukształtowania terenu, urbanistyki, lokalizacji anten serwerów czasu itp.

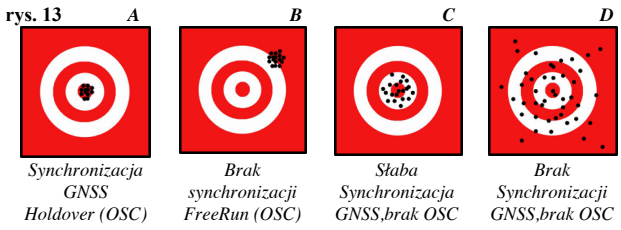
Jeszcze nie tak dawno, niecałą dekadę temu, ich użycie w segmencie synchronizacji było sporadyczne. Nieliczne

przypadki użycia były na tyle słabo udokumentowane, że trudno było odróżnić celowe zagłuszanie od wpływu zakłóceń elektromagnetycznych. Obecnie używanie urządzeń zagłuszających rozpowszechnia się. Londyńska giełda co kilka dni odnotowuje incydenty z ich użyciem, a niektóre przypadki wymuszają okresowe przerwy w notowaniach. Podobne próby mogą mieć miejsce również w sektorze energetyki w strukturze z rys. 7 .



rys. 12 *Skuteczność zasięgu zagłuszaczy GNSS zależy od siły nadajnika. W polu oznaczonym kolorem czerwonym (lewa część) odbiór GPS jest niemożliwy. W środkowej części odbiór jest losowy i sporadyczny, a w części z prawej strony mogą wystąpić problemy z odbiorem GPS i synchronizacją.*

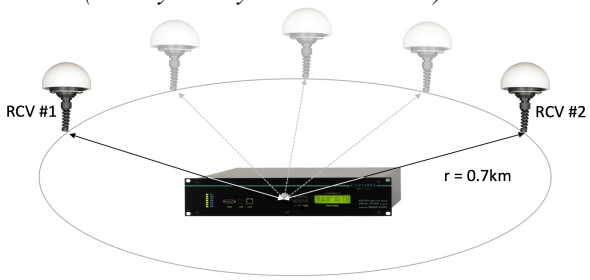
O ile zegar #1 (**rys. 12**) nie posiada alternatywnych dla GNSS dróg pozyskiwania wzorcowego czasu UTC (np. z NMI i zdalnie dostępnych serwerów NTP/PTP), jego czas w zależności od stabilności wbudowanych oscylatorów będzie sukcesywnie degradował się, podając coraz bardziej nieprawidłowe wskazanie względem UTC. Jeżeli zegar posiada wbudowane wysokiej jakości oscylatory, to proces degradacji (tempo wzrostu błędu UTC) może zostać spowolniony lub zatrzymany do czasu przywrócenia odbioru sygnału satelitarnego GNSS. Aby mogło tak być, oscylatory muszą uprzednio zsynchronizować się do GNSS lub zdalnie do NMI. Taki autonomiczny tryb pracy zegara nazywa się trybem *holdover*. W zależności od stabilności oscylatorów i żądanej precyzji synchronizacji, czas UTC w trybie *holdover* może być autonomicznie utrzymywany: godziny (TCXO), dni (OCXO), a nawet tygodnie i miesiące (Rubid). Ważnym, niezbędnym do spełnienia warunkiem jest podtrzymanie zasilania oraz nieresetowanie serwera NTP/PTP. Niezsynchronizowany z GNSS oscylator pracuje w trybie *FreeRun* zapewniając stabilną częstotliwość sygnału, ale nie gwarantując dokładnego czasu UTC. Synchronizację oraz jej błąd można zilustrować przy pomocy tarcz strzelniczych, których środek symbolizuje wzorcowy czas UTC (rys. 13).



Zegary i serwery NTP/PTP bez wbudowanych oscylatorów *holdover* reagują natychmiast na zagłuszanie GNSS i wprowadzają duży narastający błąd synchronizacji UTC.

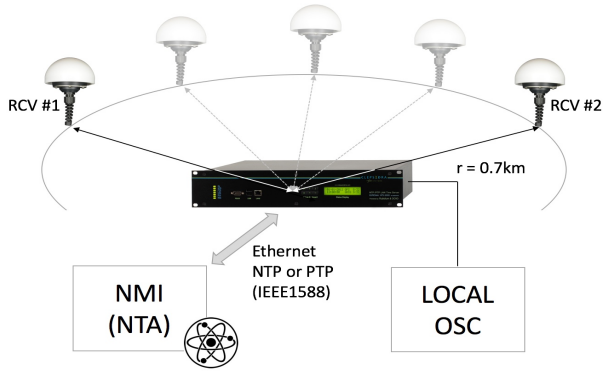
Rozwiązań problemu zagłuszania należy szukać w prostej dywersyfikacji polegającej na jednoczesnym użyciu minimum 3 niezależnych od siebie źródeł czasu i metod dostawy UTC. Sygnały czasu można uzyskać z:

1) *wielu rozproszonych odbiorników GNSS* (**rys. 14**)
2) *sieci Ethernet i zdalnych serwerów NMI*
3) *zsynchronizowanych wcześniej OSC holdover (lokalnych oscylatorów holdover)*



rys. 14 *Rozmieszczone w promieniu 0.7km od serwera ELPROMA NTS-5000 dwa niezależne odbiorniki GNSS minimalizują skuteczność zagłuszania GNSS*

