ELEKTRONIKA PRAKTYCZNA

EP.com.pl

● Międzynarodowy magazyn elektroników konstruktorów ● kwiecień ● 4/2026 ●

Tylko Prenumeratorzy

- mają dostęp do artykułów przed ich publikacją w EP na www.ep.com.pl – **EP W TOKU**
- mają dostęp do materiałów dodatkowych, takich jak pliki źródłowe projektów na naszym serwerze **FTP** www.ulubionykiosk.pl/media

ELEKTRONIKA W SYSTEMACH PŁATNICZYCH

TEMAT NUMERU

inspirujące, użyteczne projekty

• Prosty odtwarzacz audio • Zasilacz warsztatowy • Drivery magistral szeregowych RS232, RS422, RS485 zgodne z Grove

podzespoły, sprzęt, aplikacje

• Wydajne mikrokontrolery, zintegrowane peryferia – recepta na wyzwania projektowe nowoczesnych systemów wbudowanych • Elektronika w systemach płatniczych • *Si vis pacem, para bellum cum intelligentia artificiali*. Jeśli chcesz pokoju, szykuj się do wojny z użyciem AI • Moduły SoC i SoM w elektronice

tutoriale

• Kondensatory tantalowe • Płynna regulacja poziomu głośności

kursy

• Programowanie w środowisku MicroPython. Komunikacja przez ESP-NOW • Pomiary charakterystyk częstotliwościowych. Obwody w.cz.

TEMAT SPECJALNY

Elektronika na froncie

SOM, SOC, SBC I NIE TYLKO

ISSN 1230-3526 Indeks 357677

9 771230 352269 04

20 zł (w tym 8% VAT)

nr 4/2026 • PRICE: 8 EUR

prenumerata

–15%
NA START
170 zł

–30%
po pierwszym roku prenumeraty
140 zł

–40%
po drugim roku prenumeraty
120 zł

–50%
po trzecim roku nieprzerwanej prenumeraty
100 zł

Odkryj korzyści z prenumeraty drukowanej – większe oszczędności z każdym rokiem!

Rozpocznij swoją przygodę z *Elektroniką Praktyczną*. Decydując się teraz na roczną prenumeratę drukowaną, otrzymasz nie tylko dostęp do najnowszych wydań, ale i **znakomity start dzięki zniżce 15%** na pierwsze zamówienie!

Prenumerata to nie tylko wygoda dostępu do treści, ale także sposób na znaczące oszczędności. Dołącz do grona naszych stałych Czytelników i ciesz się coraz lepszymi warunkami.

Im dłużej jesteś z nami, tym więcej oszczędzasz:
- po roku nieprzerwanej prenumeraty zapewnimy Ci **30% rabatu** na kolejny rok,
- po dwóch latach wierności zaoferujemy **40% rabatu**,
- po trzech latach lojalności osiągniesz **najwyższy poziom rabatu – 50%!**

Jak otrzymać rabat za lojalność?
Zaloguj się na swoje konto prenumeratora na **www.UlubionyKiosk.pl** i zamów prenumeratę, korzystając z przycisku PRZEDŁUŻ w zakładce „Prenumeraty".

Przeglądaj wcześniej, płać mniej – postaw na e-prenumeratę!

Wybierz prenumeratę cyfrową PDF i ciesz się dostępem do czasopisma nawet 7 dni przed oficjalną premierą w kioskach. Oszczędzaj czas i pieniądze – skorzystaj z **rabatu 30%** na roczną e-prenumeratę w cenie 112 zł.

Dodatkowa oferta dla prenumeratorów wersji drukowanej: jeśli już subskrybujesz wersję papierową, możesz dokupić równoległe e-wydania w cenie 32 zł/rok – z niesamowitym **rabatem 80%**.

Zyskaj nieograniczony dostęp do zasobów dla pasjonatów elektroniki!

Tylko Prenumeratorzy mają pełny dostęp do:
- artykułów przed ich publikacją w *Elektronice Praktycznej* na www.ep.com.pl – EP W TOKU
- materiałów dodatkowych (takich jak pliki źródłowe projektów) na www.UlubionyKiosk.pl/media

Zamów prenumeratę drukowaną lub e-prenumeratę na www.UlubionyKiosk.pl lub przez przelew na konto Wydawnictwa AVT, a po zaksięgowaniu wpłaty wyślemy Ci mailowo kod dostępu do portalu.

Zacznij korzystać z pełnych zasobów już dziś!

Zamów prenumeratę lub e-prenumeratę na www.UlubionyKiosk.pl/prenumerata
tel. 22 257 84 22 (godz. 10–14) | prenumerata@avt.pl | AVT Korporacja sp. z o.o. ul. Leszczynowa 11, 03-197 Warszawa
rachunek bankowy: 18 1050 1012 1000 0024 3173 1013

Powrót do marzeń

W chwili, w której kwietniowy numer „Elektroniki Praktycznej” trafia do drukarni, misja Artemis II trwa w najlepsze. Gdy tuż po północy 2 kwietnia oglądałem transmisję ze startu w czasie rzeczywistym, naszła mnie pewna refleksja – z punktu widzenia elektronika istota tego niezwykle ważnego wydarzenia nie sprowadza się do samego (cokolwiek widowiskowego) startu ani też do faktu, że po przeszło pięciu dekadach ludzkość powraca w pobliże Księżyca. Dla mnie to przede wszystkim demonstracja tego, czym dziś jest elektronika kosmiczna: skrajnie niezawodna, redundantna, odporna na błędy i zaprojektowana tak, by działać w środowisku, w którym nie ma miejsca ani na serwis, ani na wymianę na drugi egzemplarz urządzenia.

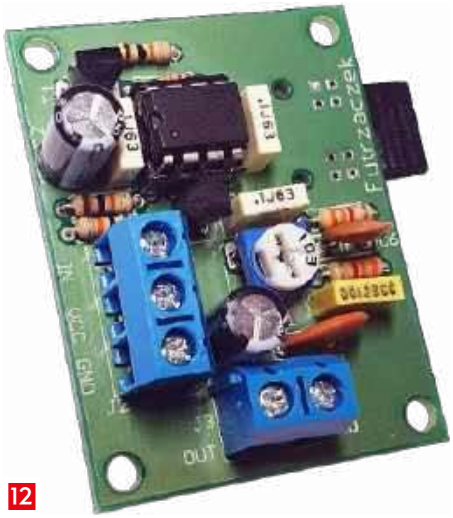
Przez dziesięciolecia loty załogowe kojarzyły się głównie z potęgą wielkich silników rakietowych, masywnymi osłonami termicznymi i mechaniką wielkich struktur odpowiedzialnych zarówno za konstrukcję statku, jak i infrastrukturę naziemną. Tymczasem w programie Artemis równie ważny jest inny wymiar tej technologii – niewidoczna na pierwszy rzut oka warstwa elektroniki pokładowej. Orion nie jest po prostu kapsułą, lecz złożonym systemem awioniki, sensorów, magistral komunikacyjnych, układów zasilania i komputerów zarządzających lotem. W oficjalnych materiałach NASA podkreśla, że „mózgiem” statku są dwa komputery Vehicle Management Computer opracowane przez firmę Honeywell, a każdy z nich zawiera dwa redundantne moduły obliczeniowe FCM (Flight Computer Module), co daje łącznie aż cztery nadmiarowe tory sterowania. W porównaniu z epoką Apollo oznacza to nie tylko wzrost mocy obliczeniowej, ale przede wszystkim jakościową zmianę filozofii projektowania: dziś niezawodność nie wynika z (miejscami wręcz topornej) prostoty, lecz z doskonale kontrolowanej złożoności, deterministycznej komunikacji i rozbudowanej diagnostyki pokładowej. O znaczeniu tej ostatniej nietrudno było zresztą przekonać się tuż przed startem rakiety SLS – wszak nieznaczne opóźnienie wynikało właśnie z konieczności szybkiego zdiagnozowania problemu zgłoszonego przez jeden z podsystemów. Dopiero po wielokrotnych potwierdzeniach od wszystkich kontrolerów odpowiedzialnych za misję, że systemy przez nich nadzorowane są w pełnej gotowości, dowódca wydał rozkaz uruchomienia odliczania ostatnich 10 minut przed zapłonem silników.

Szczególnie interesujące jest to, że Orion porusza się w przestrzeni, w której klasyczna nawigacja satelitarna przestaje być oczywistym punktem odniesienia. Dlatego system GN&C (oprócz samych odbiorników GPS) zawiera także zestaw wyspecjalizowanych czujników: inercyjne jednostki pomiarowe (IMU), trackery optyczne do śledzenia gwiazd, kamerę Optical Navigation (OpNav) obserwującą Ziemię i Księżyc czy też sensory słoneczne. NASA zwraca uwagę, że większość tych podsystemów jest zwielokrotniona, aby zwiększyć niezawodność, a oprogramowanie pokładowe stale zestawia dane z wielu źródeł, wyznaczając położenie, orientację i trajektorię lotu. To właśnie taka wielowarstwowa fuzja danych stanowi dziś sedno elektroniki kosmicznej: nie pojedynczy czujnik, lecz architektura, która potrafi rozpoznać rozbieżność, odrzucić błędny sygnał i utrzymać sterowanie statkiem nawet mimo częściowych uszkodzeń. Nie mniej wymowna jest sama sieć komunikacyjna Oriona. W jego awionice zastosowano TTEthernet – deterministyczną odmianę Ethernetu, która pozwala przesyłać jedną infrastrukturą zarówno dane krytyczne czasowo, jak i ruch mniej istotny. Według TTTech rozwiązanie to łączy blisko 50 punktów komunikacyjnych i pracuje z przepływnościami do 10/100/1000 Mbit/s. W świecie elektroniki kosmicznej nie chodzi tu jednak o imponujące liczby same w sobie, lecz o coś ważniejszego: o gwarantowany czas dostarczenia informacji, przewidywalność pracy i możliwość budowy systemu, który nie „zawiesza się” w klasycznym sensie, tylko przechodzi do wcześniej zdefiniowanego, bezpiecznego stanu. Warto też pamiętać, że Artemis nie jest wyłącznie amerykańską opowieścią o powrocie na Księżyc. To projekt międzynarodowy, a europejski moduł serwisowy ESM dostarcza Orionowi napęd, wodę, powietrze, kontrolę termiczną i zasilanie. ESA podkreśla, że przy jego budowie instalowano kilometry kabli, elementy elektroniki pokładowej i liczne podsystemy opracowywane w wielu krajach europejskich. To ważny sygnał również dla nas: współczesna elektronika kosmiczna jest wynikiem pracy całych łańcuchów kompetencji, rozciągniętych od laboratoriów sensorycznych, przez firmy projektujące elektronikę wysokiej niezawodności, po integratorów systemów awionicznych. Polski akcent w tym obrazie nie jest przy tym symboliczny. Już w bezzałogowej w misji Artemis I na pokładzie Oriona znalazły się detektory podczerwieni firmy VIGO Photonics, pracujące w systemie monitorowania składu atmosfery kabiny i skafandrów, a zespół z Instytutu Fizyki Jądrowej PAN dostarczył detektory promieniowania jonizującego do badań dawek poza niską orbitą okołoziemską. To są właśnie te miejsca, w których elektronika z Polski styka się z najbardziej wymagającym frontem technologii: pomiarami gazów oddechowych, detekcją promieniowania, aparaturą naukową czy systemami bezpieczeństwa załogi. Polska nie jest już tylko obserwatorem programu kosmicznego – coraz częściej staje się dostawcą konkretnych rozwiązań aparaturowych i uczestnikiem ambitnych przedsięwzięć technologicznych. Artemis przypomina więc, że podbój przestrzeni kosmicznej nie zaczyna się ani na wyrzutni, ani nawet w centrum kontroli lotów. Zaczyna się znacznie wcześniej: na poziomie projektu płytki, architektury magistrali, doboru procesora, odporności czujnika, budżetów mocy zasilania i łącza danych, protokołów telemetrii czy wielopoziomowych procedur obsługi błędów. I właśnie dlatego elektronika kosmiczna należy dziś do najbardziej fascynujących obszarów naszej branży. Bo tam każdy bit, każdy pomiar i każdy układ scalony naprawdę mają znaczenie.

Przemysław Musz

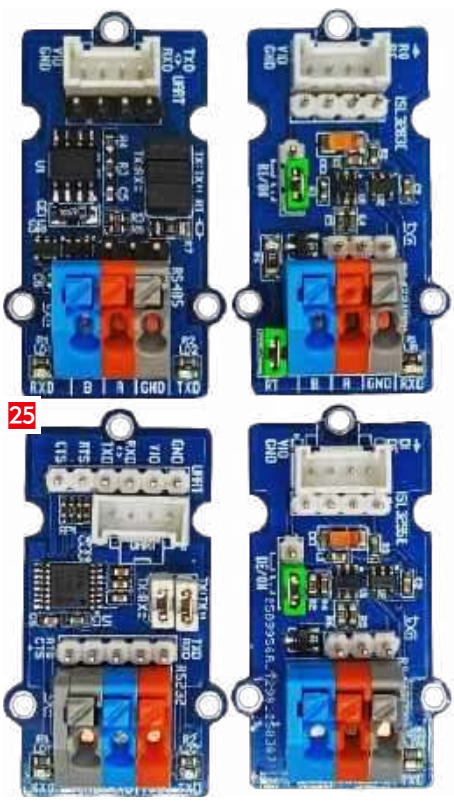
ELEKTRONIKA PRAKTYCZNA

nr 4 (398) • kwiecień 2026



12

16



25

Praca z 5 V w każdych warunkach

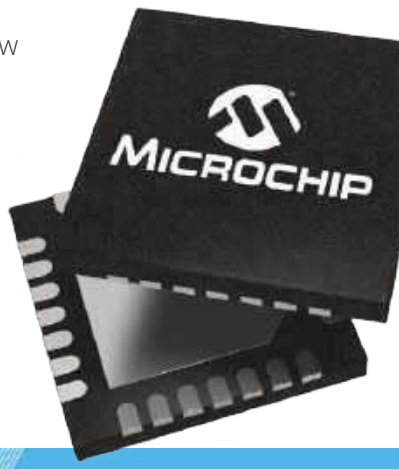
Wydajność bez strat energii

Mikrokontrolery PIC32CM PL10 na nowo definiują możliwości dla inżynierów poszukujących idealnej równowagi między prostotą a wydajnością. Jednostki te bazują na rdzeniu ARM Cortex-M0+ i zapewniają pracę przy zasilaniu 5 V, co jest cechą rzadko spotykaną wśród 32-bitowych mikrokontrolerów, gwarantując wyjątkową odporność na zakłócenia w zastosowaniach przemysłowych, AGD i motoryzacyjnych. Dzięki zaawansowanemu wykrywaniu dotyku, wyjątkowo niskiemu zużyciu energii i bezproblemowej obsłudze znanych narzędzi programistycznych, PIC32CM PL10 łączą prostotę i wydajność z solidną pojemnościową obsługą dotyku i niezawodny, działaniem przy zasilaniu 5 V.

Kluczowe cechy

- Działanie przy zasilaniu 5 V: Niezawodność i wydajność w obecności zakłóceń
- Zaawansowane wykrywanie dotyku: Peryferyjny kontroler dotykowy obsługuje dużą liczbę kanałów i jest odporny na zakłócenia
- Tryby ultraniskiego poboru mocy: Funkcja sleepwalking i mały prąd pobierany w trybie czuwania wydłużają żywotność baterii
- Łatwa migracja: Zaprojektowany dla użytkowników 8-bitowych, umożliwiając bezproblemową aktualizację
- Znane narzędzia programistyczne: Zgodne z Microsoft® Visual Studio Code (VS Code®) i MPLAB® Code Configurator oraz obsługiwane przez partnerskie łańcuchy narzędzi, takie jak IAR Embedded Workbench, Keil i Segger.
- Konkurencyjna cena: Zaawansowana funkcjonalność bez dodatkowych kosztów

Ulepsz swój kolejny projekt dzięki mikrokontrolerowi PIC32CM PL10 i ciesz się 32-bitową wydajnością bez dodatkowej komplikacji układu.

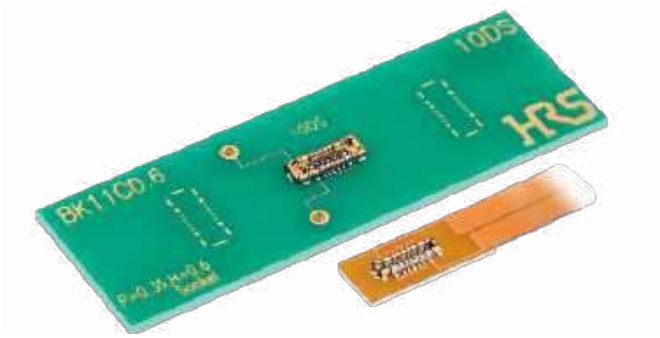


MICROCHIP

microchip.com/pic32cm-pl10

nowe podzespoły

Z kilkuset nowości wybraliśmy te, których nie wolno przeoczyć. Bieżące nowości można śledzić na www.elektronikaB2B.pl



Miniaturowe złącza o prądzie przewodzenia do 4 A do łączenia taśm FPC z płytką drukowaną

Złącza z nowej serii BK11 firmy Hirose są przeznaczone do łączenia elastycznych taśm FPC z płytką drukowaną w urządzeniach przenośnych o ograniczonej przestrzeni montażowej. Charakteryzują się rastrem 0,35 mm, wysokością (po złączeniu) wynoszącą 0,6 mm oraz całkowitą szerokością 1,9 mm. Są złączami hybrydowymi, umożliwiającymi jednoczesne doprowadzenie zasilania i sygnałów sterujących do kilku modułów z wykorzystaniem jednego połączenia.

