11/2017 listopad
10,00 zł (w tym 5% VAT)

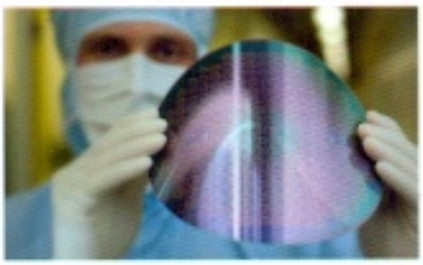
Wywiad: Witold Bereszczyński, dyrektor zarządzający w firmie Weidmüller – str. 26

ISSN 1248-4030
INDEKS 340 731

www.elektronikaB2B.pl

Elektronik

MAGAZYN ELEKTRONIKI PROFESJONALNEJ



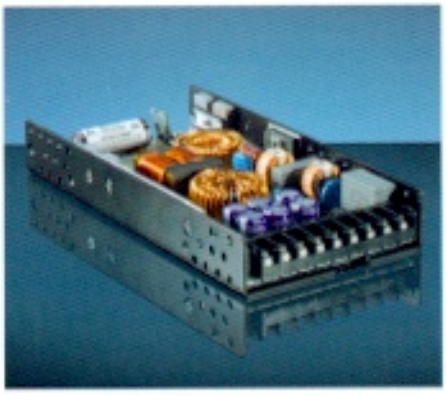
Krzem, krzemogerman, InGaAs, a może nanorurki węglowe, czyli przyszłość branży półprzewodników

Branża półprzewodnikowa wyróżnia się pozytywnie na tle innych gałęzi przemysłu tym, że już od ponad 50 lat rozwija się mniej więcej w jednakowym tempie. Bezsprzecznie z technologią krzemową dochodzimy do kresu gęstości upakowania układów scalonych w płaszczyźnie poziomej, ale rozwijają się technologie 3D. W artykule przyglądamy się kierunkom i zjawiskom determinującym rozwój technologii półprzewodnikowej. Patrz str. 21

W numerze

Urządzenia technologiczne do produkcji – infrastruktura dla rozwoju innowacji

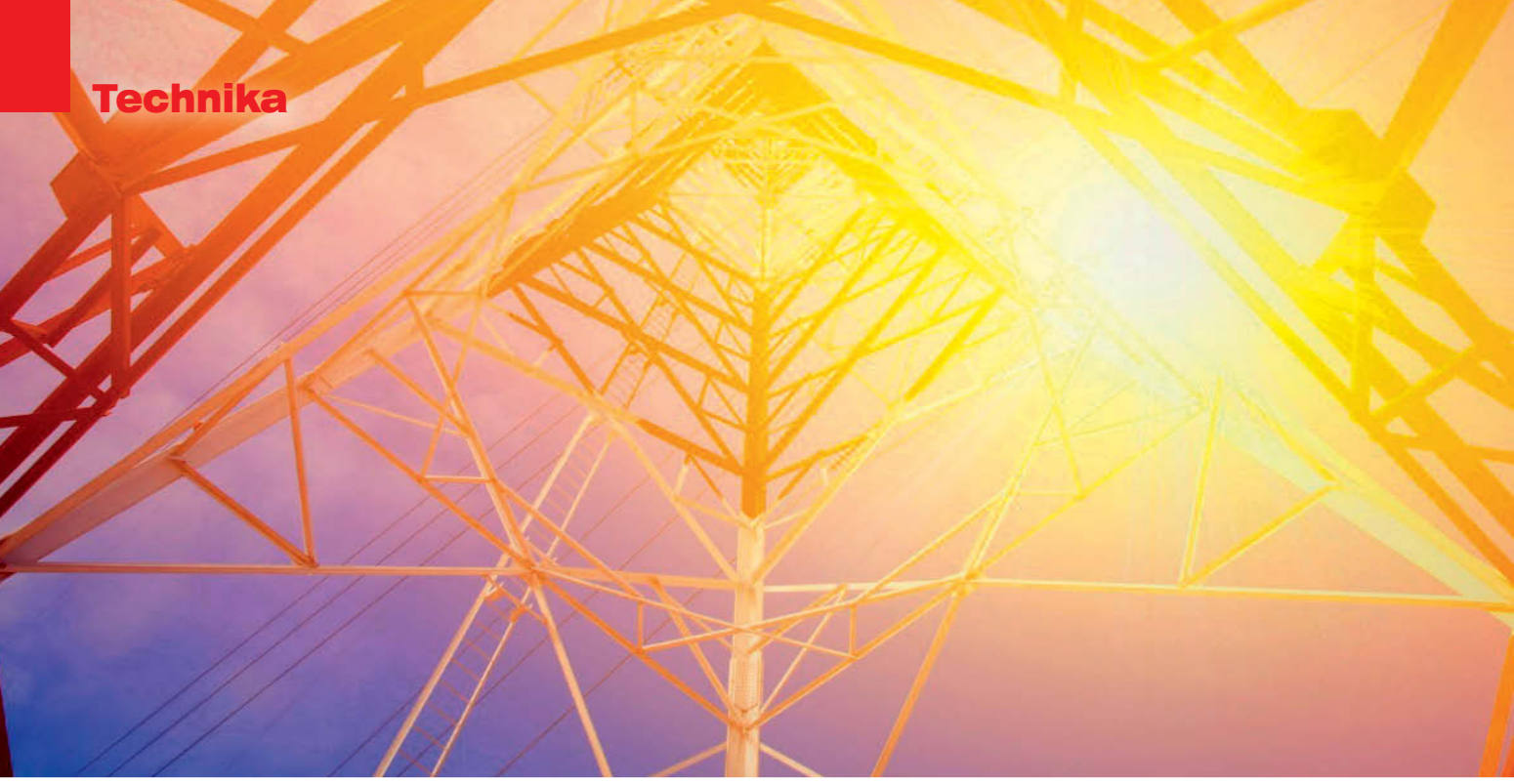
Rynek sprzętu produkcyjnego wykorzystywanego w produkcji elektroniki rozwija się dzisiaj w wielu kierunkach. Pierwszy to powstawanie nowych firm i rozbudowa biznesu istniejących graczy. Drugi kierunek rozwoju wynika ze zmian technologicznych, a więc miniaturyzacji urządzeń, coraz mniejszych komponentów, większej złożoności układowej, a także wzrostu znaczenia technologii mobilnych. Trzeci, to nowe otwarcia, takie jak oświetlenie LED, IoT, aplikacje smart cities. W naszym opracowaniu omawiamy zjawiska panujące na rynku, przedstawiamy firmy zajmujące się taką działalnością oraz analizujemy wszystkie istotne trendy. Patrz str. 30