Spoofing GNSS polega na fałszowaniu wiązki sygnału satelitarnego w celu wprowadzenia odbiornika w błąd pozycji i czasu. Wybrane systemy GNSS (np. GALILEO) przewidują wprowadzenie płatnej usługi zabezpieczającej przed takim zagrożeniem. Obecnie urządzenia spoofingowe pozostają na tyle drogie, że prawdopodobieństwo ich użycia jest zdecydowanie mniejsze niż użycie urządzeń zagłuszających. Celowe wprowadzenie odbiornika w błąd wiąże się z konkretnym celem działania. Takie przypadki odnotowuje się w sektorze finansowym w pobliżu dużych giełd finansowych w USA i w Wielkiej Brytanii. Kary za takie praktyki wyrażają się w liczbach 9 cyfrowych. Karane są banki inwestycyjne np. z segmentu HFT, które próbują w ten sposób wykorzystywać chwilowo wywołane perturbacje na rynku finansowym.



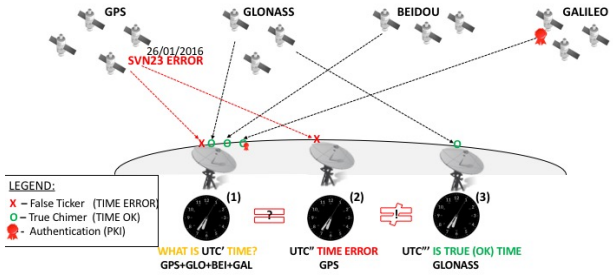
rys. 15 *Fałszywe sygnały GNSS mogą być rozpoznane i odrzucone, jeżeli serwer korzysta jednocześnie z alternatywnych źródeł i metod dostawy czasu*

W przypadku spoofingu, podobnie jak przy zagłuszaniu ważna jest dywersyfikacja ryzyka i używanie wielu źródeł UTC jednocześnie. Nie mniej ważna jest dywersyfikacja metod dostarczania czasu. Pomocą może być alternatywna dla GNSS droga dostrajania serwera do zdalnych wzorców NMI oraz dbanie o prawidłowy czas lokalnych oscylatorów *holdover* (rys. 15). Zarówno zagłuszanie jak i spoofing GNSS mogą być też rozpoznane przy pomocy specjalnych urządzeń. Niektóre z nich (rys. 16) mogą wskazać nawet kierunek, z którego pochodzi emisja sygnału zakłócającego. Stosowanie takich urządzeń wymaga stworzenia stosownych regulacji prawnych oraz ustanowienia procedur postępowania przez służby ochrony mienia.

rys. 16 *Urządzenie rozpoznające zagłuszanie i wskazujące kierunek źródła*

2. Nieodporność komercyjnych odbiorników GNSS na wewnętrzne błędy systemowe GPS, GLONASS itp.

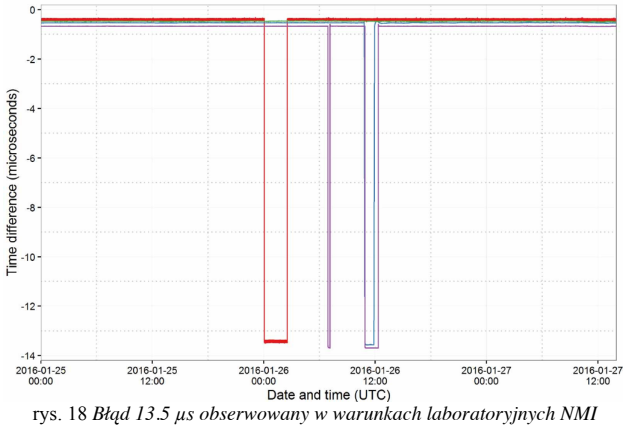
Przypadek błędu UTC znanego jako SVN23[8] wydarzył się w dniu 26 stycznia 2016 r. Wewnętrzny błąd systemu GPS wprowadził do odbiorników komercyjnych na Ziemi błąd 13.5µs względem czasu UTC, utrzymywanego prawidłowo przez pozostałe systemy GNSS (GLONASS, BEIDOU, GALILEO) oraz instytuty metrologii NMI, dysponujące zegarami atomowymi. Błąd wykazały nawet odbiorniki multi-satelitarne GNSS, ponieważ najczęściej wiodącym systemem bazowym nadal pozostaje GPS. Część odbiorników na Ziemi, mogła wskazać inny błąd, np. mniejszy niż 13.5 µs. Mogło by tak być w przypadku, gdy średnia ważona wytwarzanego w odbiorniku UTC sygnału czasu uwzględniała większą rolę pozostałych prawidłowo pracujących systemów GNSS. Możliwe, że część odbiorników (np. takie, które nie używały GPS a były skonfigurowane do pracy wyłącznie z systemami GLONASS i BEIDOU, bez GPS) nie były podatne na błąd 13.5µs. Błąd zarejestrowały, ale nie powieliły go narodowe instytuty metrologii (NMI) dysponujące własnymi zegarami atomowymi i wytwarzające własne skale UTC(k).