Złącza BK11 zawierają 2 główne styki zasilania o obciążalności prądowej po 4 A, 4 pomocnicze styki zasilania o obciążalności po 2,5 A oraz styki sygnałowe o obciążalności po 0,3 A. Maksymalna rezystancja styku wynosi 30 mΩ w przypadku torów zasilania i 50 mΩ dla torów sygnałowych, natomiast minimalna rezystancja izolacji pomiędzy stykami to 50 MΩ.

Konstrukcja mechaniczna została wzmocniona poprzez zastosowanie prowadnic metalowych, chroniących korpus przed uszkodzeniem w trakcie łączenia. Zakres samonaprowadzania, wynoszący do ±0,32 mm, ułatwia prawidłowe pozycjonowanie przy montażu automatycznym i ręcznym. Mechanizm blokujący generuje wyczuwalne kliknięcie po pełnym złączeniu, co pozwala jednoznacznie potwierdzić poprawne połączenie elektryczne. Zarówno wtyk, jak i gniazdo zawierają po 3 pola lutownicze dla każdego głównego styku zasilania, co zwiększa odporność połączenia na odrywanie padów od laminatu.

Złącza BK11 są przystosowane do pracy w szerokim zakresie temperatur otoczenia od –55 do +85°C. Są odporne na udary mechaniczne do 49 g (11 ms), a ich trwałość mechaniczną producent określa na 10 cykli łączenia.

www.hirose.com

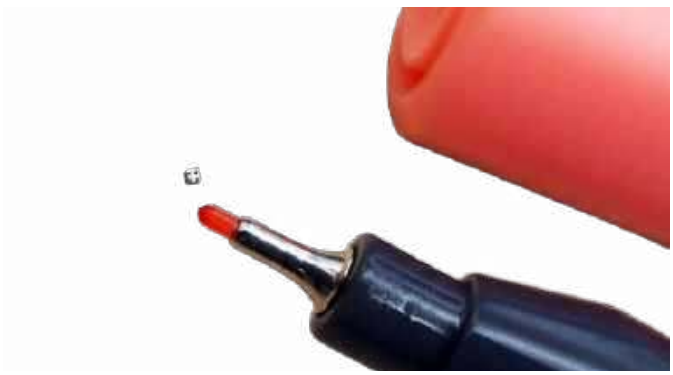
Przetworniki elektroakustyczne o grubości od 2 mm do zastosowań w słuchawkach

Same Sky rozszerza ofertę przetworników elektroakustycznych przeznaczonych do zastosowań w słuchawkach. Miniaturowe przetworniki z serii CMR są produkowane w 11 wariantach o poziomie ciśnienia akustycznego od 103 dB do 135 dB i częstotliwości rezonansowej od 100 Hz do 550 Hz. Charakteryzują się małą powierzchnią, wynoszącą od 12×6 mm i grubością zaledwie 2 mm.

W ofercie producenta są dostępne warianty okrągłe (fot.) i prostokątne, wyposażone w pola lutownicze do montażu SMT lub styki sprężynujące, co pozwala na bezpośredni montaż na płytkach drukowanych bądź w gniazdach. Producent oferuje różne typy membran o charakterystyce akustycznej dopasowanej do konkretnego projektu.

Przetworniki CMR są produkowane w zakresie mocy znamionowej od 3 mW do 200 mW. Ich impedancja znamionowa może wynosić 16 Ω, 30 Ω, 32 Ω lub 50 Ω, co pozwala na zastosowania zarówno we wzmacniaczach słuchawkowych, jak i w aplikacjach o wyższym napięciu wyjściowym. Wybrane modele, w tym CMR-3466-1050SP-X7, CMR-12062S-67 i CMR-15062S-67, charakteryzują się stopniem ochrony IPX7 świadczącym o odporności na wilgoć i krótkotrwałe zanurzenie w wodzie. Ponadto niektóre modele zawierają demontowalną osłonę do ochrony membrany przed uszkodzeniami mechanicznymi i zanieczyszczeniami.

www.sameskydevices.com



Miniaturowe rezonatory MEMS 32...76,8 MHz o wysokiej odporności na udary i wibracje

Nowa platforma Titan firmy SiTime obejmuje rezonatory MEMS, zrealizowane w technologii FujiMEMS 6. generacji. Są one produkowane w obudowach 0505 CSP (0,46×0,46 mm), co oznacza przynajmniej 4-krotną redukcję powierzchni montażowej w porównaniu z powszechnie stosowanymi, miniaturowymi rezonatorami kwarcowymi. Oferta obejmuje zarówno warianty do montażu na płytce drukowanej, jak i wersje typu „bare die", przeznaczone do integracji

w układach SoC lub mikrokontrolerach – takie rozwiązanie pozwala zredukować liczbę elementów dyskretnych w projekcie.

Rezonatory Titan pobierają moc zasilania mniejszą nawet o połowę, a ich czas rozruchu został skrócony o około 66% w porównaniu do rezonatorów kwarcowych. Ponadto wykazują one znacznie lepszą stabilność częstotliwości w długim okresie użytkowania. Producent gwarantuje utrzymanie parametrów katalogowych przez 5 lat przy pracy w maksymalnej dopuszczalnej temperaturze otoczenia.

Pozostałe właściwości:

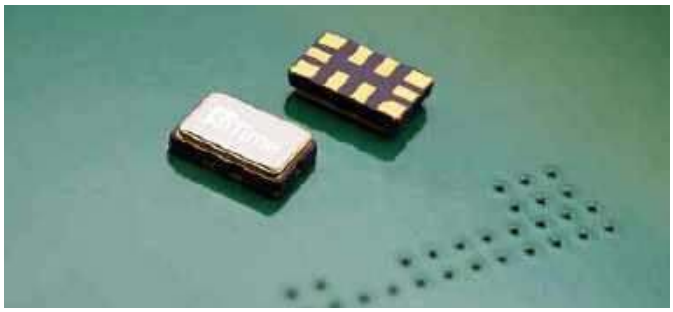
- nawet 50-krotnie większa odporność na udary i wibracje w porównaniu do oscylatorów kwarcowych,
- wersje o częstotliwości nominalnej od 32 MHz do 76,8 MHz,
- zakres temperatury roboczej od –40 do +125°C.

www.sitime.com

750-woltowe tranzystory CoolSiC MOSFET G2 w nowych obudowach Q-DPAK i D2PAK

750-woltowe tranzystory CoolSiC MOSFET G2 są teraz dostępne w nowych obudowach Q-DPAK i D2PAK, pozwalających zredukować rezystancję RDS(ON) nawet do 4 mΩ. Są to tranzystory umożliwiające uzyskanie rekordowej sprawności i gęstości mocy w aplikacjach przemysłowych i motoryzacyjnych, takich jak ładowarki pokładowe, wysokonapięciowe konwertery DC/DC i przełączniki zasilania. Obudowa Q-DPAK typu top-side cooled pozwala uzyskać równocześnie małą rezystancję termiczną i długi czas bezawaryjnej pracy, zaś niewielkie wartości iloczynów RDS(ON) × QOSS i RDS(ON) × Qfr zapewniają małe straty przy przełączaniu, zarówno w topologii hard-switching, jak i soft-switching. Napięcie progowe VGS(th) równe 4,5 V @ +25°C i bardzo mały stosunek QGD/QGS zapewniają wysoką odporność na przypadkowe włączenie tranzystora, wynikające z wpływu parametrów resztkowych. Bramki mogą pracować z napięciem statycznym już od –7 V (do –11 V w impulsie), co poszerza marginesy projektowe i zapewnia kompatybilność z wieloma podobnymi tranzystorami dostępnymi obecnie na rynku.

www.infineon.com



Precyzyjny oscylator Super-TCXO do systemów lokalizacji, nawigacji i synchronizacji

ENDR-TTT to skompensowany termicznie oscylator Super-TCXO, przeznaczony do zastosowań w systemach lokalizacji, nawigacji i synchronizacji czasu (PNT), w tym w lotniczych, wojskowych i przemysłowych odbiornikach GNSS. Został zaprojektowany z myślą o zapewnieniu długiej pracy w trybie holdover, czyli utrzymania dużej dokładności przy braku sygnałów GNSS, a także wyróżnia się dużą odpornością na zakłócenia i próby spoofingu.

ENDR-TTT wykazuje stabilność częstotliwości ±50 ppb w całym zakresie temperatury pracy od –55 do +125°C. Jego czułość

na przyspieszenie wynosi 0,004 ppb/g, co jest wynikiem znacznie lepszym od osiągów typowych oscylatorów kwarcowych, umożliwiając zachowanie dużej dokładności w środowiskach o silnych wibracjach. Układ jest odporny na udary mechaniczne do 30 000 g. Bardzo dobra stabilność długoterminowa (±0,5 ppm w ciągu 20 lat) eliminuje konieczność przeprowadzania kalibracji. Częstotliwość wyjściowa może być dostrajana przez interfejsy I²C i SPI.

Dzięki zastosowaniu architektury MEMS, ENDR-TTT wykazuje nawet 20-krotnie dłuższy holdover oraz 20-krotnie wyższą dokładność w porównaniu z tradycyjnymi oscylatorami kwarcowymi. Umożliwia to ograniczenie szerokości pętli śledzenia sygnału GNSS, zwiększając odporność na spoofing. Jeśli chodzi o aplikacje militarne i lotnicze, ENDR-TTT może znaleźć zastosowanie w bezzałogowych pojazdach powietrznych, systemach kierowania pocisków, pojazdach wojskowych, radiokomunikacji oraz satelitach niskoorbitalnych. Aplikacje przemysłowe obejmują systemy synchronizacji sieci energetycznych, robotykę, eksplorację podwodną i górnictwo.

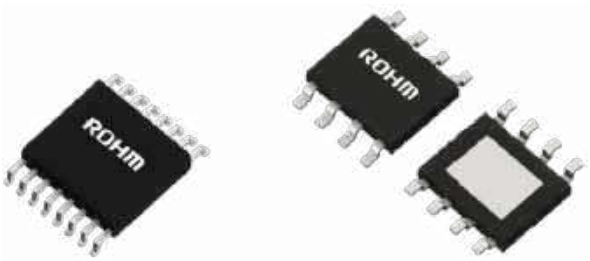
www.sitime.com

Precyzyjny enkoder przyrostowy o dokładności pozycjonowania 0,1°

Firma Faulhaber rozszerza ofertę o nowy enkoder przyrostowy o bardzo wysokiej rozdzielczości i powtarzalności, mogący znaleźć zastosowanie m.in. w metrologii, urządzeniach optycznych (mikroskopy, teleskopy) oraz automatyce i robotyce. Ze względu na optyczną metodę pomiaru, model IERF3 L jest niewrażliwy na zaburzenia elektromagnetyczne. Zapewnia dokładność pozycjonowania 0,1° i powtarzalność równą 0,007°. Pracuje z napięciem zasilania 4,5...5,5 V, pobierając około 45 mA prądu, a jego zakres dopuszczalnej temperatury pracy rozciąga się od –40 do +100°C.

Model IERF3 L jest dostępny w trzech rozmiarach (∅ 22 mm, ∅ 32 mm i ∅ 42 mm) i charakteryzuje się małą grubością, wynoszącą 6,2 mm. Został zoptymalizowany do współpracy z miniaturowymi, płaskimi silnikami BLDC z rodziny BXT. Standardowo zawiera sterownik liniowy z wyjściem komplementarnym, a opcjonalnie może być wyposażony w hamulec.

www.faulhaber.com



Sterowniki szczotkowych silników DC do pracy w sprzęcie AGD i urządzeniach biurowych

BD60210FV i BD64950EFJ to sterowniki szczotkowych silników DC, przeznaczone do sterowania pracą wentylatorów, zaworów, mechanizmów przesuwu i szczotek w urządzeniach AGD i sprzęcie biurowym. Mogą też znaleźć zastosowanie w prostych aplikacjach przemysłowych, obejmujących sterowanie drzwiami automatycznymi, roletami czy niewielkimi przenośnikami.

Układ BD60210FV jest przystosowany do pracy z napięciem zasilania od 8 V do 18 V i zawiera dwa wewnętrzne mostki, umożliwiające sterowanie dwoma niezależnymi silnikami. Taka konfiguracja pozwala również na współpracę z bipolarnymi silnikami krokowymi i elektromagnesami. Sterowanie jest realizowane bezpośrednio sygnałem PWM, bez potrzeby stosowania dodatkowych konwerterów. Architektura mostkowa pozwala na uproszczenie schematu aplikacyjnego i ograniczenie liczby współpracujących elementów zewnętrznych. Układ może pracować z prądem ciągłym o natężeniu do 1 A/fazę i prądem szczytowym do 4 A/fazę.

	Kanały	VCC (maks.)	I_{OUT} (maks.)	Ogranicznik prądowy	Pobór prądu w trybie standby	Rezystancja wyjściowa	Obudowa
BD60210FV	2	20 V	1,0 A	nie	1,0 µA	0,95 Ω	SSOP-B16
BD64950EFJ	1	40 V	3,5 A	tak	1,0 µA	0,55 Ω	HTSOP-J8

BD64950EFJ to jednokanałowy sterownik z wyjściem mostkowym, przeznaczony do aplikacji o większej mocy. Charakteryzuje się dopuszczalnym napięciem roboczym 40 V oraz zdolnością dostarczania do obciążenia prądu ciągłego do 3,5 A i prądu szczytowego do 6 A. Obsługuje zarówno bezpośrednie sterowanie PWM, jak i sterowanie PWM z regulacją prądu stałego. Niska rezystancja RDS(ON) ogranicza straty mocy i wydzielanie ciepła, co zwiększa sprawność energetyczną i upraszcza system chłodzenia w aplikacjach zasilanych z magistrali 24 V.

Oba układy zaprojektowano z myślą o zastosowaniu zarówno w nowych, jak i modernizowanych projektach. Pobierają one bardzo mały prąd w stanie czuwania, wynoszący maksymalnie 1,0 µA.

www.rohm.com

Szybkie bezpieczniki chipowe o zakresie prądów znamionowych od 0,315 A do 7 A

Vishay Intertechnology wprowadza na rynek dwie serie szybkich bezpieczników chipowych, zamykanych w obudowach SMD o rozmiarach 0402, 0603 i 1206. Są to bezpieczniki cienkowarstwowe o stabilnych parametrach elektrycznych i małej rezystancji wewnętrznej, produkowane w zakresie prądów znamionowych od 0,315 A do 7 A. Przyrost temperatury obudowy nie przekracza +75°C przy przepływie pełnego prądu znamionowego. Bezpieczniki spełniają wymogi normy branżowej UL 248-14, a ich zakres dopuszczalnej temperatury roboczej wynosi od –25 do +125°C.

Najważniejszą różnicą między bezpiecznikami z serii S2F i S3F jest charakterystyka czasowo-prądowa, a w szczególności szybkość zadziałania przy przeciążeniu równym 200% prądu znamionowego. Bezpieczniki serii S2F są klasyfikowane jako szybkie i zostały zaprojektowane tak, aby ulegać przepaleniu w czasie krótszym niż 1 minuta. Tolerują krótkotrwałe impulsy prądu udarowego, które nie powinny spowodować natychmiastowego wyłączenia obwodu, a jednocześnie zapewniają ochronę przed długotrwałym przeciążeniem. Z kolei bezpieczniki serii S3F, określane jako bardzo szybkie, ulegają przepaleniu w czasie krótszym od 5 s przy 200% prądu znamionowego. Są przeznaczone do ochrony wrażliwych obwodów, w których nawet krótkie przeciążenie może prowadzić do uszkodzenia elementów półprzewodnikowych lub degradacji parametrów układu. Dzięki temu projektant może dobrać odpowiedni typ bezpiecznika w zależności od dopuszczalnej energii zwarcia oraz dynamiki zmian prądu w danej aplikacji.

www.vishay.com

Mikrofon MEMS do nowej generacji aparatów słuchowych AI

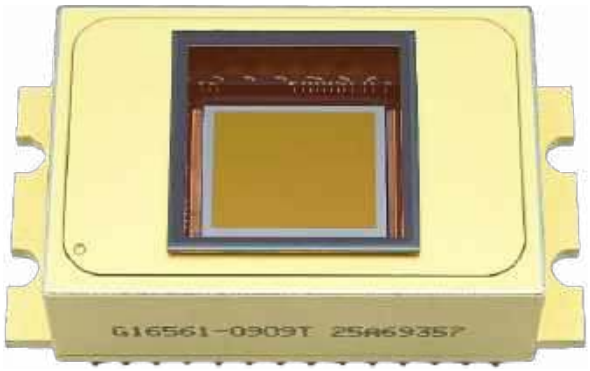
Mikrofon MM60 firmy Knowles został zaprojektowany specjalnie do zastosowań w aparatach słuchowych AI, pozwalając zmaksymalizować skuteczność działania

algorytmów sztucznej inteligencji do analizy i przetwarzania dźwięku w czasie rzeczywistym. Jego struktura obejmuje czujnik MEMS i układ ASIC – a całość jest zamknięta w obudowie o wymiarach 3,35×2,50×1,30 mm. Dostępny jest też wariant MM61 o zbliżonych parametrach i znacznie mniejszej grubości, wynoszącej 0,96 mm.