Zasilacz – cyfrowy czy analogowy?

W urządzeniu elektronicznym od zawsze czymś oczywistym był analogowy zasilacz stabilizowany, a zasilacz cyfrowy bywa uważany za ekstrawagancję. W rzeczywistości technika cyfrowa poszerza dotychczasowe właściwości zasilacza. W artykule przedstawiamy błędne opinie, które często maskują korzyści z odpowiednio wykorzystanej do stabilizacji napięcia wyjściowego zasilaczy techniki cyfrowej. Patrz str. 76

Nowe kontrolery USB-C z wbudowanymi obwodami zabezpieczającymi – str. 68



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

W latach 2015-2017 firma Elproma uczestniczyła w międzynarodowym projekcie DEMETRA Horizon 2020. Projekt dostarczył 9 nowych usług synchronizacji, wspierających wdrażany przez UE system Galileo i był poprzedzony 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. Niniejszy artykuł przybliża problematykę synchronizacji i dystrybucji czasu.

Zgodnie z wymaganiami opisanymi w dokumentach IEEE, synchronizacja powinna zapewniać zgodny czas, tzn. pracę we wspólnej domenie czasowej (Time Domain) skali UTC oraz zapewnienie dokładności 1 µs przy założeniu maksymalnej liczby 16 przejść (hop) przez przełączniki i routery sieci Ethernet. Dokładność 1 µs jest niezbędna do zarządzania dystrybucją energii elektrycznej, która odbywa się poprzez pomiar kąta za pomocą urządzeń PMU (Phasor Measurement Unit) używających różniącej od UTC o 37 sekund skali czasu atomowego TAI. Zapewnienie aż 16 przejść hop nakłada konieczność zapewnienia 200 nanosekundowej precyzji na wyjściu serwera czasu. Warto jeszcze wspomnieć o pewnej poddziedzinie synchronizacji w energetyce, wymagającej dużych precyzji rzędu co najmniej 500 ns. Tak dokładny czas używany jest do pomiaru fali bieżącej (travelling wave) – reakcji na wzorzec, używanej do diagnozowania stanu linii przesyłowych i wskazywania miejsca uszkodzeń. Automatyczna kontrola dystrybucji energii, która jest podstawą nowoczesnych sieci smart grid, jest zagrożona cyberatakami na infrastrukturę synchronizacji, której skutkiem mógłby być np. blackout. Mimo, że prawdopodobieństwo skuteczności takiego ataku wydaje się nadal niewielkie, to znane obecnie nowe okoliczności podob-