rys. 17*Wewnętrzne błędy poszczególnych systemów GPS, GLONASS, BEIDOU, GALILEO mogą wprowadzić błąd jak SVN23 z 26/01/2016*

W przypadku błędu GPS 13.5 µs (SVN23) (rys. 17) zdestabilizował on na wiele godzin pracę systemów informatycznych, co opisano w mediach (np. BBC[9]). Wielkość błędu, choć pozornie niewielka, zagroziła stabilności sektora energetycznego, przekraczając 13.5 razy żądaną dokładność UTC (max. dopuszczalny błąd czasu). Błąd stanowił też zagrożenie dla sektora finansowego. Przypadek SVN23 pokazał, że systemy grupy GNSS nie są wolne od błędów. Wielkość offsetu 13.5 µs mogłaby być większa, gdyby błąd dotyczył bardziej znaczących bitów rejestru danych, reprezentujących numerycznie czas w systemie satelitarnym GPS. Znane są też inne przypadki podobnych błędów w systemach GPS, GLONASS itp.

Skutki błędów SVN23, nie różnią od symptomów spoofingu GPS i stanowią ten sam problem do rozwiązania. Aby wykryć taki błąd należy dysponować dostępem do innego źródła UTC nie obarczonego błędem. Takimi niezależnymi od GPS źródłami dysponują narodowe instytuty metrologii (NMI).



rys. 18 *Błąd 13.5 µs obserwowany w warunkach laboratoryjnych NMI*

Pokazane (na rys. 18) wyniki odchyleń 13.5µs testowanych laboratoryjnie w NMI różnych urządzeń odbiorczych GPS (kolor przyporządkowany jest konkretnemu urządzeniu) pokazują, że testowane odbiorniki i serwery GPS reagują z różnym opóźnieniem i bezwładnością na ten sam błąd SVN23. Wytwarza to nieoczekiwane dodatkowe różnice czasu między odbiornikami, które nie wystąpiłyby, gdyby odbiorniki były identyczne chociaż nadal podatne na błąd SVN23. Powyższe raz jeszcze skłania do przemyśleń nad budową rozwiązań, które mogłyby uzyskiwać wzorcowy czas UTC z niezależnych źródeł i niezależnymi od siebie metodami: GNSS, NMI (Ethernet), OSC.

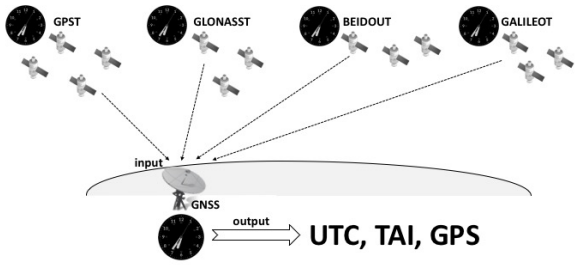
3. Wielosekundowa rozbieżność czasu między skalami GPST, GLONASST, BEIDOUT, GALILEOT[10]

Potocznie mówi się o „*czasie z GPS*", ale w praktyce prawie zawsze chodzi o skalę czasu UTC. Nieścisłe terminy i żargon mogą jednak prowadzić do błędu skutkującego wielosekundowymi rozbieżnościami w przedziale od 18 do 37 sekund, różniącymi od siebie skale czasu GPST, TAI od skali UTC.

Mało znanym faktem jest, że poszczególne systemy satelitarne grupy GNSS używają wewnętrznie różniących się od siebie o wiele sekund skal czasu[10]: GPST, GLONASST, BEIDOUT, GALILEOT (rozszerzenie T oznacza czas). Skale te bywają udostępniane jako opcja konfiguracji odbiorników komercyjnych. Źle skonfigurowane mogą udostępniać na wyjściu np. udostępniać czas na wyjściu (np. serwera PTP/NTP) z wielosekundowym błędem względem UTC (rys. 19).

[8] GNSS Inside (SVN23) http://www.insidegnss.com/node/4829
[9] BBC http://www.bbc.com/news/technology-35491962

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

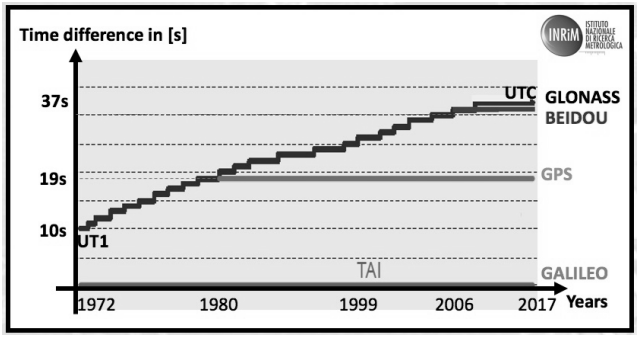


rys. 19 *Wyjściowy czas OUTPUT odbiornika i serwera GNSS może być wyrażony w skali UTC, TAI lub GPST*

Wynikowy czas UTC otrzymywany na wyjściu odbiornika satelitarnego, wyliczany jest w tym konkretnie odbiorniku. Odbiorniki (np. GPS) często traktowane są w sposób podobny do karty sieciowej LAN/WiFi, tzn. tak, jakby odbierały czas z satelity i przekazywały go dalej do systemu IT. Jest to duże uproszczenie.