Podstawowym elementem konstrukcyjnym MM60 jest nowo opracowany czujnik MEMS, którego geometria i zastosowane materiały zapewniają skuteczną ochronę przed zalaniem i wnikaniem zanieczyszczeń. Jest on odporny na zanurzenie w wodzie do głębokości 2 m oraz na działanie powietrza o ciśnieniu przekraczającym 100 psi, znacząco przewyższając pod tym względem wcześniejsze modele. Blokuje przedostawanie się do wnętrza układu cząstek o średnicy kilku mikrometrów, co przekłada się na znacznie mniejszą awaryjność przy pracy w trudnych warunkach środowiskowych.

Wewnętrzny układ ASIC przetwarza i kształtuje sygnał elektroakustyczny, zgodnie ze specyfikacjami producenta aparatu słuchowego. Realizuje dwuetapową kontrolę wzmocnienia, pozwalając na precyzyjne ustawienie zakresu dynamiki i poziomu szumów własnych mikrofonu. Zawiera programowalne filtry o zakresie częstotliwości od 25 Hz do 20 kHz, umożliwiające kształtowanie charakterystyki częstotliwościowej oraz zapewnia dopasowanie offsetu DC do wymagań stopnia wejściowego przedwzmacniacza, co redukuje liczbę elementów korekcyjnych w torze sygnałowym. Dodatkowe zalety to wąskie tolerancje produkcyjne, redukujące różnice parametrów pomiędzy układami, a także odporność na wyładowania ESD do co najmniej 15 kV.

www.knowles.com



Czujniki obrazu InGaAs 640×512 pikseli na zakres bliskiej podczerwieni

Firma Hamamatsu Photonics wprowadza na rynek serię matrycowych czujników obrazu G1656x o rozdzielczości 640×512 pikseli, przeznaczonych do pracy w zakresie bliskiej podczerwieni. Są to czujniki zrealizowane w technologii InGaAs, zaprojektowane do aplikacji wymagających jednocześnie sporej szybkości akwizycji, dużej dynamiki sygnału i niskiego poziomu szumów własnych. Rejestrują promieniowanie w zakresie długości fali od 0,95 do 1,69 µm, charakterystycznym dla specyficznych aplikacji takich jak sortowanie tworzyw sztucznych, kontrola żywności czy niektóre zastosowania w rolnictwie. Ich duża czułość w zakresie bliskiej podczerwieni pozwala na wykrywanie słabych sygnałów optycznych, trudnych do zarejestrowania przy użyciu czujników krzemowych.

Dzięki zastosowaniu 3-stopniowego chłodzenia termoelektrycznego, czujniki G1656x wyróżniają się bardzo małym prądem ciemnym, co przekłada się na poprawę stosunku sygnału do szumu, zwłaszcza przy pracy w warunkach słabego oświetlenia i przy długich czasach integracji. Sprzyja to stabilnej pracy w środowiskach przemysłowych, gdzie zmiany temperatury mogą wpływać na jakość akwizycji obrazu. Maksymalna szybkość rejestracji 116 fps pozwala na zastosowania w procesach wymagających analizy w czasie zbliżonym do rzeczywistego, na przykład na liniach produkcyjnych i w maszynach sortujących. Zastosowany mechanizm wielolinio-wego odczytu danych umożliwia elastyczne dostosowanie sposobu akwizycji do konkretnego zadania pomiarowego, co jest istotne przy integracji z niestandardowymi systemami przetwarzania sygnałów. Szeroki zakres dynamiczny (do 3500) umożliwia rejestrację obrazu w obszarach o znacznej różnicy intensywności promieniowania. Ma to znaczenie w aplikacjach, w których badane obiekty wykazują niejednorodne właściwości optyczne lub gdy warunki oświetleniowe ulegają zmianom w trakcie pomiaru.

www.hamamatsu.com

Dwuelektrodowy odgromnik gazowy do ładowarek, systemów HVAC i fotowoltaiki

Dwuelektrodowy odgromnik gazowy GDT25H firmy Bourns zapewnia ochronę obwodów przed przepięciami o dużej energii. Został zaprojektowany do zastosowań w aplikacjach wysokonapięciowych, narażonych na impulsy przepięciowe o dużej szybkości narastania, indukowane przez wyładowania atmosferyczne lub zakłócenia w sieciach elektroenergetycznych. Spełnia wymogi normy UL 1449, co odróżnia go od wersji kwalifikowanych wyłącznie według starszej kategorii UL 497B.

Struktura wewnętrzna odgromników z serii GDT25H bazuje na rurkach gazowych, w których jonizacja gazu następuje po przekroczeniu określonego napięcia zapłonu, prowadząc do gwałtownego obniżenia impedancji i odprowadzenia prądu udarowego do masy. Zapewnia to niezwykle szybką reakcję, co jest istotne w przypadku ochrony przed przepięciami o bardzo krótkich czasach narastania.

W porównaniu z klasycznymi odgromnikami gazowymi, nowy model GDT25H charakteryzuje się węższym zakresem napięcia ograniczenia, co redukuje napięcie na chronionym obwodzie. Umożliwia przewodzenie dużych prądów udarowych, zapewniając skuteczne rozpraszanie energii przepięć, bez trwałej degradacji parametrów. Mała pojemność własna i niewielkie straty wtrącone umożliwiają stosowanie go również w aplikacjach z sygnałami wysokoczęstotliwościowymi. Stabilna charakterystyka w okresie eksploatacji ogranicza natomiast zmiany napięcia zapłonu i parametrów dynamicznych w trakcie wielokrotnych wyładowań.

Odgromnik jest produkowany w obudowie SMD przystosowanej do pracy w trudnych warunkach środowiskowych. Jego zakres temperatury pracy od –55 do +125°C pozwala na zastosowania zarówno w instalacjach zewnętrznych, jak i w urządzeniach pracujących w podwyższonej temperaturze.

Żywotność odgromnika GDT25H-75*					
Maks prąd udarowy	Nominalny prąd udarowy impulsu			Nominalny prąd udarowy AC	
8/20 µs	8/20 µs	10/350 µs	10/1000 µs	11 cykli @ 60 Hz	1 s
10 kA (1 impuls)	5 kA (10 impulsów)	1 kA (1 impuls)	100 A (300 impulsów)	20 A rms (1 impuls)	7 A rms (10 impulsów)
* po określonej liczbie impulsów udarowych, napięcie zapłonu DC może wzrosnąć o >20% w stosunku do wartości początkowej, ale element nadal zachowuje funkcję ochronną bez rozszczelnienia ani uszkodzenia					

Konstrukcja mechaniczna i technologia produkcji zostały zoptymalizowane z wykorzystaniem symulacji komputerowych, co pozwoliło uzyskać mały rozrzut parametrów między egzemplarzami.

www.bourns.com

Precyzyjny 6-osiowy układ IMU do pracy w temperaturze otoczenia od –40 do +110°C

Nowy 6-osiowy układ nawigacyjny IMU SCH16T-K20 firmy Murata, zrealizowany w technologii MEMS, zawiera 3-osiowy żyroskop i 3-osiowy akcelerometr, zamknięte w obudowie SOIC-24 o wymiarach 14×12×3 mm. Jest to wariant z kwalifikacją AEC-Q100 Grade 1, przystosowany do pracy w temperaturze otoczenia od –40 do +110°C. Zachowuje pełną zgodność rozkładu wyprowadzeń i kompatybilność programową z wcześniejszymi odpowiednikami z serii SCH16T.

Wewnętrzny żyroskop w SCH16T-K20 pracuje w zakresie pomiarowym ±300°/s i charakteryzuje się typową gęstością szumów na poziomie 0,0004 (°/s)/√Hz oraz dokładnością 0,3°/h. Parametry te zapewniają mały błąd całkowania w systemach nawigacji inercyjnej, stabilizacji obrazu i sterowania ruchem, w których nawet niewielki dryft prowadzi do zauważalnych błędów pozycjonowania. Lepsza kalibracja temperaturowa, zoptymalizowana pod kątem temperatury roboczej od –40 do +85°C, przekłada się na mniejsze przesunięcie offsetu.

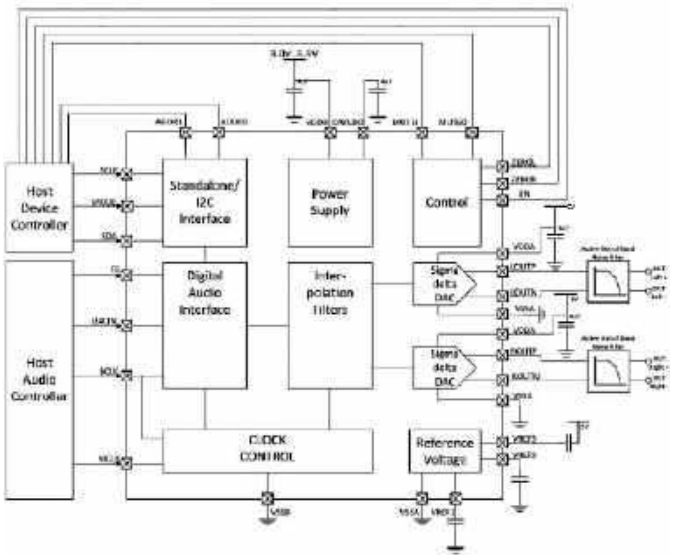
W wewnętrznym akcelerometrze zastosowano technikę pomiaru podwójnie różnicowego, znaną z wcześniejszych wersji SCA3400 i SCA103T. Zapewnia ona skuteczną redukcję szumów własnych, kompensację wpływu temperatury oraz poprawę stabilności długoterminowej. Akcelerometr pracuje w zakresie pomiarowym ±8 g i charakteryzuje się gęstością szumu 33 µg/√Hz.

Czujnik SCH16T-K20 może być zasilany napięciem od 3,0 do 3,6 V. Zakres napięć interfejsu I/O rozciąga się od 1,7 do 3,6 V, co ułatwia integrację z różnymi rodzinami mikrokontrolerów i procesorów sygnałowych. Komunikacja jest realizowana przez interfejs SafeSPI 2.0. Dane wyjściowe mogą być przesyłane z rozdzielczością 16 lub 20 bitów.

Ważnym elementem układów z serii SCH16T jest rozbudowany system autodiagnostyki. W każdej ramce SPI raportowany jest status, oparty na monitorowaniu ponad 200 wewnętrznych sygnałów diagnostycznych. Funkcje te umożliwiają wykrywanie uszkodzeń, anomalii pracy oraz degradacji parametrów w trakcie eksploatacji, co jest istotne w systemach o podwyższonych wymogach bezpieczeństwa.

SCH16T-K20 jest przeznaczony do zastosowań wymagających bardzo dobrej stabilności pomiarów, odporności na narażenia środowiskowe i powtarzalności parametrów w długim okresie użytkowania. Przykładem mogą być samochodowe systemy nawigacji inercyjnej, sterowanie ruchem robotów, stabilizacja kamer oraz bezzałogowe statki powietrzne.

www.murata.com



Stereofoniczny 24-bitowy przetwornik C/A do profesjonalnych systemów audio

W ofercie firmy Nuvoton pojawił się nowy, stereofoniczny przetwornik C/A do profesjonalnych systemów audio. NAU8421YG to przetwornik o 24-bitowej rozdzielczości, dużej dynamice, niewielkich zniekształceniach i przesłuchach międzykanałowych oraz skutecznym tłumieniu tętnień obecnych na linii zasilania. Zawiera interfejsy wejściowe I²S i PCM oraz wyjście różnicowe o zakresie pełnej skali 8,3 V_{p-p}, eliminujące konieczność stosowania dodatkowych wzmacniaczy.

NAU8421YG może pracować z częstotliwością próbkowania od 8 do 192 kHz. Charakteryzuje się stosunkiem sygnału do szumu 128 dB, zawartością harmonicznych i szumów na poziomie –99 dB oraz separacją kanałów dochodzącą do 140 dB @ 1 kHz. Ma to znaczenie w systemach wielokanałowych oraz w zastosowaniach studyjnych, gdzie jednocześnie przetwarzane są sygnały znacznie różniące się amplitudą. Wysoki współczynnik tłumienia tętnień zasilania (105 dB @ 1 kHz) ułatwia integrację z systemami, w których jakość sygnału zasilającego może być ograniczona przez inne bloki funkcjonalne.

NAU8421YG pracuje z oddzielnymi napięciami zasilania sekcji cyfrowej i analogowej, wynoszącymi od 3,3 do 5 V. Jego typowy pobór mocy na poziomie kilkudziesięciu mW pozwala na zastosowania w urządzeniach energooszczędnych. Konfiguracja parametrów pracy odbywa się za pomocą magistrali I²C, przy czym część funkcji może być wybierana sprzętowo, poprzez odpowiednie sterowanie wyprowadzeniami, co umożliwia pracę w trybie autonomicznym, bez udziału mikrokontrolera. Mechanizmy automatycznego wykrywania sygnału zegarowego upraszczają sekwencje uruchamiania i wyłączania systemu oraz zmniejszają ryzyko generowania zakłóceń podczas zmiany trybu zasilania.

NAU8421YG jest zamykany w obudowie QFN-32 o powierzchni 5×5 mm. Może pracować w zakresie temperatury otoczenia od –40 do +85°C. Jego typowe zastosowania obejmują m.in. instrumenty muzyczne, profesjonalne systemy audio/wideo i konsole do gier.

www.nuvoton.com

TAWOIA Glass (szkło kwarcowe)

https://sklep.avt.pl/pl/menu/tawoia-glass-4505.html

BESTSELLERY sklepu AVT – sklep.avt.pl

3 unikalne serie gniazdek i włączników

Rabat dla Czytelników EP
przy zakupie podaj kod **EP2505GW**

-5%

Rabat dla Prenumeratorów EP
przy zakupie podaj numer prenumeraty

-10%

Ceramic Loft (ceramika)

https://sklep.avt.pl/pl/menu/seria-ceramic-loft-4190.html

Retro PRL (bakelit)

https://sklep.avt.pl/pl/series/retro-prl-3237.html

W ofercie AVT*
AVT6099

Najważniejsze parametry:
- odtwarzanie pojedynczego pliku WAV zapisanego na karcie microSD sformatowanej w systemie FAT32,
- rozpoczęcie odtwarzania po podaniu na zacisk wejściowy impulsu napięcia 3...30 V,
- wyjście monofoniczne o poziomie sygnału regulowanym potencjometrem,
- obsługa plików 8- i 16-bitowych, mono- i stereofonicznych, próbkowanych z częstotliwością 8...48 kHz,
- wbudowany prosty przetwornik cyfrowo-analogowy typu PWM,
- niski pobór prądu w stanie spoczynku: do 230 µA,
- pobór prądu podczas odtwarzania: około 30 mA,
- zasilanie napięciem stałym 4,5...18 V (lub 2,7...3,6 V z pominięciem wbudowanego stabilizatora).

Projekty pokrewne na stronie www.ep.com.pl
(aktywne linki do artykułów):
- Stacjonarny odtwarzacz audio Media Pi
- Odtwarzacz audio z Raspberry Pi
- Strumieniowy odtwarzacz audio na i.MX6ULL
- Audiofilski odtwarzacz muzyki z Raspberry Pi
- Przetwornik audio DAC z układem PCM5102A
- Odtwarzacz sieciowy audio dla NanoPi
- Przedwzmacniacz gramofonowy MM z pasywną korekcją
- RaspbPI_DAC – przetwornik audio dla Raspberry Pi

* **Uwaga!** Elektroniczne zestawy do samodzielnego montażu. Wymagana umiejętność lutowania! Podstawową wersją zestawu jest wersja **[B]** nazywana potocznie KIT-em (z ang. zestaw). Zestaw w wersji **[B]** zawiera elementy elektroniczne (w tym **[UK]** – jeśli występuje w projekcie), które należy samodzielnie wlutować w dołączoną płytkę drukowaną (PCB). Wykaz elementów znajduje się w dokumentacji, która jest podlinkowana w opisie kitu. Mając na uwadze różne potrzeby naszych klientów, oferujemy dodatkowe wersje:
- **wersja [C]** – zmontowany, uruchomiony i przetestowany zestaw **[B]** (elementy wlutowane w płytkę PCB),
- **wersja [A]** – płytka drukowana bez elementów i dokumentacji.

Kity, w których występuje układ scalony wymagający zaprogramowania, mają następujące dodatkowe wersje:
- **wersja [A+]** – płytka drukowana **[A]** + zaprogramowany układ **[UK]** i dokumentacja,
- **wersja [UK]** – zaprogramowany układ.