nych wcześniejszych awarii wskazują zagrożenie za bardzo realne. Analiza East Coast Blackout (2003) wskazała jako jedną z ważnych przyczyn błąd związany z rozsynchronizowaniem systemu General Electric SCADA XA/21. Wywołało to zjawisko hazardu (skutek wyprzedził przyczynę) danych telemetrycznych otrzymywanych z PMU, a w konsekwencji wydano błędne decyzje, które doprowadziły do przeciążenia i efektu kaskady awarii na dużym obszarze od USA po Kanadę.

Z uwagi na takie ryzyko nowym wyzwaniem staje się ochrona infrastruktury energetycznej wrażliwej na skutki rozsynchronizowania.

Pięć grup ryzyka powstawania błędów synchronizacji czasu

W procesie transferu czasu ryzyko błędów synchronizacji, zarówno tych przypadkowych jak i będących wynikiem celowych działań, występuje w następujących etapach:

- transfer sygnału ziemia-kosmos, czyli błędy wewnętrzne GNSS (np. błąd 13,5 µs w GPS znany jako SVN23 który wystąpił w dniu 26/01/2016)
- transfer sygnału kosmos-odbiornik GNSS na Ziemi: zagłuszanie sygnałów GPS (Jamming), symulacja naziemna sygnałów GPS (Spoofing), brak obsługi sekundy przestępnej (Leap Second), błędy wewnętrzne odbiorników satelitarnych GNSS, wielosekundowe różnice skal czasu w systemach nawigacji,
- transfer Biuletynu-C publiczną siecią Internet bez zabezpieczeń kryptograficznych,
- transfer siecią Ethernet: wpływ asymetrii łączy na dokładność synchronizacji, celowe wprowadzanie opóźnień podczas przejść hop (np. Time Delay Attack),
- transfer siecią Ethernet (protokół PTP/IEEE1588): brak autentykacji przesyłanych protokołem danych, reprezentacja UTC w postaci składowych TAI i #Leap_Second), błędy ludzkie (ustawień konfiguracji, profili PTP itp.), błędy niezgodności (kompatybilności) PTP/IEEE1588, błędy skal czasu (reprezentacja: UTC, POSIX, TAI).

Wielkość błędu synchronizacji może się wahać w przedziale od nanosekund, aż po całe sekundy, a nawet dni i lata.

Przykładowe źródła błędów synchronizacji

Jamming, to możliwość lokalnego zagłuszania sygnałów GNSS przy pomocy niedrogich, ale bardzo skutecznych nadajników. Skuteczność zagłuszania zależy od ukształtowania terenu i budynków, lokalizacji anten serwerów czasu itp. Jeszcze nie tak dawno, niecałą dekadę temu, ich użycie w segmencie synchronizacji było sporadyczne. Obecnie używanie urządzeń zagłuszających rozpowszechnia się. Skuteczność zasięgu zagłuszaczy GNSS zależy od siły nadajnika. Gdy zegar wzorcowy nie ma 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 ma wbudowane wysokiej jakości oscylatory, to proces degradacji (tempo wzrostu błędu UTC) może zostać spowolniony lub zatrzymany do czasu przywrócenia odbioru sygnału satelitarnego GNSS.

GNSS spoofing 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.