Aby wyznaczyć prawidłowy czas UTC, odbiornik musi nie tylko odebrać i zdekodować informacje z satelity, ale też musi on uwzględnić szereg matematycznych poprawek, związanych z ruchem satelitów (np. dylatację czasu wynikającą ze szczególnej teorii względności, propagację mikrofal w atmosferze itp).

Ostateczna jakość (dokładność i precyzja) produkowanego przez odbiornik GNSS czasu UTC zależy od wbudowanego w firmware algorytmu, wydajności sprzętu (układów w.cz, procesora itp.) z jakiego zbudowano odbiornik, oraz od stabilności i precyzji wewnętrznego oscylatora. Odbierany cyklicznie, prawidłowo dekodowany sygnał satelitarny, jest przetwarzany i dostraja on wewnętrzny oscylator, który jest podstawą wyjściowego czasu w wybranej skali czasu (np. UTC). Odbiornik może zarówno faworyzować (np. GPS) lub umniejszać rolę poszczególnych systemów grupy GNSS zwiększając lub zmniejszając ich wagi podczas uśrednień wyznaczania UTC. Algorytm i wartości wag pozostają zawsze informacją poufną producenta i nie są podawane w specyfikacji technicznej komercyjnego odbiornika GNSS.



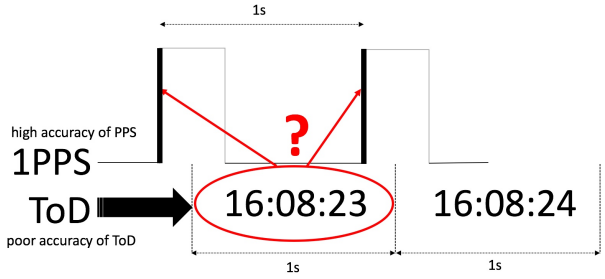
rys. 20 *Historyczna ewolucja zmian w różnicach czasu między poszczególnymi skalami GNSS (GPST, GLONASST, BEIDOUT, GALILEOT)*

Nie należy mniemać, że układ odbiorczy amerykańskiej firmy będzie używał jako wiodącego amerykańskiego systemu GPS, chociaż wydaje się z naturalnych powodów, że właśnie tak powinno być. W dobie globalizacji i międzynarodowych przejęć korporacyjnych, związek miejsca wytwarzania odbiornika i miejsca rejestracji firmy (właściciela), mogą wprowadzać w błąd i powodować niewłaściwe opinie. Błędy wynikające z różnic skal czasu GPST, GLONASST, BEIDOUT, GALILEOT (**rys. 20**) to kolejna możliwość prowadząca do wielosekundowych rozbieżności w synchronizowanej infrastrukturze.

4. Odbiorniki GNSS – błąd PPS

Wydawać by się mogło, że niemożliwe jest, by zabiegając o duże precyzje wyrażane w nanosekundach, mikrosekundach, milisekundach nie wpaść łatwo w pułapkę dużego błędu nawet *jednej sekundy* (stąd nazwa 1PPS).

Błąd *jednej sekundy* wiąże się z trudnością prawidłowego powiązania, dwóch wytwarzanych w odbiorniku GNSS sygnałów wyjściowych: 1PPS-out (częstotliwość) i informacji ToD-out (faza) referencyjnego wzorca czasu UTC (rys. 21).



rys. 21 *Który z sygnałów 1PPS (lewy czy prawy) prawidłowo określa początek znacznika ToD godziny 16:08:23*

Sygnał 1PPS (*puls per second*) jest bardzo precyzyjnym wzorcem wyznaczającym początek sekundy. Jest to odpowiednik wahadła w zegarze grawitacyjnym. Nie zawiera informacji o godzinie, minutach ani o liczbie sekund. Informację tę wskazuje drugi z wzorców - ToD (*time of a day*) i uzupełnia je informacją z kalendarza (rok, miesiąc, dzień).

Wzorzec 1PPS jest co najmniej o trzy rzędy wielkości precyzyjniejszy od informacji ToD, ale wyznacza jedynie początek sekundy, a ta musi być przypisana do prawidłowego znacznika ToD. Powodem możliwości powstawania *błędu sekundy* jest trudność przyporządkowania prawidłowego zbocza 1PPS właściwemu znacznikowi ToD (rys. 21). Związane z nim niepowodzenia synchronizacji i błędy rozbieżności czasu należy tłumaczyć słabą współpracą pomiędzy grupami IT i specjalistami ds. synchronizacji. Podczas gdy jedni zakładają bezbłędność zakupionych odbiorników GNSS, to drudzy uważają, że omawiany problem jest oczywisty i jasny dla każdego. Problem ten niestety nie omija najbardziej renomowanych firm i urządzeń.

5. Sekunda przestępna (*leap second*)

Powodem wprowadzania dodatkowej sekundy przestępnej (*leap second*) jest obserwowane od lat spowalnianie ruchu obrotowego Ziemi. Korekta pozwala utrzymać relację między skalą UTC (opartą o atomową skalę czasu TAI), a obserwowanym czasem słonecznym (UT1). Ostatnia 37 sekunda przestępna dodana była o północy UTC 31 grudnia 2016. W Polsce był już Nowy Rok 2017.