Nie każdy zestaw AVT występuje we wszystkich wersjach! Każda wersja ma załączony ten sam plik PDF! Podczas składania zamówienia upewnij się, którą wersję zamawiasz! **http://sklep.avt.pl**

W przypadku braku dostępności na stronie sklepu osoby zainteresowane zakupem płytek drukowanych (PCB) prosimy o kontakt via e-mail: **kity@avt.pl**

Prosty odtwarzacz audio

Odtwarzacze plików muzycznych często dysponują wieloma funkcjami, takimi jak możliwość wyboru utworu i zatrzymania odtwarzania, cyfrowa regulacja głośności i inne. Jednak w niektórych zastosowaniach potrzeba czegoś wyjątkowo prostego, co pod wpływem zewnętrznego impulsu ma odtworzyć plik dźwiękowy. I tyle, nic więcej. Właśnie do tego służy opisany układ.

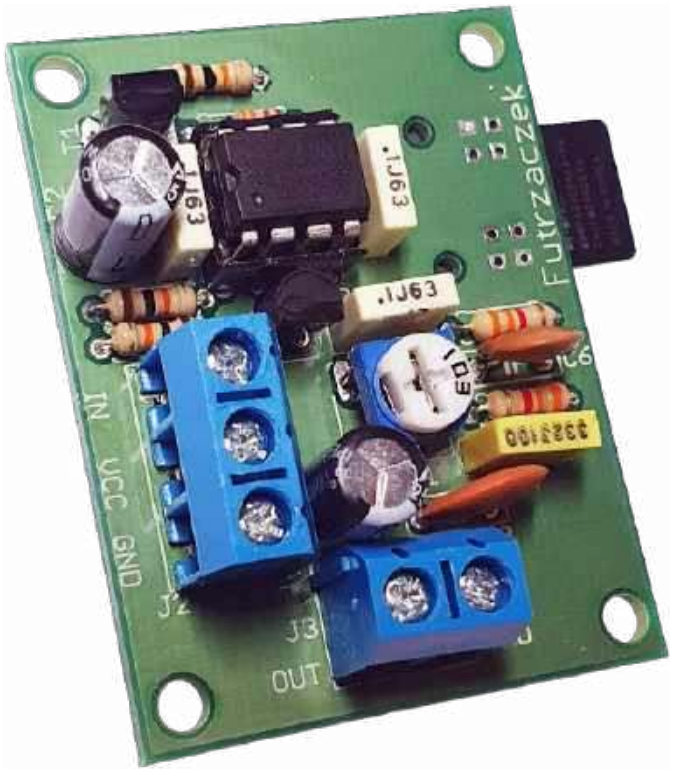
Drzwi, które samoczynnie witają klientów, witryna z czujnikiem ruchu, która fotokomórką wykrywa obecność zainteresowanego człowieka lub prosta instrukcja głosowa, uruchamiana wciśnięciem przycisku – te i inne aplikacje znane z codziennego użytku, które zostały zautomatyzowane elektroniką, wymagają odtwarzania komunikatów głosowych. W latach dziewięćdziesiątych służyły do tego układy z serii ISD, które odeszły już w zapomnienie. To nawet lepiej, bo oferowana przez nie jakość była… taka, jaką udało się wtedy uzyskać. Dzisiaj mamy do dyspozycji znacznie pojemniejsze i tańsze nośniki danych, co umożliwia odtwarzanie dźwięków o zdecydowanie lepszej jakości.

Dzięki temu, że nośnikiem pliku dźwiękowego jest zwykła karta microSD, którą dzisiaj można kupić dosłownie za kilkanaście złotych, można ów dźwięk wygodnie edytować na komputerze, tablecie lub smartfonie, po czym wgrać na kartę jak każdy inny, zwykły plik. To wygodne rozwiązanie, ponieważ pliki WAV są obsługiwane przez wszystkie systemy operacyjne, również te mobilne. Nie jest potrzebna jakakolwiek konwersja do formatu binarnego czy innego, odczytywanego przez bardzo proste systemy mikroprocesorowe.

Zadanie tego układu jest skrajnie proste: po podaniu napięcia na wejście rozpoczyna się odtwarzanie zapisanego pliku. Jeżeli wejście jest aktywowane stale, odtwarzanie przebiega w pętli tak długo, jak długo na wejściu jest obecne napięcie. Po zakończeniu odtwarzania układ wraca do stanu spoczynku. Dlatego można go zaadaptować do bardzo wielu zastosowań, ponieważ nie wymaga od użytkownika jakiegokolwiek dodatkowego działania.

Budowa

Schemat ideowy omawianego układu znajduje się na **rysunku 1**. Głównym podzespołem zawiadującym jego pracą jest niewielki mikrokontroler typu ATtiny85 z 8-bitowym rdzeniem AVR, taktowanym sygnałem o częstotliwości 16 MHz, dla którego wzorcem jest wewnętrzny generator RC o częstotliwości oscylacji 8 MHz. Wbudowany układ PLL służy do podwojenia częstotliwości dla rdzenia oraz do uzyskania sygnału o częstotliwości aż 64 MHz na potrzeby generowania sygnału PWM. Ten zaś służy do realizacji przetwarzania cyfrowo-analogowego.



Skąd decyzja o wyborze właśnie takiego mikrokontrolera? Po pierwsze jego pamięć Flash pomieści przeszło 6 kB programu. Po drugie jest wyposażony w 512 bajtów pamięci RAM, co jest konieczne przy odczytywaniu bloków z karty SD, które to przychodzą w pakietach po 256 bajtów – wartość ta jest charakterystyczna dla użytej darmowej biblioteki Petit FatFs. Po trzecie układ ma dosyć unikatową – jak na ośmiobitowe, małe mikrokontrolery – możliwość taktowania licznika sygnałem o częstotliwości aż 64 MHz, przez

Wykaz elementów:

Rezystory: (THT o mocy 0,25 W)
R1, R3, R4: 10 kΩ
R2, R5, R6: 3,3 kΩ
P1: potencjometr montażowy 10 kΩ (jednoobrotowy, leżący)

Półprzewodniki:
T1: BC546 (TO92)
US1: ATtiny85-20PU (DIP8)
US2: LP2950-33 (TO92, opis w tekście)

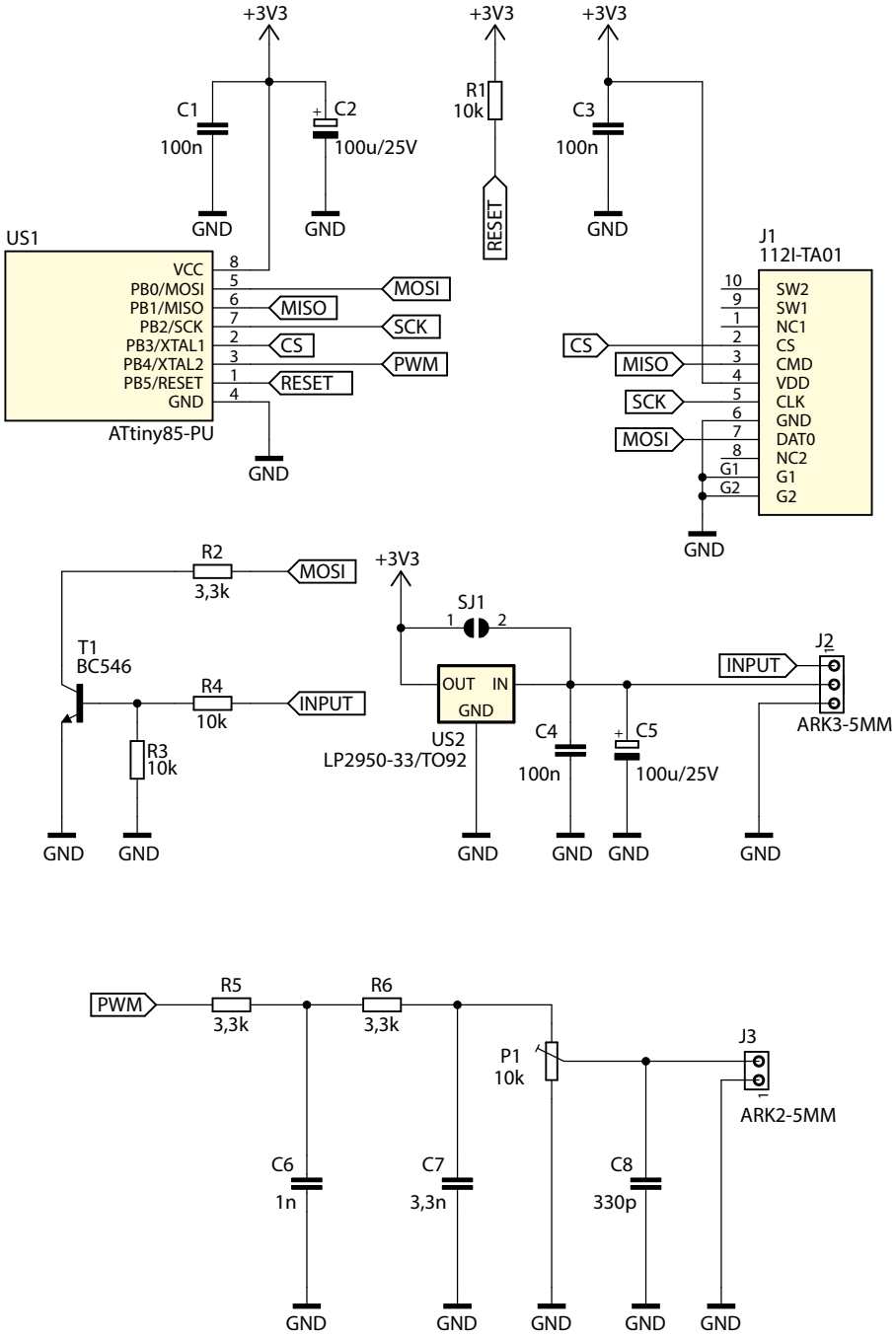
Kondensatory:
C1, C3, C4: 100 nF (raster 5 mm, MKT)
C2, C5: 100 µF/25 V (raster 2,5 mm)
C6: 1 nF (raster 5 mm, monolityczny)
C7: 3,3 nF (raster 5 mm, MKT)
C8: 330 pF (raster 5 mm, monolityczny)
Kondensator elektrolityczny 100 µF/16 V (opis w tekście)

Pozostałe:
J1: 112I-TA01
J2: ARK3/500
J3: ARK2/500
Jedna podstawka DIP8

co można generować z jego użyciem sygnał PWM o częstotliwości 250 kHz i rozdzielczości 8 bitów (64 MHz/256=250 kHz), co jest w zupełności wystarczające do odtworzenia sygnału spróbkowanego z częstotliwością 48 kHz lub niższą. Ze względu na niewielką liczbę konfigurowalnych wyprowadzeń (ATtiny85 ma ich zaledwie pięć) nie jest możliwe podanie zewnętrznego sygnału zegarowego stabilizowanego rezonatorem kwarcowym, lecz w tak prostym zastosowaniu wbudowany generator RC jest całkowicie wystarczający.

Mikrokontroler nawiązuje połączenie z kartą microSD poprzez standardowy interfejs SPI, co jest bardzo wygodne z uwagi na jego niewielką liczbę wyprowadzeń. Użyte w tym projekcie złącze karty microSD ma metalową obudowę, która została solidnie połączona z masą układu, a to ze względu na fakt, że w testach pierwszego prototypu okazało się, że regularne odczytywanie danych z karty SD powodowało powstawanie przydźwięku w wytwarzanym sygnale audio. Dopiero zaekranowanie samej karty oraz ścieżek łączących ją z mikrokontrolerem, co zostało zrealizowane poprzez użycie płytki dwustronnej z wylewką masy na jednej stronie, zniwelowało ten przykry odsłuchowo efekt praktycznie do zera.

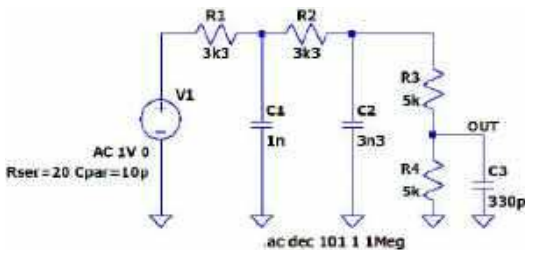
Z uwagi na wymaganą w tym projekcie oszczędność linii mikrokontrolera, wejście wyzwalające odtwarzanie zostało podłączone do jednej z linii interfejsu SPI, która podczas spoczynku ma stan wysoki, wymuszony przez wbudowany w mikrokontroler rezystor podciągający do dodatniej linii zasilania. Tranzystor T1, który wchodzi w nasycenie po podaniu zewnętrznego impulsu wyzwalającego, nadaje tej linii stan niski za pośrednictwem rezystora R2. W ten sposób, po rozpoczęciu odtwarzania, dalsza obecność impulsu wejściowego nie zaburza współpracy na linii karta microSD – mikrokontroler, ponieważ rezystor ten obciąża ją jedynie prądem o wartości około 1 mA, co jest całkowicie akceptowalne. Po zakończeniu odtwarzania wyprowadzenie znów przyjmuje stan wysoki.



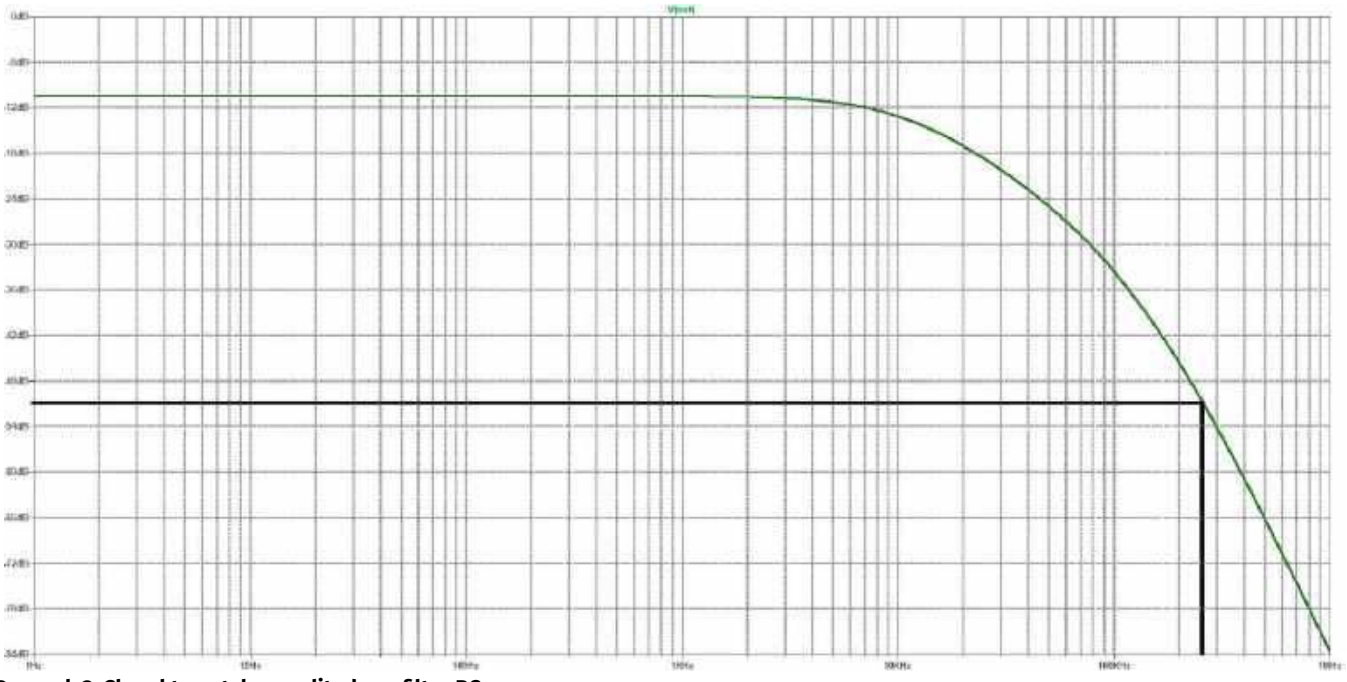
Rysunek 1. Schemat ideowy miniaturowego odtwarzacza audio

Napięcie zasilające układ wymusza tutaj karta microSD, ponieważ toleruje ona wartości z przedziału 2,7…3,6 V. Na szczęście takie same wartości akceptuje również mikrokontroler, więc nie ma tutaj konfliktu interesów i oba te podzespoły mogą się komunikować bez potrzeby translacji poziomów napięcia. W celu uzyskania stabilizowanego napięcia o wartości 3,3 V, na płytce został dodany stabilizator LDO typu LP2950-33 (US2). Pobiera on jedynie 50 µA prądu spoczynkowego, co jest bardzo dobrym wynikiem, choć przy zasilaniu bateryjnym każdy mikroamper staje się cenny. Stabilizator może okazać się zbyteczny, kiedy mamy do dyspozycji takie właśnie napięcie – montaż US2 można pominąć, zwierając przy tym kroplą spoiwa lutowniczego pola SJ1.