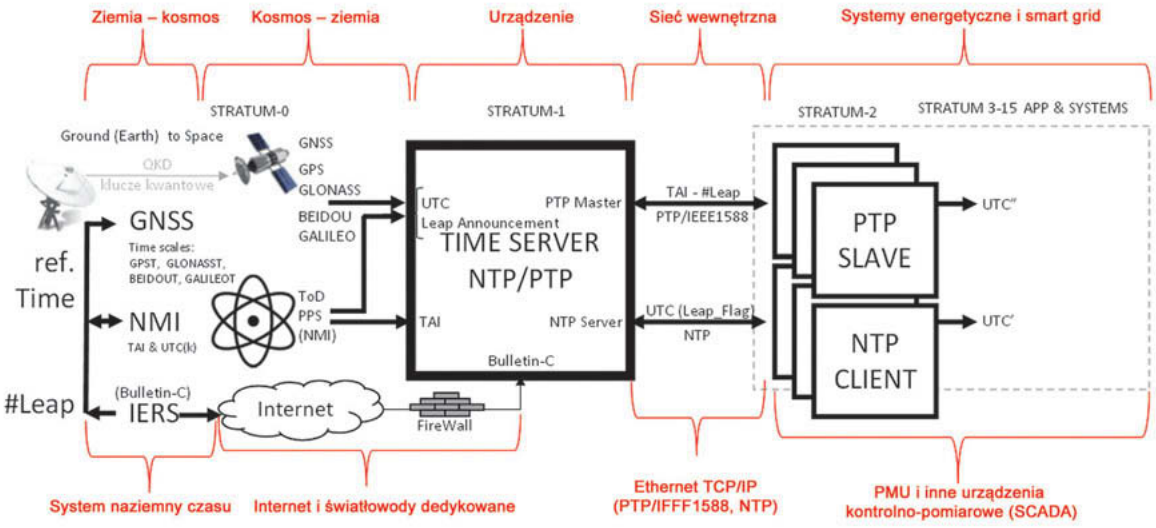
Słabe strony synchronizacji za pomocą GNSS

Wizje lokalne istniejących instalacji odbiorników satelitarnych wykorzystywanych do synchronizacji czasu w energetyce 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. Monitorowanie stanu pracy tak licznych odbiorników i anten nie jest możliwe i najczęściej pomijane w procedurach. Sprawdza się jedynie stan pracy urządzeń takich jak serwery NTP/PTP używające odbiorników GNSS w dalszym etapie transferu czasu.

Brakuje też redundancji serwerów NTP/PTP. Często produkty są niewłaściwie dobrane i nie mają oscylatorów lokalnych podtrzymujących czas UTC. Ponadto nie ma alternatywnych sposobów dostawy czasu światłowodem np. z narodowych instytutów metrologii (NMI).

Jakość odbiornika satelitarnego

Typowo wynikowy czas UTC otrzymywany na wyjściu odbiornika satelitarnego, wyliczany jest w tym konkretnie odbiorniku. Odbiorniki (np. GPS) często traktowane są w sposób podobny



Rys. 1. Pięć etapów dystrybucji czasu UTC w energetyce obarczonych zagrożeniem błędów i utraty synchronizacji

do karty sieciowej LAN/Wi-Fi, 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 wewnętrzny oscylator, który jest podstawą wyjściowego czasu w wybranej skali czasu. Odbiornik może zarówno faworyzować któryś z systemów (np. GPS) lub umniejszać rolę poszczególnych systemów grupy GNSS zwiększając lub zmniejszając ich wagi podczas uśrednień wyznaczania UTC w oparciu o wewnętrzne skale GPST itp. Algorytm i wartości wag pozostają zawsze informacją poufną producenta i nie są podawane w specyfikacji technicznej komercyjnego odbiornika GNSS. Zjawisko to może prowadzić do rozbieżności czasowych o wielkości nawet do 37 sekund!

Konieczne jest wiele źródeł synchronizacji

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. Istotne jest zapewnienie większej liczby niezależnych od siebie źródeł wzorcowego UTC, z których system może sam wybrać najlepsze i odrzucić błędne. Dlatego trzeba tworzyć odporne na zakłócenia czasu systemy, oceniające jakość otrzymywanego wzorca czasu, pochodzącego jednocześnie z: GNSS, instytutów metrologii i lokalnych oscylatorów. Dla nowego europejskiego systemu satelitarnego Galileo pojawia się ważna rola wzmocnienia GNSS, którą dziś współtworzą wyłącznie wojskowe systemy satelitarne GPS (USA), Glonass (Rosja), Beidou (Chiny). W Polsce rolę NMI pełni Główny Urząd Miar. Opublikowane w Dz.U. 56/2004 (poz. 548) rozporządzenie Ministra Gospodarki określa sposoby dystrybucji wzorcowego czasu urzędowego UTC (PL), np. z użyciem serwerów NTP. Skale państwowe, do których zalicza się UTC (PL) zapewniają dokładność lepszą od 100 ns.

Rys. 2. Przykład wadliwej instalacji anten

T. Widomski, K. Borgulski,
J. Użycki, P. Olbrysz, J. Kowalski
Elproma Elektronika

Elproma Elektronika sp. z o.o.
Szymanowskiego 13, 05-092 Łomianki
tel. 22 751 76 80, faks 22 751 76 81
info@elpromaelectronics.com
www.elpromatime.com