O decyzji dodania lub odjęcia sekundy przestępnej decyduje (i oznajmia o tym) z wielomiesięcznym wyprzedzeniem IERS (International Earth Rotation Service). Informacje publikowane są w formie piku *biuletynu C*[11]. Istnieją dwa dozwolone scenariusze dodania lub odjęcia sekundy przestępnej:

Scenariusz 1
30 czerwca godz.
23:59:60 UTC

Scenariusz 2
31 grudnia godz.
23:59:60 UTC

Formuła zależności skal UTC-TAI

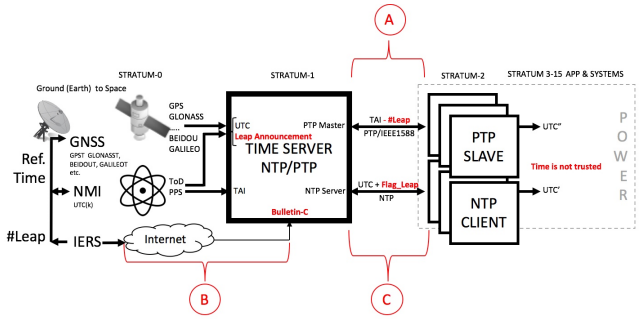
TAI - UTC
=
#Leap-Seconds

rys. 22 *Scenariusze zmian sekundy przestępnej oraz zależność TAI-UTC*

Istnieją też dwa zapasowe (3,4) nieużywane dotychczas scenariusze zmian z datami: 31 marzec i 30 wrzesień.

Protokół dystrybucji PTP/IEEE1588 przekazuje siecią jedynie składniki skali UTC w postaci: *czasu TAI* oraz liczby sekund (*#Leap-Seconds*), które należy odjąć od TAI, aby otrzymać czas UTC po stronie klienta (*slave PTP*). Synchronizowany klient PTP sam scala otrzymane protokołem PTP/IEEE1588 dane wg formuły pokazanej na rys. 22, i tym samym przekazuje na stronę PTP-Slave pełną odpowiedzialność za prawidłowe obliczenie ostatecznego czasu UTC w systemie klienckim. Może się to odbywać na poziomie interfejsu sieciowego, aplikacji (APP) lub we wnętrzu jądra systemu operacyjnego.

W każdym przypadku podejście takie wydaje się niebezpieczne i może prowadzić do powstawania sekundowych różnic czasu, wynikających ze zróżnicowanych metod wytracania sekundy przestępnej. Protokół PTP/IEEE1588 nie zapewnia też ochrony kryptograficznej przekazywanej siecią Ethernet informacji, co tworzy lukę bezpieczeństwa, powalającą na zmianę danych protokołu (np. parametru *#Leap_Scond*). Prawdopodobnie odporność na takie sytuacje nie jest brana pod uwagę w energetyce.



rys. 23 *Dystrybucja czasu UTC w sieci Ethernet. Słabe punkty, w systemie dystrybucji czasu z wykorzystaniem protokołów NTP i PTP (punkt A i C). Brak autentykacji plików Biuletynu-C (punkt B) pozwala na manipulację ilością sekund przestępnych. Strona kliencka może produkować różniące się od siebie czasy UTC' i UTC".*

Protokół NTP przekazuje gotowy do użycia czas UTC bez wyszczególniania składowych *TAI i #Leap_Sconds,* tak jak to robi PTP/IEEE1588. Protokół NTP anonsuje jedynie zmianę sekundy przestępnej, która ma nastąpić po to, aby przygotować system kliencki NTP do usunięcia lub wytracenia kolejnej nadmiarowej sekundy przestępnej.

Zapowiedzi sekund przestępnych mogą być dostarczone zarówno za pośrednictwem systemów satelitarnych GNSS, i poprzez sieć Ethernet TCP/IP (Biuletyn-C), jak i pośrednio przez flagę zapowiedzi w protokółach NTP i PTP/IEEE1588. Jednak w każdym przypadku za obsługę sekundy przestępnej odpowiedzialna jest strona klienta i jego system operacyjny lub firmware urządzenia. Możliwe są następujące sposoby obsługi sekundy przestępnej:

1) ***Cofnięcie czasu systemu klienckiego o 1 sekundę na koniec sekundy przestępnej***, a więc w nowej dobie UTC dwukrotnie wystąpi ta sama sekunda 00 zanim pojawi się sekunda 01,
2) ***Cofnięcie o 1 sekundę na początku sekundy przestępnej*** (podobnie jak w p.1 wyżej), ale powtórzona zostanie sekunda 59, zanim pojawi się nowa sekunda 00,
3) ***Zatrzymanie na 1 sekundę*** zegara klienckiego
4) ***Zatrzymanie zegara UTC przy jednoczesnym minimalnym zwiększaniu zawartości liczników i stempli czasu.*** *To płynne wytracanie jednej sekundy nie wywołuje skoków czasu.*

Systemy IT w energetyce pochodzące z różnych dekad różnią się metodami obsługi sekundy przestępnej (punkty 1-4). Może to spowodować powstanie błędu 2 sekundy przedziałach od 12 godzin przed do 12 godzin po północy UTC podczas obsługi sekundy przestępnej.