Na sam koniec została rzecz najciekawsza, przynajmniej z mojego punktu widzenia, czyli dolnoprzepustowy filtr odtwarzający sygnał akustyczny z generowanego przez mikrokontroler przebiegu PWM. Zadowalająca charakterystyka, godząca kompromis między zapewnieniem szerokiego pasma przenoszenia a minimalizacją poziomu szumu, generowanego przez prostokątny sygnał nośny o częstotliwości 250 kHz, została uzyskana w toku obliczeń i eksperymentów. Przyjęto, że wariantem optymalnym będzie dwuczłonowy filtr RC (R5-C6 i R6-C7), obciążony potencjometrem regulującym głośność, za którym będzie się znajdowała jeszcze jedna pojemność, zwierająca składowe o najwyższych częstotliwościach. Z uwagi

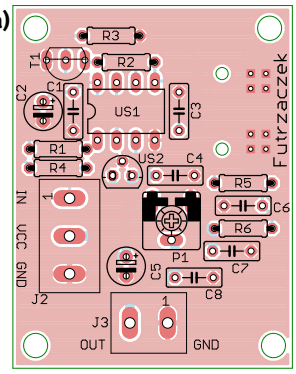


Rysunek 2. Schemat symulacyjny dolnoprzepustowego filtru RC

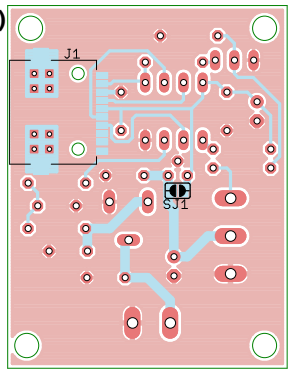


Rysunek 3. Charakterystyka amplitudowa filtru RC

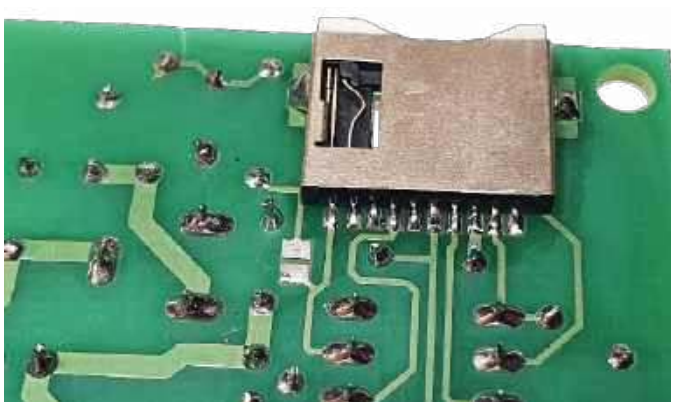
a)



b)



Rysunek 4. Schemat montażowy płytki (a – strona TOP, b – strona BOTTOM)



Fotografia 1. Widok przylutowanego złącza karty microSD

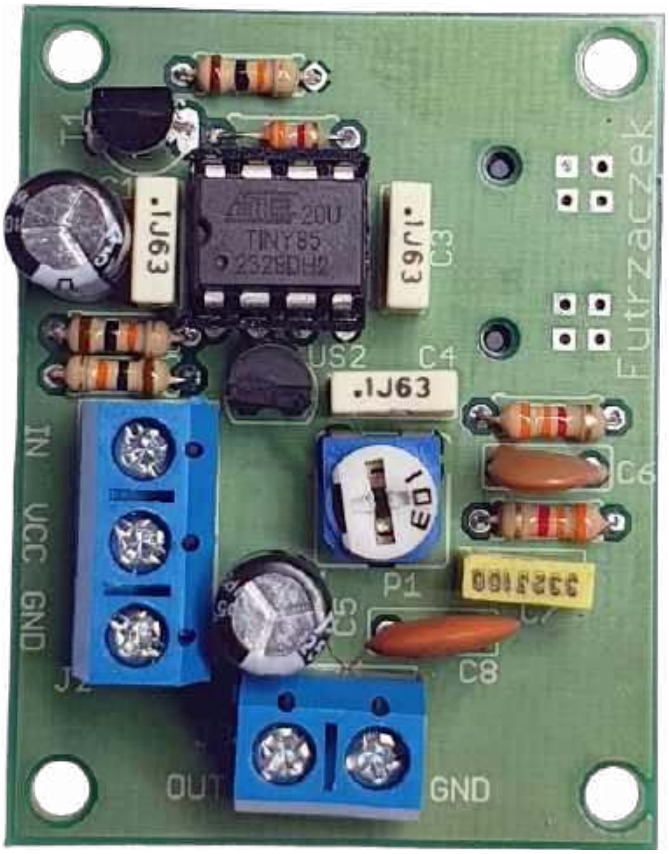
na miniaturyzację oraz założenie, że ma to być realizacja budżetowa, zrezygnowano z filtrów aktywnych, zawierających wzmacniacze operacyjne. Warto dodać, że tak utworzony sygnał analogowy będzie miał niezerową składową stałą – jego wartość chwilowa zawsze będzie nie mniejsza niż 0 V, co bywa przydatne w sterowaniu niektórych wzmacniaczy. Założyłem, że w razie potrzeby użytkownik może wstawić kondensator w torze sygnału i gotowe.

Schemat symulacyjny owego filtru został utworzony w programie LTspice – **rysunek 2** – i uwzględnia podstawowe parametry pasożytnicze wyjścia mikrokontrolera. Potencjometr P1 ustalający głośność został tutaj ustawiony w połowie. Wykreślony przebieg charakterystyki znajduje się na **rysunku 3**, na którym dodatkowo zaznaczono częstotliwość sygnału PWM (250 kHz) i odpowiadające jej tłumienie. Z wykresu można odczytać, że tłumienie w zakresie częstotliwości akustycznych jest niemal stałe i zaczyna wzrastać dopiero powyżej ok. 8 kHz. Tłumienie 6 dB, odpowiadające dwukrotnemu spadkowi amplitudy, zaczyna się przy częstotliwości 20 kHz, co oznacza, że całe pasmo akustyczne będzie odwzorowane możliwie wiernie. Trzeba przy tym cały czas mieć na uwadze, że zastosowano tutaj bardzo prosty, ośmiobitowy przetwornik PWM równie prostym filtrem, a całość ma służyć do odtwarzania komunikatów informacyjnych (tudzież powitalnych melodyjek), nie zaś do audiofilskiego odsłuchu. Częstotliwość nośna jest tłumiona o 40 dB, co odpowiada spadkowi stukrotnemu – ten parametr również uważam za bardzo dobry jak na tak prosty układ.

Montaż i uruchomienie

Układ został zmontowany na dwustronnej płytce drukowanej o wymiarach 37 mm × 48 mm. Jej wzór ścieżek oraz schemat montażowy przedstawia **rysunek 4**. Wszystkie otwory montażowe zostały umieszczone w odległości 3 mm od krawędzi płytki i mają średnicę 3,2 mm.

Montaż proponuję rozpocząć od przylutowania złącza J1, które jest jedynym podzespołem montowanym nie dość, że powierzchniowo (SMD), to na dodatek po przeciwnej stronie niż pozostałe elementy. Ten proces ułatwi fakt, że złącze wyposażono w dwa



Fotografia 2. Widok zmontowanej płytki prototypowej – strona TOP

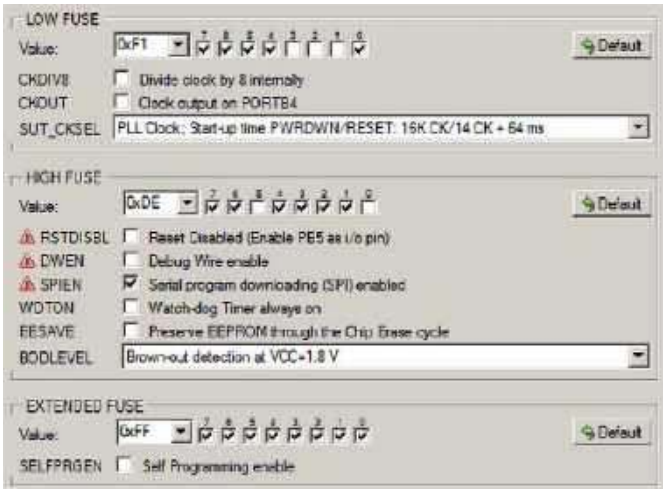
kołki centrujące, które wchodzą w dedykowane im otwory na płytce, przez co można łatwo ustalić jego położenie przed przylutowaniem. Na początek proponuję przylutować dwie metalowe „łapki" po bokach złącza, regulując tym samym położenie wyprowadzeń (umieszczonych na jego tylnej krawędzi) względem pól lutowniczych na płytce drukowanej. Kiedy mamy pewność, że złącze tkwi już nieruchomo, a jego wyprowadzenia są na środku dedykowanych pól lutowniczych, można je przylutować, do czego wystarczy zwykłe spoiwo lutownicze i kalafonia. Całość powinna wyglądać jak na **fotografii 1**. Montaż przewlekany proponuję rozpocząć od elementów o najmniejszej wysokości obudowy, czyli rezystorów. Pod układ scalony US1 proponuję zastosować podstawkę, aby ułatwić jego programowanie i wymianę w razie uszkodzenia. Zmontowany układ można zobaczyć na **fotografii 2**.

Na etapie uruchamiania konieczne jest zaprogramowanie pamięci Flash mikrokontrolera dostarczonym wsadem oraz zmiana wartości jego bitów zabezpieczających. Oto ich nowe ustawienia:

```
Low Fuse=0xF1
High Fuse=0xDE
```

Szczegóły są widoczne na **rysunku 5**, który zawiera widok okna konfiguracji tychże bitów z programu BitBurner. W ten sposób zostanie uruchomiony wbudowany generator RC z układem PLL powielającym jego częstotliwość oraz Brown-Out Detector, który wprowadzi mikrokontroler w stan zerowania, jeżeli jego napięcie zasilające spadnie poniżej 1,8 V. To znacznie zmniejsza ryzyko zawieszenia się mikrokontrolera podczas uruchamiania.

Poprawnie zaprogramowany układ jest gotowy do działania po włożeniu karty microSD do złącza J1 oraz po podłączeniu zasilania do zacisków złącza J2 (VCC i GND). Powinno to być napięcie stałe, dobrze filtrowane, najlepiej stabilizowane, z przedziału 4,5…18 V. Pobór prądu wynosi 230 µA w stanie spoczynku i około 30 mA w trakcie odtwarzania. Można zredukować pobór prądu w stanie spoczynku o 50 µA, czyli do około 180 µA, poprzez wylutowanie stabilizatora US2 i zwarcie jego wejścia z wyjściem poprzez nałożenie kropli spoiwa lutowniczego na pola lutownicze SJ1



Rysunek 5. Szczegóły ustawienia bitów zabezpieczających

– trzeba wtedy pamiętać o konieczności zasilania układu napięciem z przedziału 2,7…3,6 V. Dlatego jego źródłem nie może być akumulator litowo-jonowy, którego napięcie po naładowaniu przekracza 4 V.

Wejście wyzwalające (IN) akceptuje napięcie z przedziału 3…30 V. Prąd wejściowy wynosi od około 0,25 mA przy 3 V do około 3 mA przy 30 V. Większe wartości tego napięcia nie są wskazane z uwagi na wytrzymałość termiczną rezystora R4.

Eksploatacja

Na karcie microSD, sformatowanej w systemie FAT32, powinien się znajdować jeden plik o dowolnej nazwie i z rozszerzeniem *.wav. Jeżeli będzie ich więcej, odczytywany będzie tylko pierwszy, a reszta zostanie przez układ pominięta. Plik powinien być umieszczony w katalogu głównym karty, nie zaś w folderze. Parametry tego pliku:

- kodowanie PCM lub LPCM (Linear-PCM),
- próbkowanie z przedziału 8…48 kHz,
- rozdzielczość 8 bitów lub 16 bitów (ale nie 24 bity),
- zapis monofoniczny (1 kanał) lub stereofoniczny (2 kanały),
- próbki 16-bitowe zapisane ze znakiem (signed) lub 8-bitowe bez znaku (unsigned).

Taki plik może mieć dowolny czas trwania. Jego odtwarzanie rozpocznie się po podaniu na wejście IN napięcia wyzwalającego. W czasie odtwarzania nie jest możliwe zatrzymanie ani przewinięcie odtwarzania, jedynie wyłączenie zasilania zatrzyma działanie odtwarzacza. Po odtworzeniu pliku układ wraca do stanu spoczynku. Jeżeli napięcie wyzwalające będzie obecne w chwili zakończenia odtwarzania, układ rozpocznie działanie na nowo, od razu po zakończeniu poprzedniego.

Michał Kurzela, EP

W ofercie AVT*
AVT6100

Najważniejsze parametry:
- konstrukcja: liniowa z szeregowym tranzystorem MOSFET i sterowaniem cyfrowym,
- napięcie wyjściowe: 1...24 V z rozdzielczością 500 mV,
- prąd wyjściowy: 50...1000 mA z rozdzielczością 50 mA,
- sprzętowe zabezpieczenie nadprądowe sterowane cyfrowo,
- obsługa za pomocą dwóch enkoderów obrotowych i wyświetlacza THT 128×160 px,
- wbudowany przycisk do szybkiego załączania i wyłączania wyjścia.

Projekty pokrewne na stronie www.ep.com.pl
(aktywne linki do artykułów):
- Regulowany zasilacz warsztatowy – RPS-02 z kolorowym wyświetlaczem i sterowaniem dotykowym
- Zasilacz warsztatowy
- Modułowy zasilacz warsztatowy
- Regulowany zasilacz warsztatowy ze sterowaniem mikroprocesorowym

* **Uwaga!** Elektroniczne zestawy do samodzielnego montażu. Wymagana umiejętność lutowania! Podstawową wersją zestawu jest wersja **[B]** nazywana potocznie KIT-em (z ang. zestaw). Zestaw w wersji **[B]** zawiera elementy elektroniczne (w tym **[UK]** – jeśli występuje w projekcie), które należy samodzielnie wlutować w dołączoną płytkę drukowaną (PCB). Wykaz elementów znajduje się w dokumentacji, która jest podlinkowana w opisie kitu. Mając na uwadze różne potrzeby naszych klientów, oferujemy dodatkowe wersje:
- **wersja [C]** – zmontowany, uruchomiony i przetestowany zestaw **[B]** (elementy wlutowane w płytkę PCB),
- **wersja [A]** – płytka drukowana bez elementów i dokumentacji.

Kity, w których występuje układ scalony wymagający zaprogramowania, mają następujące dodatkowe wersje:
- **wersja [A+]** – płytka drukowana **[A]** + zaprogramowany układ **[UK]** i dokumentacja,
- **wersja [UK]** – zaprogramowany układ.

Nie każdy zestaw AVT występuje we wszystkich wersjach! Każda wersja ma załączony ten sam plik PDF! Podczas składania zamówienia upewnij się, którą wersję zamawiasz! http://sklep.avt.pl

W przypadku braku dostępności na stronie sklepu osoby zainteresowane zakupem płytek drukowanych (PCB) prosimy o kontakt via e-mail: kity@avt.pl

Zasilacz warsztatowy (2)

Jakiś czas temu na jednym z forów poświęconych praktycznym konstrukcjom elektronicznym, pewien uczestnik zadał pytanie o możliwość samodzielnego zbudowania zasilacza do swojej pracowni. Z kontekstu wynikało, że jest raczej początkujący i szuka prostych, sprawdzonych konstrukcji łatwych do powielenia. Początkowo dyskusja koncentrowała się wokół tego, co ewentualnie można wykonać nie mając doświadczenia. Jednak dość szybko ktoś zapytał: po co robić, jeżeli można kupić? Szybko, tanio i podobno dobrze. Czy na pewno? W drugiej części artykułu kontynuujemy opis naszego zasilacza DIY – tym razem skupimy się na sterowniku oraz aspektach montażowych urządzenia.

Pierwszy odcinek znajduje się pod adresem:
https://ulubionykiosk.pl/media

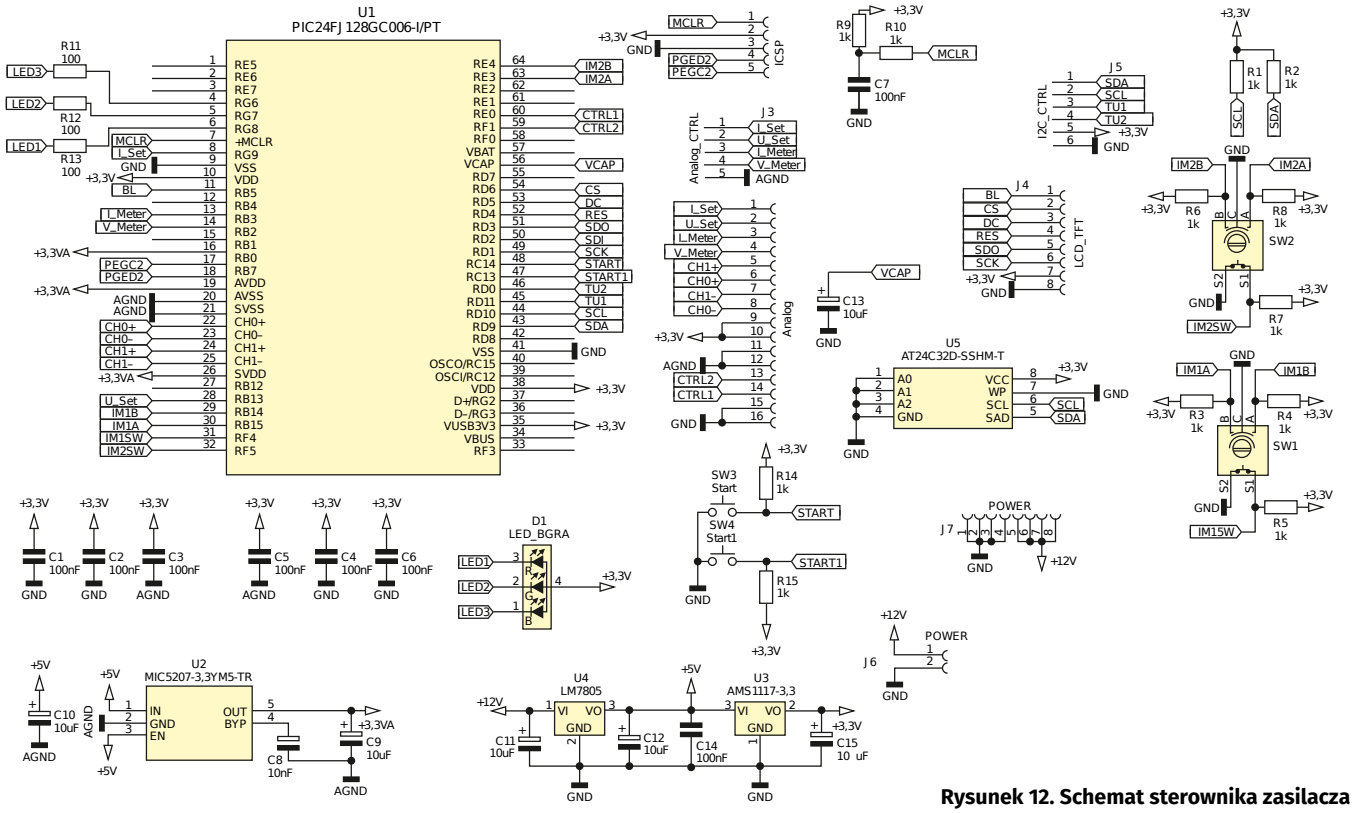
Interfejs użytkownika – sterownik mikroprocesorowy

Druga, po torze analogowym, część zasilacza to sterownik mikroprocesorowy. Spełnia on dwie podstawowe funkcje:
- ustawia napięcie wyjściowe i wartość ograniczenia prądowego przez podawanie napięć z przetworników cyfrowo-analogowych na wejścia USet i ISet oraz mierzy napięcie wyjściowe UMeter i prąd wyjściowy IMeter za pomocą przetworników analogowo-cyfrowych;
- realizuje funkcje interfejsu użytkownika z obsługą kolorowego wyświetlacza LCD-TFT, impulsatorów nastawczych i klawisza START. Wbudowana nieulotna pamięć EEPROM zapamiętuje bieżące nastawy i odtwarza je po włączeniu zasilania.

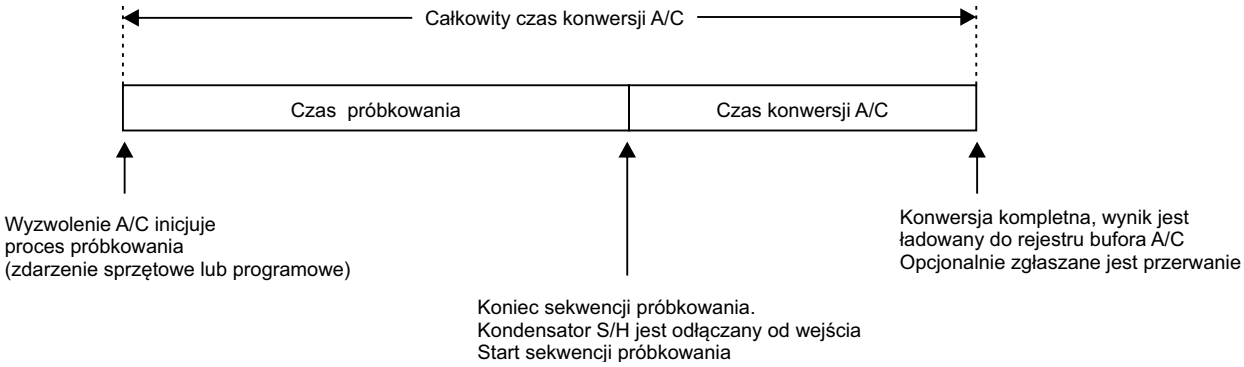
Schemat sterownika został pokazany na **rysunku 12**.

Układ zasilania modułu sterownika

Moduł sterownika jest zasilany napięciem +12 V, pochodzącym z modułu sekcji analogowej, przez 8-pinowe złącze goldpin oznaczone POWER. Stabilizator U4 typu 7805 jest zasilany napięciem +12 V i dostarcza napięcie +5 V, które zasila dwa kolejne



Rysunek 12. Schemat sterownika zasilacza



Rysunek 13. Sekwencja czasowa konwersji A/C typu SAR

stabilizatory o napięciu wyjściowym +3,3 V: U3 typu 1117 oraz U2 typu MIC5207. Stabilizator U3 obsługuje część cyfrową sterownika, czyli mikrokontroler i pamięć EEPROM (U2 typu 24C32) z interfejsem I²C. Drugi stabilizator U2 (MIC5207) jest źródłem napięcia +3,3 V dla obwodów analogowych sterownika, które poprzez pin AVDD zasila także wewnętrzne bloki analogowe mikrokontrolera: przetworniki DAC i PADC, komparatory, wzmacniacze operacyjne i źródło napięcia odniesienia. Wbudowany 16-bitowy przetwornik ADC typu delta-sigma (tu nie wykorzystywany) jest natomiast zasilany przez wyprowadzenie SVDD. Napięcie +3,3 V ze stabilizatora U2 jest również odniesieniem dla przetwornika analogowo-cyfrowego PADC oraz zasila układ czujnika prądu INA250 na płytce sekcji analogowej zasilacza.

Jak się łatwo domyślić, zastosowanie dodatkowego, niskoszumnego stabilizatora zasilającego tylko układy analogowe, ma na celu znacząco ograniczyć przenikanie impulsowych zakłóceń przenoszonych po liniach zasilania z części cyfrowej urządzenia do obwodów analogowych.

Mikrokontroler modułu sterownika

W projekcie zastosowano 16-bitowy mikrokontroler PIC24FJ128GC006. Podstawowym kryterium wyboru tego układu były jego analogowe układy peryferyjne, konieczne do budowy opisanego poprzednio, analogowego toru zasilacza. Producent – firma Microchip – chwali się dobrymi parametrami analogowymi tego układu:

- 12-bitowym, szybkim przetwornikiem analogowo-cyfrowym PADC z zaawansowanymi funkcjami akwizycji, takimi jak auto-accumulate czy Threshold Detect,
- 16-bitowym przetwornikiem analogowo-cyfrowym ADC z modulatorem delta-sigma,
- dwoma 10-bitowymi przetwornikami cyfrowo-analogowymi DAC,
- dwoma wzmacniaczami operacyjnymi Rail-to-Rail o paśmie przenoszenia 2,5 MHz,
- trzema komparatorami Rail-to-Rail,
- wbudowanym programowalnym źródłem napięcia odniesienia.

W układzie zasilacza zastosowano 12-bitowy przetwornik analogowo-cyfrowy PADC do pomiaru napięcia wyjściowego zasilacza i do pomiaru prądu wyjściowego. Dwa przetworniki cyfrowo-analogowe zostały użyte do ustawiania napięcia wyjściowego zasilacza i do ustawienia poziomu ograniczenia prądowego. Pierwotnie planowano wykorzystanie zewnętrznych przetworników ADC i DAC o dobrej dokładności i liniowości, ale ostatecznie wybór padł na wbudowane moduły. Parametry przetworników znajdujących się w mikrokontrolerach są zazwyczaj gorsze w porównaniu do zewnętrznych układów tego typu. Założono jednak, że w przypadku niewystarczającej dokładności konwersji wprowadzone zostaną korekty programowe, a zastosowanie wbudowanych modułów znacznie upraszcza projekt. Należy też pamiętać, że nie budujemy tutaj przyrządu pomiarowego, ale zasilacz warsztatowy, zatem nie będą potrzebne bardzo dokładne pomiary.

Jak wiemy, w sekcji analogowej zasilacza zostały użyte wzmacniacze operacyjne pełniące funkcje wzmacniacza błędu i wzmacniacza napięcia stałego. Są to podwójne wzmacniacze typu OP296. Podstawowym powodem, dla którego nie zostały użyte wzmacniacze wbudowane w mikrokontroler, jest zbyt duży offset wejściowy, wynoszący typowo 2 mV, a maksymalnie nawet 14 mV. To mogło powodować problemy z poprawnym działaniem (dokładnością) układu regulacji, jak i układu pomiarowego. Zastosowany ostatecznie wzmacniacz operacyjny ma typowy, katalogowy offset na poziomie ok 30 µV, a maksymalny na poziomie 300 µV. Ponadto jest on przystosowany do pracy z pojedynczym napięciem zasilania +12 V, co upraszcza układ zasilania.

Oprócz bardzo istotnej sekcji analogowej, mikrokontroler sterujący graficznym wyświetlaczem TFT z interfejsem SPI powinien być stosunkowo szybki. Niestety, z tym nie jest najlepiej. Niezbyt szybki, 16-bitowy rdzeń PIC24F taktowany częstotliwością 16 MHz to istotne ograniczenie i dlatego zastosowano ekran o relatywnie małej rozdzielczości 128×160 pikseli, niewymagający przesyłania przez SPI dużych ilości danych przeznaczonych do wyświetlania. Chodziło o to, by interfejs użytkownika był w miarę responsywny. Lepszym wyborem byłby mikrokontrolery z rdzeniem ARM, np. STM32F4 lub ESP32, ale autorowi zależało na dobrej jakości sekcji analogowej zintegrowanej w jednym mikrokontrolerze. Ostatecznie, po zastosowaniu zabiegów optymalizacyjnych, PIC24F poradził sobie z tym zadaniem.

Wykaz elementów:

Część cyfrowa
Rezystory: (SMD1206, 1%)
R1...R10, R14, R15: 1 kΩ
R11...R13: 100 Ω

Kondensatory:
C1...C7, C14: 100 nF (SMD 1206)
C8: 10 nF (SMD 1206)
C9...C13, C15: 10 µF (tantalowy SMD)

Półprzewodniki:
D1: dioda LED RGB
U1: PIC24FJ128GC006-I/PT
U2: MIC5207-3,3YM5-TR
U3: AMS1117-3,3
U4: LM7805
U5: AT24C32D-SSHM-T

Pozostałe:
J1, J2: gniazdo IDC 16 pinów (raster 2,54 mm)
J3: goldpin 1×5 (raster 2,54 mm)
J5: goldpin 1×6 (raster 2,54 mm)
J6: goldpin 1×2 (raster 2,54 mm)
J7: gniazdo IDC 8 pinów (raster 2,54 mm)
SW1, SW2: enkoder obrotowy z przyciskiem
SW3, SW4: przycisk THT
Wyświetlacz LCD TFT 128×160 px ze sterownikiem ST7735S (wyprowadzenia goldpin 1×8)

Przetwornik analogowo-cyfrowy

Microchip wbudował w mikrokontroler nietypowy, 12-bitowy przetwornik nazwany *High Speed Pipeline A/D Converter*, czyli przetwornik analogowo-cyfrowy z przetwarzaniem potokowym. W typowym konwerterze SAR faza próbkowania to czas, w którym kondensator próbkujący (S/H) konwertera analogowo-cyfrowego jest podłączony do analogowego wyprowadzenia wejściowego. Proces próbkowania jest uruchamiany przez obwody przetwornika analogowo-cyfrowego na przykład poprzez programowe wymuszenie konwersji. Dla każdego konwertera jest zdefiniowany minimalny czas próbkowania, który gwarantuje, że kondensator S/H zapewni wystarczającą dokładność konwersji analogowo-cyfrowej. Zdarzenie wyzwalające konwersję A/C rozpoczyna odliczanie czasu próbkowania. Po upływie tego czasu układy sprzętowe przetwornika automatycznie rozpoczynają konwersję, a jej czas jest potrzebny przetwornikowi analogowo-cyfrowemu na przekonwertowanie napięcia utrzymywanego przez kondensator S/H na postać cyfrową. Sekwencja czasowa konwersji A/C typu SAR została pokazana na **rysunku 13**.

Główną różnicą między przetwornikami analogowo-cyfrowymi z przetwarzaniem potokowym, a przetwornikami z rejestrem aproksymacji sukcesywnej (SAR) jest szybkość. W typowej konwersji opartej na SAR, cyfrowa część procesu generowania wyników odbywa się szeregowo i zazwyczaj tylko jeden komparator analogowy jest używany do konwersji jednego bitu danych wynikowych na cykl zegara analogowo-cyfrowego. Konwerter potokowy używa wielu wewnętrznych komparatorów analogowych pracujących równolegle, aby umożliwić przetwarzanie wielu wyników na kilku różnych etapach konwersji. Umożliwia to wykonywanie jej w sposób „potokowy" (tj. każda konwersja jest ściśle etapowana, jedna po drugiej). W rezultacie układ może generować jeden wynik konwersji na każdy okres zegara analogowo-cyfrowego (TAD).

Duża szybkość to podstawowa zaleta, ale główną wadą przetwornika analogowo-cyfrowego typu pipeline jest wyższy poziom szumów w porównaniu z przetwornikami SAR. W praktyce, aby uzyskać pożądane rezultaty, pobiera się i uśrednia wiele próbek. W naszym urządzeniu nie potrzebujemy dużej szybkości, ale przydałby się niski poziom szumów. Zgodnie z sugestią, w programie obsługującym konwersję zastosowałem uśrednianie 32 próbek.

Przetworniki cyfrowo-analogowe

Mikrokontroler ma wbudowane dwa niezależne moduły przetworników cyfrowo-analogowych: DAC1 i DAC2. Każdy z modułów ma rozdzielczość 10 bitów, czyli dane wejściowe mają postać 10-bitowej wartości cyfrowej, zapisywanej w formacie wyrównania do lewej lub prawej strony. Sygnał wyjściowy to napięcie analogowe, proporcjonalne do cyfrowej wartości wejściowej. Moduł może generować napięcia wyjściowe między napięciem AVSS a skonfigurowanym dodatnim napięciem odniesienia DAC. U nas odniesieniem jest napięcie AVDD (+3,3 V) podane na port RB0 (DVREF+). Wyzwolenie konwersji następuje po zapisaniu nowej wartości do rejestru danych modułu.

Wyświetlacz

Wyświetlacz zastosowany w projekcie ma wbudowany, dość popularny sterownik ST7735S komunikujący się z mikrokontrolerem przez interfejs SPI. Blok SPI mikrokontrolera PIC24FJ128GC006 pracuje tutaj z częstotliwością zegara równą 16 MHz. Interfejs wyświetlacza jest zbudowany z linii:

- zegara (SCK),
- wyjścia danych z MCU (MOSI),
- linii D/C identyfikującej rodzaj danych przesyłanych do sterownika (D/C=0 – kod komendy, D/C=1 – dane do wyświetlenia),
- linii zerowania (RES).

Dodatkowo wyświetlacz ma także wyprowadzoną linię BL do sterowania podświetleniem: stan wysoki na tym wyprowadzeniu włącza podświetlenie.

Interfejs użytkownika

Interfejs użytkownika (**fotografia 1**) ma zadanie umożliwić interakcję operatora ze sterownikiem zasilacza i jest zbudowany z:

- enkodera obrotowego opisanego jako SET_U, ustawiającego napięcie wyjściowe z zakresu od +1 V do +24 V ze skokiem 0,5 V,
- drugiego enkodera obrotowego SET_I do ustawiania poziomu zabezpieczenia prądowego w zakresie od 50 mA do 1000 mA, ze skokiem co 50 mA,
- przycisku do sterowania przekaźnikiem wyjściowym złączającym i wyłączającym napięcie wyjściowe,
- ekranu wyświetlacza LCD pokazującego: zmierzone/ustawione napięcie wyjściowe – górny wiersz, prąd wyjściowy – środkowy wiersz i nastawioną wartość ograniczenia prądowego – dolny wiersz.

Obsługa zasilacza została maksymalnie uproszczona, ale z zachowaniem zasad ergonomii, stąd zastosowanie dwóch niezależnych enkoderów do regulacji napięcia wyjściowego i nastawy ogranicznika prądowego. Skok zmiany napięcia wyjściowego co 0,5 V to wynik doświadczeń z eksploatacji zasilaczy używanych przez autora – mniejszy skok zazwyczaj nie jest potrzebny, a wymaga większej liczby kroków nastaw. Można było użyć jednego enkodera do zgrubnej zmiany napięcia co 1 V, a drugiego do dokładniejszej (np. co 0,2 V), a zabezpieczenie prądowe ustawiać na przykład po naciśnięciu ośki jednego z enkoderów. Konfiguracja sprzętowa sterownika umożliwia takie sterowanie, więc jest to tylko kwestia oprogramowania. Jak wspomniano, obecna konfiguracja interfejsu sterującego jest zdaniem autora optymalna.