Brak kryptograficznego zabezpieczenia PKI pliku biuletynu C[12] wnosi ryzyko zamiany całego pliku wraz z danymi dotyczącymi liczby i harmonogramu zmian. Pozostawia to zasadniczą lukę w systemie bezpieczeństwa systemów IT wykorzystujących taki plik i może posłużyć do rozsynchronizowania całego systemu. Zawartość pliku jest wprawdzie zabezpieczona funkcją skrótu SHA, ale brak autentykacji PKI, np. w postaci cyfrowego podpisu kluczem prywatnym IERS, osłabia znacząco bezpieczeństwo synchronizacji. Z kolei brak uwierzytelnienia (*authentication*) protokołu PTP (IEEE1588) i fakt przekazywania protokołem informacji rozbitej na składowe *TAI i #Leap-Sec*, wywoła ten sam skutek: zmianę liczby sekund przestępnych.

Z wymienionych wyżej powodów prawidłowa i bezkolizyjna dla cyber-bezpieczeństwa obsługa sekundy przestępnej (*leap second*) pozostaje jednym z najtrudniejszych wyzwań informatyki, w tej i prawdopodobnie następnej dekadzie. Dlatego ważne jest wprowadzenie niezbędnych regulacji prawnych normujących zasady obsługi tej sekundy w systemach IT. Obsłudze sekundy przestępnej towarzyszyć może też szereg efektów ubocznych. Niektóre prowadzić mogą do niedeterministycznego zachowania się kontrolerów, a nawet całych systemów w energetyce. Ilustruje to przypadek opisany jako: https://access.redhat.com/solutions/154793).
Z kolei, destabilizację częstotliwości dystrybuowanej energii spowodowaną błędną obsługą sekundy przestępnej opisuje link: http://leapsecond.com/pages/mains/.

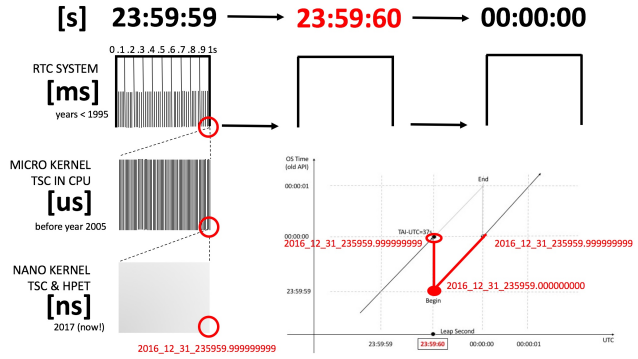
[11] IERS Biuletyn-C: ftp://hpiers.obspm.fr/iers/bul/bulc/

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

6. Destabilizacja systemu operacyjnego (firmwaru) z przetwarzania UTC na poziomie jądra OS

Czytelny format reprezentacji czasu i daty, znany z wyświetlaczy (rys. 24 górna część) formatowany jest w wyższych warstwach systemu operacyjnego.

Im bardziej zagłębiamy się w stronę jądra systemu (*OS kernel*), tym bardziej reprezentacja czasu przybiera kanoniczną postać unikalnego znacznika czasu reprezentowanego za pomocą liczby. Zmiana liczby odzwierciedla upływ czasu i za zmianę tę odpowiadają specjalne liczniki, które ściśle powiązane są z konkretną architekturą i sprzętem (systemów, kontrolerów PMU itp.).



rys. 24 Obsługa czasu we wnętrzu systemu operacyjnego. Cofnięcie zegara klienta wstecz (np. wstawienie sekundy przestępne replikuje zdarzenia, które nie powinny być wykonane dwukrotnie).

Czas w postaci znaczników ma mniej czytelną postać, ale za to pozwala na reprezentację czasu z bardzo dużą rozdzielczością i precyzją (rys. 24 lewa kolumna).

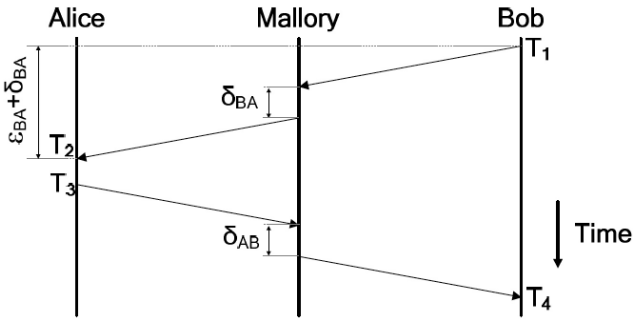
Zarządzanie procesami (współbieżność) i zadaniami (wielowątkowość) powiązane są ze znacznikami czasu. Podczas obsługi sekundy przestępnej, wskazanie obserwowane na wyświetlaczu jako 61 sekunda (rys. 24 górna środkowa kolumna na czerwono), we wnętrzu systemu operacyjnego OS obsługiwane jest inaczej.

System po przeskalowaniu cofa się w czasie powoduje powtórne wykonanie pewnej ilości znaczników (rys. 24 prawa dolna część – wykres). Może to spowodować niepożądane powtórne wykonanie czynności. W pewnych przypadkach jak np. w przypadku systemu Linux Redhat[12] może to zdestabilizować pracę całego systemu.