Fotografia 1. Płyta czołowa interfejsu użytkownika

Po włączeniu zasilania układu przekaźnik podający napięcie na wyjście zasilacza jest wyłączony. Napięcie na wyjściu może się pojawić dopiero po przyciśnięciu przycisku START. Kolejne przyciśnięcia START powodują sekwencyjne włączanie i wyłączanie. Wyłączenie przekaźnika wyjściowego i odcięcie wyjścia zasilacza od układu tuż po włączeniu zasilania sieciowego zabezpiecza też przed pojawieniem się na wyjściu zasilacza napięć stanów nieustalonych, generowanych w czasie stabilizacji parametrów pracy pętli regulacji napięcia wyjściowego.

W kolejnym kroku wartości napięcia wyjściowego i ograniczenia prądowego, zapisane przed wyłączeniem zasilania, są odczytywane z pamięci EEPROM i ustawiane przez przetworniki DAC. Po tych czynnościach sterownik sekwencyjnie mierzy napięcie i prąd na wyjściu oraz sprawdza, czy został przyciśnięty przycisk START lub obrócona oska jednego z enkoderów. Jeżeli tak, to odpowiednio reaguje na te zdarzenia, przełączając przekaźnik wyjściowy, zmieniając napięcie wyjściowe lub wartość zabezpieczenia prądowego.

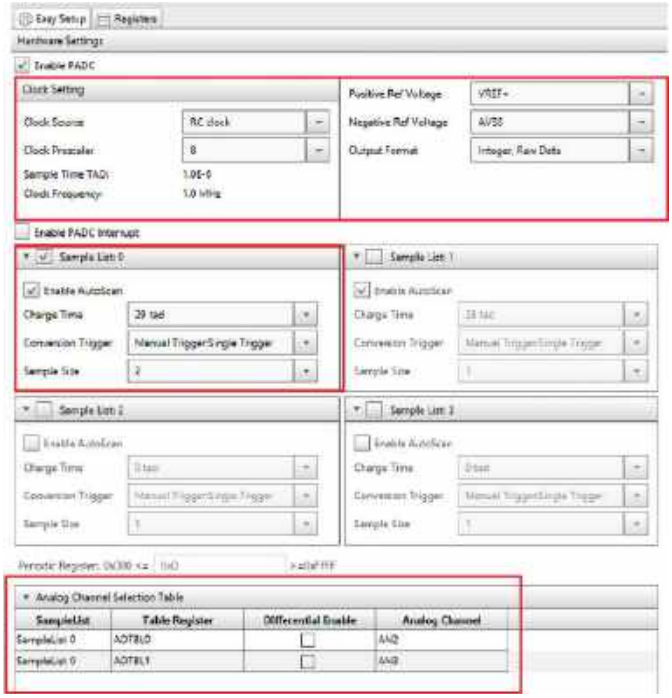
Oprogramowanie sterownika

Program sterujący został napisany w języku C i uruchomiony w środowisku MPLAB X IDE. Wykorzystałem tu darmową, w pełni funkcjonalną wersję kompilatora MPLAB XC16, która jest dostępna na stronie firmy Microchip. Na płytce drukowanej sterownika, na złączu ICSP, są wyprowadzone sygnały dla programatora/debuggera w standardzie urządzeń z rodziny Pickit. W trakcie pracy nas oprogramowaniem autor użył Pickit 4, który jest w pełni zintegrowany ze środowiskiem MPLAB X IDE i realizuje programowanie pamięci mikrokontrolera oraz funkcje debuggera. Bardzo pomocnym elementem w trakcie pracy nad programem okazała się wtyczka MCC, przeznaczona do konfigurowania układów peryferyjnych. Chociaż Microchip od dłuższego czasu bardzo oszczędnie dokumentuje procedury generowane przez MCC i często jest z tym problem, to i tak okazuje się to bardzo dużym ułatwieniem.

Przetwornik analogowo-cyfrowy – programowanie

Układ konfiguracji przetwornika potokowego jest dość skomplikowany i zawiera dużą liczbę rejestrów konfiguracyjnych. Jak już wspomniano, w projekcie użyto do konfiguracji wtyczki MCC.

Na **rysunku 14** pokazano okno konfiguracyjne przetwornika PADC.



Rysunek 14. Okno konfiguracyjne PADC

W pierwszym oknie od góry konfiguruje się podstawowe parametry pracy przetwornika:

- źródło zegara taktującego przetwornik i częstotliwość taktowania;
- dodatnie i ujemne napięcia referencyjne. W naszym przypadku dodatnim napięciem referencyjnym jest napięcie podane na linie portu RB0 (VREF+), a ujemnym – potencjał masy (AVSS);
- format danych wyjściowych. W naszym przypadku są to surowe dane 12-bitowe typu integer (liczba całkowita bez znaku).

Znaczenie tych danych konfiguracyjnych jest jasne i nie wymaga komentarza. Wyjaśnienia potrzeba za to odnośnie sekcji konfiguracji opisanej jako *Sample List* 0…3. Nie jest to bowiem, jak mogłoby się wydawać, konfiguracja bufora przeznaczonego do zapisywania próbek.

W wielu projektach pożądane jest skonfigurowanie przetwornika analogowo-cyfrowego do automatycznego próbkowania

```
void PADC1_Initialize(void)
{
 // ADSLP disabled; ADSIDL disabled; PWRLVL Low-Power mode; PUMPEN disabled; FORM Integer, Raw Data; ADCAL disabled; ADON enabled;
 ADCON1 = (0x8000 | 0x01) & 0x7FFF;            // Full power mode, Enable ADC later
 ADCON2 = (0x4000 | 0x0300);                   // NVCFG0 AVSS; PVCFG VREF+; REFPUMP disabled; BUFORG disabled;

 ADCON2bits.BUFORG = 1;                        // Result buffer organized as indexed mode
 BUFCON1 = 0x00;                               // BUFOE disabled; BUFSTBY Normal; BUFEN disabled; BUFSIDL disabled; BUFSLP disabled;
                                               // BUFREF 1.2 V;
 ADCON3 = 0x8004;                              // SLEN3 disabled; SLEN2 disabled; SLEN1 disabled; ADRC RC clock; SLEN0 disabled; ADCS 8;
                                               // Set Sample lists
 // MULCHEN One at a time; CTMEN disabled; CM Matching is disabled; SLINT No interrupt; WM All conversion results saved; SAMC 29 tad; ASEN
enabled;
 ADL0CONH = 0x801D;
 ADL0CONHbits.SLINT = 0x01;                    // interrupt after autoscan completion
 // THSRC Buffer register; SLTSRC Manual Trigger:Single Trigger; SLEN enabled; SLENCLR disabled; SLSIZE 2; SAMP disabled;
 ADL0CONL = (0x8001 & 0x7FFF) | 0x4000;        // open manual switch and Enable sample list later
                                               // Set table registers

 ADTBL0 = 0x2;                                 // UCTMU disabled; ADCH AN2; DIFF disabled;
 ADTBL1 = 0x3;                                 // UCTMU disabled; ADCH AN3; DIFF disabled;
                                               // Set table pointer registers

 ADL0PTR =0;
 ADL1PTR =0;
 ADL2PTR =0;
 ADL3PTR =0;
 ACCONL = 0x00;                                // TBLSEL ADTBL0; COUNT 0;
 ACCONH = 0x00;                                // ACIE disabled; ACEN disabled
 ADCON1bits.ADON = 1;                          // Enable ADC
 while(!(PADC1_IsReadyForConversion()));       // Poll the ADREADY bit
 ADCON1bits.ADCAL = 1;                         // Start calibration
 while(!(PADC1_IsReadyForConversion()));       // Poll the ADREADY bit
 ADTMRPR = 0x00;                               // Set ADC timer register
                                               // Enable sample list
 ADL0CONLbits.SLEN = 1;                        // Enable Sample list 1
 ADL0CONLbits.SAMP = 0;                        // Close sample switch
}
```

Listing 1. Konfiguracja PADC

i konwersji wielu kanałów wejściowych, bez ingerencji procesora przy każdej konwersji. We wcześniejszych układach PIC24F funkcja automatycznego skanowania umożliwiała próbkowanie i skanowanie wielu kanałów w sekwencji o ustalonej numeracji wejść. Dopóki moduł nie został ponownie zainicjalizowany, te same parametry próbkowania i konwersji były używane dla każdego kanału w trakcie sekwencji próbkowania. PADC oferuje tę samą funkcjonalność dzięki wykorzystaniu list próbek, a jednocześnie zapewnia znacznie szerszy zakres opcji skanowania i próbkowania. Listę próbek można traktować jako listę instrukcji dla modułu przetwornika, która informuje sprzęt, co ma robić podczas automatycznych operacji próbkowania i konwersji. Zawiera ona między innymi informacje o tym, które kanały analogowe mają być próbkowane, w jakiej kolejności, które źródło wyzwalania ma być użyte do zainicjalizowania próbkowania itp. Może również określać, czy grupa kanałów ma być próbkowana jednokrotnie, czy też powtarzalnie w pętli ciągłej.

PADC obsługuje do czterech list próbek, z których każda jest konfigurowalna. Pozwala to na niezależne ustawienie każdej listy próbek z jej własnymi ustawieniami próbkowania, konwersji, progów detekcji i generowania przerwań. Ponadto każda lista próbek jest monitorowana przez osobny rejestr statusu, który pokazuje aktualny stan zdarzeń wyzwalających i statusy przerwań. Włączona lista próbek może zawierać od jednego do maksymalnie 64 wpisów (zależnie od układu).

Chociaż w naszym przypadku doskonale sprawdziłaby się konfiguracja starszych PIC24F, to tu nie mamy wyjścia i musimy skorzystać z jednej z list (Sample List 0) konfigurującej konwersję dla dwóch kanałów analogowych AN2 i AN3, przeznaczonych do pomiaru napięcia i prądu wyjściowego zasilacza. Na szczęście, jeżeli przyswoi się powyższą wiedzę na temat roli list próbek, to nie jest to zadanie trudne, szczególnie z użyciem wtyczki MCC. Kolejność operacji do wykonania jest następująca:

- włączamy opcję Enable Auto Scan,
- w okienku Charge Time ustawiamy 29Tad,
- wybieramy pojedyncze wyzwalanie ręczne,
- rozmiar listy próbek ustawiamy na 2.

Aby przetwornik zmierzył napięcie w dwóch kanałach analogowych, musimy go za każdym razem programowo wyzwolić. Rozmiar listy próbek określa, dla ilu kanałów analogowych ta konfiguracja jest właściwa. Konkretne kanały analogowe dla naszej listy ustawia się w oknie Analog Channel Selection Table. W naszym przypadku będą to wejścia AN2 i AN3. Można też tu włączyć tryb wejścia różnicowego dla danego kanału (u nas ta opcja nie jest wykorzystywana).

Na podstawie okna z rysunku 14 MCC wygeneruje w pliku padc1.c kilka procedur pozwalających na obsługę przetwornika. Na **listingu 1** pokazano procedurę inicjalizacji modułu. Jest dość skomplikowana i jej ręczne wygenerowanie zajęłoby sporo czasu, szczególnie jeżeli robiłoby się to pierwszy raz.

Zainicjalizowany przetwornik ze skonfigurowaną listą próbek numer zero można użyć do konwersji napięć z wejść AN2 i AN3 na postać cyfrową. Ponieważ w konfiguracji wybraliśmy ręczny start konwersji, to trzeba wywołać funkcję PADC1_SampleList0ManualConversionStart rozpoczynającą konwersję z ustawieniami listy Sample List 0 – **listing 2**.

```
void PADC1_SampleList0ManualConversionStart(void)
{
 ADL0CONLbits.SAMP = 1;
 ADL0CONLbits.SAMP = 0;
}
```

Listing 2. Wyzwolenie konwersji z zerowej listy próbek

```
void GetPDAC(uint16_t *buffer)
{
 uint32_t buf_oversampling[2];
 uint8_t i;
 buf_oversampling[0] = 0;
 buf_oversampling[1] = 0;

 for (i= 0; i< 32; i++)
 {

 while(!(PADC1_IsReadyForConversion()));
 PADC1_SampleList0ManualConversionStart();
 while(!PADC1_IsBusyInConversion());

 PADC1_SampleList0ConversionResultBufferGet(buffer, 0, 2);
 buf_oversampling[0] = buf_oversampling[0]+ buffer[0];
 buf_oversampling[1] = buf_oversampling[1]+ buffer[1];
 }

 buffer[0] = buf_oversampling[0] /32;
 buffer[1] = buf_oversampling[1] /32;

 }
```

Listing 3. Odczyt wyniku konwersji kanałów AN2 i AN3

```
bool PADC1_SampleList0ConversionResultBufferGet (uint16_t *buffer, uint8_t tableRegIndex, u int8_t slSize)
{
 uint8_t index;
 bool dataValid = false;
 if (ADSTATLbits.SL0IF != 0)
 {
 For (index=0; index < slSize; index++)
 {
 buffer[index] = *((uint16_t *) & ADRES0 + tableRegIndex);
 tableRegIndex++;
 }
 ADL0STATbits.ADLIF = 0;
 dataValid = true;
 }
 return dataValid;
}
```

Listing 4. Odczytanie wyniku konwersji

```
double Measure_V (void)
{
 uint16_t buf[2];

 double voltage;
 GetPDAC(buf);
 voltage = (double)buf[1];
 voltage = (voltage/83.6) * 0.5;
 return voltage;
}
```

Listing 5. Procedura pomiaru napięcia wyjściowego

```
double Measure_I (void)
{
 double current;

 GetPDAC(buf);
 current = (current/203.5) * 50;
 }
 return current ;
}
```

Listing 6. Procedura pomiaru prądu wyjściowego

```
void DAC2_Initialize(void)
{
// DACREF DVREF+; DACFM Right; DACEN enabled; DACTSEL CMP1; DACTRIG disabled;
DACSLP disabled; DACSIDL disabled;
 DAC2CON = 0x8001;

}
```

Listing 7. Konfiguracja przetwornika DAC2

Pozostaje teraz poczekać na koniec konwersji i odczytać rejestry wyniku konwersji dla obu kanałów analogowych AN2 i AN3. Na **listingu 3** pokazano kompletną procedurę, która:

- czeka na gotowość modułu przetwornika na konwersję analogowo-cyfrową,
- wyzwala programowo konwersję (listing 2),
- czeka na zakończenie konwersji,
- odczytuje wyniki konwersji z kanałów AN2 i AN3.

Te czynności są wykonywane w pętli 32 razy, a wyniki konwersji dla każdego z kanałów są sumowane. Po wyjściu z pętli ta suma jest dzielona przez 32, co powoduje uśrednianie wyniku w celu ograniczenia szumu w sygnale z przetwornika PADC.

Odczyt rejestrów wyniku konwersji wykonuje procedura PADC1_SampleList0ConversionResultBufferGet z argumentami: wskaźnikiem na 32-bitowy bufor wyniku, numerem listy próbek i rozmiarem listy próbek.

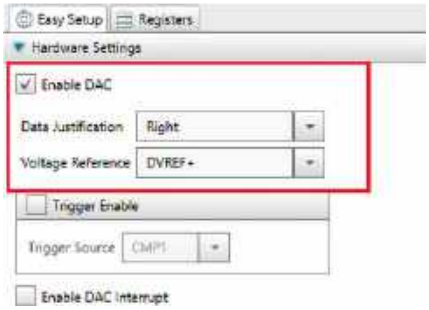
Na **listingu 5** pokazano procedurę pomiaru napięcia wyjściowego odczytującą wynik konwersji i wyliczającą na jej podstawie wartość napięcia wyjściowego. Przeliczanie 12-bitowej liczby na wartość napięcia odbywa się przy założeniu, że napięciu wyjściowemu odpowiada napięcie +3,3 V. Inaczej mówiąc, kiedy napięcie wyjściowe zasilacza ma wartość +24 V, na wejściu przetwornika panuje napięcie równe referencyjnemu, czyli +3,3 V.

Na podobnej zasadzie jest mierzony prąd wyjściowy – **listing 6**. Dla prądu 1000 mA napięcie na wejściu przetwornika wynosi +3,3 V.

Konfiguracja i obsługa przetworników DAC, w porównaniu z przetwornikiem PADC, jest banalnie prosta. Na **rysunku 15** pokazano okno konfiguracyjne wtyczki MCC. Możemy tu włączyć moduł, ustawić wyrównanie danych wejściowych (w tym przypadku do prawej) i wybrać źródło napięcia referencyjnego. Jeżeli nie odblokujemy sprzętowego wyzwalania (Trigger Enable), to każda konwersja DAC musi być wyzwalana programowo.

Konfiguracja polega na zapisaniu jednego rejestru konfiguracyjnego DACxCON – **listing 7**. Konwersja jest wyzwalana przez zapisanie rejestru DACxDAT – patrz **listing 8**. Ustawienie napięcia wyjściowego realizuje procedura SetV z argumentem stepv (**listing 9**) – argument ten jest indeksem tablicy VSet, w której są zapisane wartości wysyłane do przetwornika DAC, a zarazem indeksem drugiej tablicy VSetCor, zawierającej wartości korekcji. To rozwiązanie pozwala na ustawianie napięcia w krokach co 0,5 V i korygowanie ewentualnych błędów przetwarzania przetwornika, szczególnie na początku zakresu.