Problem jest znacznie szerszy niż obsługa sekundy przestępnej. Dotyczy wszelkich przestawień zegara poza wywołaniem API. Szczególnie niebezpieczne jest cofanie czasu systemowego. Zwracamy na to uwagę, ponieważ wydaje się, że taka czynność jest naturalna w procesie synchronizacji.

7. Atak wprowadzający opóźnienia *(Time Delay Attack)*

Firma Marvell[13] przedstawiła teoretyczny model ataku w sieci, polegającego na wprowadzeniu celowych opóźnień (rys. 25) pakietów synchronizacyjnych NTP i PTP na poziomie wędrówki *round trip*. Taki atak nie może być powstrzymany współczesnymi metodami ochrony bezpieczeństwa, ponieważ opóźnieniu podlegają nawet pakiety szyfrowane, a ich zawartość nie podlega żadnej modyfikacji. Prawdopodobnie jedyną skuteczną metodą przeciwdziałania może być w przyszłości kryptografia kwantowa całej infrastruktury sieci światłowodowej.



rys. 25 Mallory opóźnia przekazywanie pakietów synchronizacyjnych NTP/PTP pomiędzy Bobem (slave) a Alice (master)

UKRYTE SŁABE STRONY SYNCHRONIZACJI

Wizje lokalne istniejących instalacji GPS odsłoniły wiele niedoskonałości. Instalowane na dachach blisko urządzeń elektrycznych, bez pełnego widoku nieba, często blisko siebie, zmontowane na liniach instalacji odgromowych, zbyt liczne grupy anten GNSS nie tylko zakłócają wzajemnie swoją pracę, ale stanowią łatwy cel zagłuszaczy sygnałów satelitarnych GNSS. Przeprowadzone audyty systemowe pokazały obraz instalacji nieodpornych na zaniki sygnałów GPS (brak holdover). Problem stanowi też brak stałego jednoczesnego nadzoru operatorskiego wielu odbiorników satelitarnych. Niedoszkolony w zakresie dozoru i obsługi odbiorników personel wymaga okresowych szkoleń, ale przede wszystkim brakuje wdrożonych procedur postępowania w przypadkach braku synchronizacji i utraty synchronizacji. Niezbędne jest natychmiastowe sprawdzenie aktualnie posiadanej instalacji.

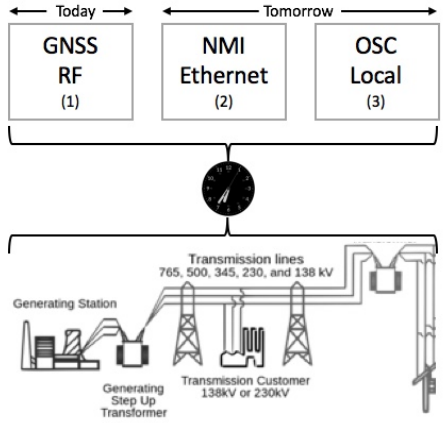
rys. 26 Przykład wadliwej *instalacji: odbiorniki zamontowane zbyt blisko siebie zakłócają się wzajemnie i dołączone są do instalacji odgromowych*

[13] Tal Mizrahi Marvel
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.720.6334&rep=rep1&type=pdf

POPRAWA SYNCHRONIZACJI

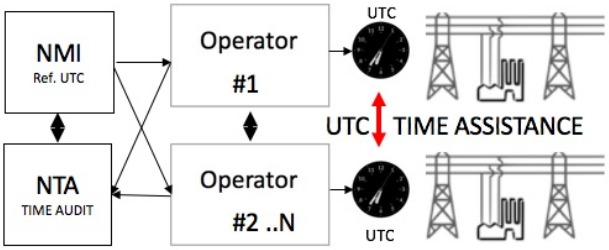
Aby zapewnić pewną synchronizację, potrzebne jest solidne, zaufane źródło czasu UTC i audytorski nadzór skuteczności synchronizacji po stronie aplikacji klienckich. Takie podejście będzie nabierało znaczenia w przyszłości w miarę zwiększania dokładności synchronizacji.

Bardzo ważne jest zapewnienie większej liczby niezależnych od siebie źródeł wzorcowego UTC, z których system może sam wybrać najlepsze i odrzucić błędne źródła. Dlatego trzeba tworzyć odporne na zakłócenia systemy, oceniające jakość otrzymywanego wzorca czasu, pochodzącego jednocześnie z: GNSS, NMI i lokalnych oscylatorów (rys. 27). Dla nowego europejskiego systemu satelitarnego GALILEO pojawia się ważna misja wzmocnienia roli GNSS, którą dziś współtworzą wojskowe systemy satelitarne GPS, GLONASS, BEIDOU.



rys. 27 *Model synchronizacji oparty o 3 grupy niezależnych dostawców czasu. Każda grupa posiada inną metodę dostawy czasu.*

Skutecznym, uzupełniającym dla GNSS i GALILEO źródłem UTC są narodowe instytuty metrologii (NMI). W Polsce rolę te pełni Główny Urząd Miar RP. Opublikowane w Dz.U 56/2004 (poz. 548) rozporządzenie Ministra Gospodarki określa sposoby dystrybucji wzorcowego czasu urzędowego UTC(PL), np. z użyciem serwerów NTP.

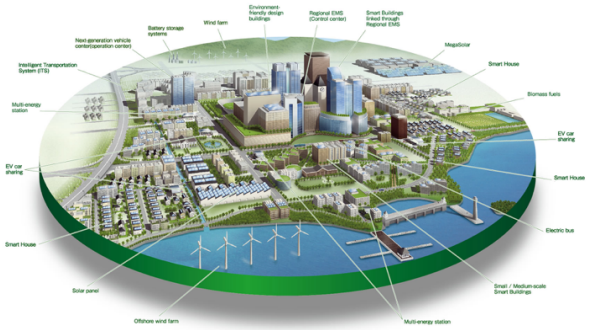


rys. 28 *Model dystrybucji i audytu czasu w systemie dystrybucji energii, którym poszczególni operatorzy wzajemnie dają sobie zapas czasu UTC*

Skale państwowe, do których zalicza się UTC(PL) zapewniają dokładność lepszą od 100 ns. Nowe możliwości synchronizacji jakie daje światłowodowy transfer czasu z użyciem protokołów takich jak *White Rabbit* i *PTPv3 profil „High-Accuracy”* pozwala synchronizować z dokładnością pojedynczych nanosekund. Te nowej jakości narzędzia o ile zostaną wdrożone, zasadniczo przyczynią się do poprawy bezpieczeństwa nie tylko w energetyce. Zapewniają one stałe i znacznie precyzyjniejsze źródła czasu UTC, niż GPS (GNSS). Okazuje się, że operując precyzjami na poziomie 10-20 ns uwidaczniają się różnice między całymi skalami państwowymi UTC(k). Czas UTC jest wyznaczany przez urzędy miar (NMI) retrospektywnie jako średnia ważona z poszczególnych wskazań zegarów atomowych. W efekcie żaden urząd nie zna aż z tak dużą dokładnością międzynarodowego czasu UTC i może on określić jedynie czas wg własnej skali narodowej UTC(k). Stąd połączenie światłowodowe urzędów metrologii NMI podobnie jak ich połączenie światłowodem z energetyką będzie odgrywać w przyszłości ważną rolę. Synchronizacja światłowodem nie zastąpi synchronizacji GNSS a jedynie ją rozszerzy o wzorce UTC dystrybuowane siecią.

W przyszłości dystrybutorzy energii sami będą zapewne organizować się i tworzyć własne centra zapasowe dystrybucji czasu UTC. Centra takie powinny powstawać we współpracy z NMI (w Polsce GUM) i pozostawać pod ich merytorycznym nadzorem. Centra będą wyposażone w wysokiej jakości zegary atomowe i serwery NTP/PTP, zapewniające zgodność synchronizacji z krajowymi wzorcami UTC(PL). Centra będą mogły jednocześnie pobierać czas z GNSS i NMI (rys. 27 rys. 28) oraz udzielać sobie wsparcia zapewniając wzajemnie zapas wzorcowego czasu UTC wysokiej jakości. Pierwsze takie systemy już powstają na świecie. Zaproponowany przez Elpromę serwis DEMETRA TSI#2 jest początkiem nowej ery rozwiązań synchronizacji jakie wzmacniają bezpieczeństwo systemów w energetyce.

Synchronizacja powinna też stać się składowym elementem strategii bezpieczeństwa energetycznego, mimo że awarie *balckout* wydarzają się rzadko. Świadomość ryzyka skutecznego cyber-ataku na infrastrukturę synchronizacji, która i tak z natury nie jest wolna od błędów (opisuje to niniejszy artykuł) daje nowe spojrzenie na bezpieczeństwo w energetyczne. Ryzyko destabilizacji synchronizacji w energetyce rośnie wraz z ewolucją współczesnych systemów energetycznych do postaci *Smart Grid* - inteligentnej sieci elektroenergetycznej, w której istnieje dwukierunkowa komunikacja między wszystkimi uczestnikami rynku energii. Ma ona na celu dostarczanie



rys. 29 Infrastruktura Smart Grid może wywołać efekt domina innych awarii

nowych usług energetycznych i telekomunikacyjnych, zapewniając obniżenie kosztu utrzymania infrastruktury. Ma też sprzyjać rozwojowi szerokorozumianej energii przyjaznej środowisku. *Smart Grid* pozwala jednocześnie dołączać do sieci odnawialne źródła. Może ona jednak uruchomić efekt domina, jeżeli nie zapewni się jej solidnej synchronizacji (*Robust Synchronization)*.

Bibliografia

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IEEE STANDARDS (*Power System Applications)*

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

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

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

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

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

[34] P. Tavella at All DEMETRA consortium formed by Aizoon, ANTARES, Deimos, ELPROMA, INRIM, Metec, NPL, ORB, Politecnico of Torino, Thales Alenia Space , UFE, Vega UK, and VTT, "Experimental Time Dissemination Services Based on European GNSS Signals: the H2020 DEMETRA Project", paper presented at The 30th European Frequency and Time Forum, April 2016.

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

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

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

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

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

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

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

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

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