Pętla główna programu jest stosunkowo prosta. Na początku mierzone i wyświetlane są wartości napięcia i prądu wyjściowego. Potem program sprawdza, czy nie zostały obrócone enkodery ustawiania napięcia lub poziomu zabezpieczenia prądowego, a także czy został przyciśnięty przycisk START (**listing 10**). W obecnej wersji programu nie przewidziano żadnych dodatkowych funkcji i menu.



Rysunek 15. Okno konfiguracyjne przetworników DAC

```
void DAC2_OutputSet (uint16_t inputData)
{
 DAC2DAT = inputData;
}
```

Listing 8. Wyzwolenie konwersji DAC2

```
void SetV (uint8_t stepv)
{

 DAC1_OutputSet( VSet[stepv] + VSetCor [stepv] );

}
//tablica ustawiania napięcia zasilacza
const int16_t VSet [] =
{

 0,21,42,63,84,
 105,126,147,168,
 189,210,231,252,
 273,294,315,336,
 357,378,399,420,
 441,462,483,504,
 525,546,567,588,
 609,630,651,672,
 693,714,735,756,
 777,798,819,840,
 861,882,903,924,
 945,966,987,1008,
};
```

Listing 9. Procedura ustawiania napięcia wyjściowego z tablicą VSet

Budowa zasilacza, montaż i uruchomienie

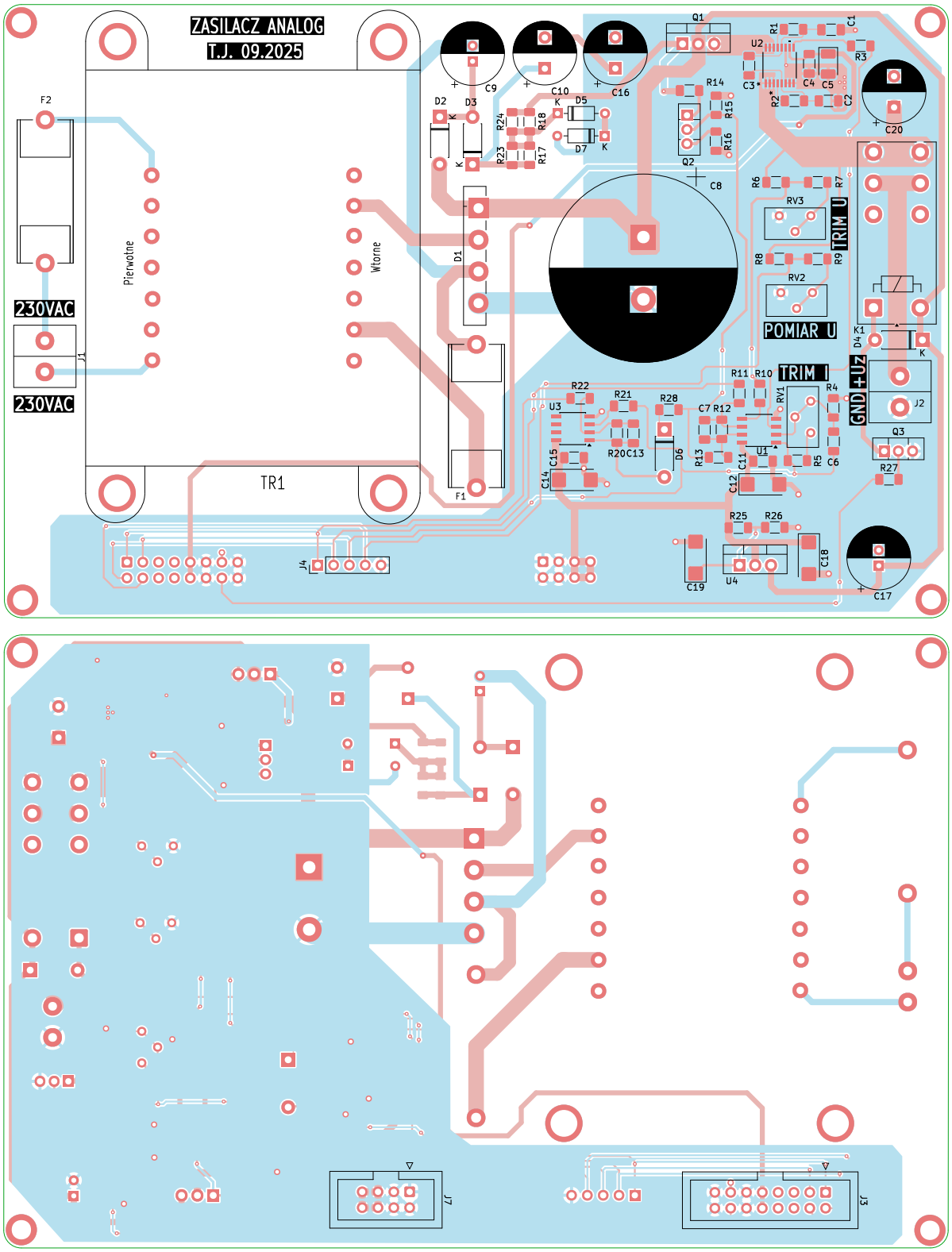
Z założenia zasilacz miał być urządzeniem kompaktowym, dlatego transformator o napięciu wyjściowym +24 V i prądzie 1 A został umieszczony na płytce drukowanej sekcji analogowej. Projekt

```
while (1)
 {
 //pomiar i wyświetlenie prądu wyjściowego
 current = Measure_I();
 HMI_CurrentDisplayFast (16, 53,current, RED, WHITE);

 //pomiar i wyświetlenie napięcia wyjściowego
 volt = Measure_V();
 HMI_VoltageDisplayFast (16,10,volt, BLUE, WHITE);

 //odczyt enkodera ustawiania napięcia
 key_v = HMI_GetEncoderV();
 //odczyt enkodera ustawiania ograniczenia prądowego
 key_i = HMI_GetEncoderI();
 //obsługa ustawienia napięcia
 if(key_v == KOD_IMP_UP_V)
 {
 ++Vstep;
 if (Vstep > 48)
 Vstep = 48;
 SetV (Vstep);
 volt = Measure_V();
 HMI_VoltageDisplayFast (16, 10, volt , BLUE, WHITE);
 }
 if(key_v == KOD_IMP_DWN_V)
 {
 --Vstep;
 if (Vstep < 1)
 Vstep = 1;
 SetV (Vstep);
 volt = Measure_V();
 HMI_VoltageDisplayFast (16, 10, volt, BLUE, WHITE)
 }

 //obsługa ustawienia prądu zabezpieczenia prądowego
 if(key_i == KOD_IMP_UP_I)
 {
 ++Istep;
 if(Istep > 19)
 Istep = 19;
 SetI(Istep);
 current_set = Istep * 50;
 HMI_OverCurrentDisplay (19, 100, current_set, GOLD, BLACK);

 }
 if(key_i == KOD_IMP_DWN_I)
 {
 --Istep;
 if(Istep <1 )
 Istep = 1;
 SetI(Istep);
 current_set = Istep * 50;
 HMI_OverCurrentDisplay (19, 100, current_set, GOLD, BLACK);

 }
 Sprawdzanie przyciśnięcia przycisku START i przełączanie przekaźnika wyjściowego
 HMI_Check_START_Button();

 }
```

Listing 10. Pętla główna programu

a)

b)



Rysunek 16. Projekt płytki sekcji analogowej: a – strona TOP, b – strona BOTTOM

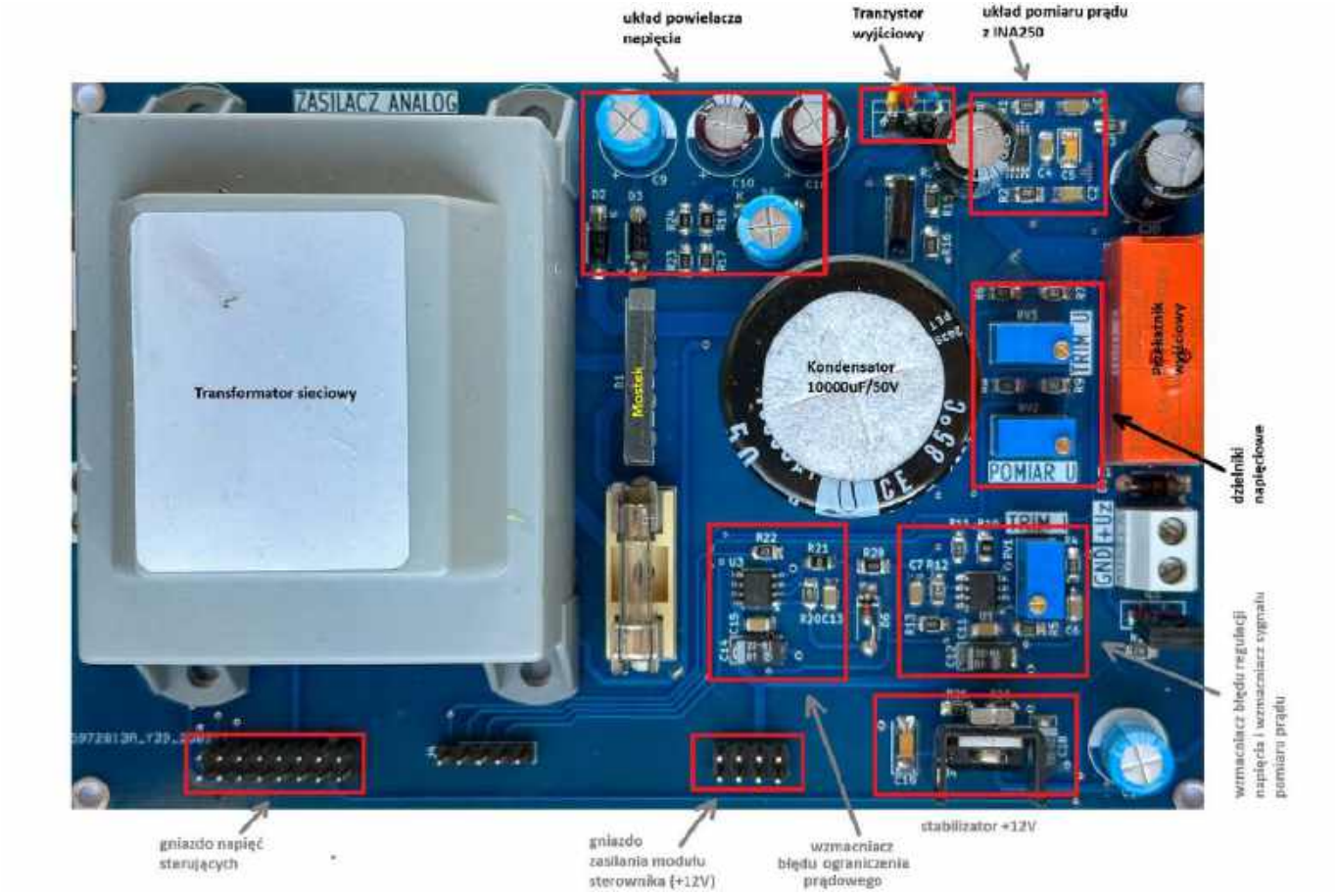
płytki pokazano na **rysunku 16**, a widok płytki z rozmieszczeniem poszczególnych układów na **fotografii 2**.

Elementy na płytce są przeznaczone do montażu przewlekanego i powierzchniowego. W pierwszej kolejności montujemy elementy od najmniejszych SMD do największych: przekaźnik, mostek prostowniczy, transformator i główny kondensator filtru.

Projekt płytki sterownika został pokazany na **rysunku 17**. Najtrudniejszym elementem do montażu będzie mikrokontroler w obudowie z 64 wyprowadzeniami w rastrze 0,5 mm. Jedną ze sprawdzonych metod jest użycie dobrego topnika w płynie i lutownicy z grotem typu minifala.

Po zasileniu układu z napięcia sieciowego 230 VAC sprawdzamy poprawność napięcia +12 V na złączu J7. Jeżeli jest poprawne, możemy połączyć moduł sekcji analogowej ze sterownikiem za pomocą płaskich kabli z zaciśniętymi wtyczkami IDC o rastrze 2,54 mm, zwracając przy tym uwagę na prawidłowe położenie wtyczek – **fotografia 3**.

Teraz sterownik jest zasilany napięciem +12 V i jeżeli wcześniej został zaprogramowany mikrokontroler, a montaż płytki sterownika został wykonany prawidłowo, to na wyświetlaczu sterownika powinien się pojawić ekran jak **fotografii 4**, ale oczywiście z innymi wartościami napięcia i prądu.



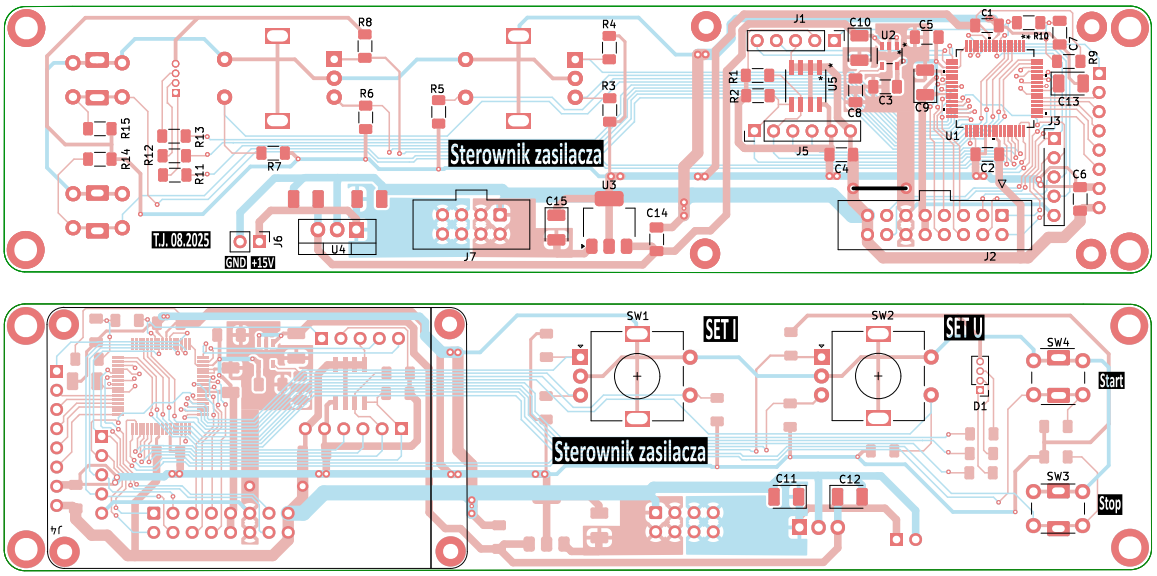
Fotografia 2. Zdjęcie płytki sekcji analogowej z rozmieszczeniem poszczególnych układów

Sterownik domyślnie po pierwszym uruchomieniu (po zaprogramowaniu pamięci Flash) ustawia napięcie wyjściowe równe +12 V i ograniczenie prądowe na 500 mA.

Następnie naciskamy przycisk START i podłączamy woltomierz do wyjścia zasilacza. Teraz potencjometrem wieloobrotowym opisanym na płytce jako TRIM_U ustawiany napięcie równe +12 V. Kręcenie enkoderem SET_U powinno zmieniać napięcie wyjściowe ze skokiem 0,5 V. Zwiększamy teraz napięcie wyjściowe do +24 V i ewentualnie korygujemy je potencjometrem TRIM U. Tę czynność można powtórzyć klika razy – tak, by napięcie

a)

b)



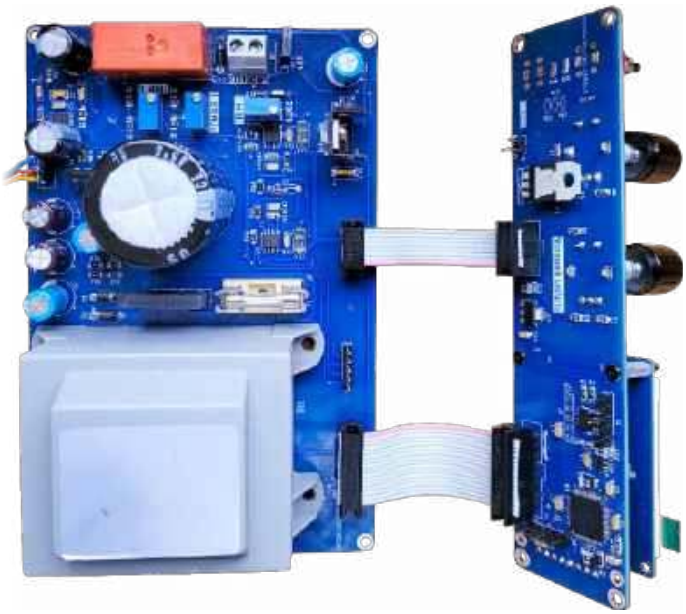
Rysunek 17. Projekt płytki sterownika zasilacza: a – strona TOP, b – strona BOTTOM

wyjściowe zmieniało się jak najdokładniej z krokiem 0,5 V. W prototypie konieczna była drobna korekta wartości tablicy VSetCor na końcach zakresów, szczególnie dla niskich napięć wyjściowych, co najprawdopodobniej było spowodowane nieliniowością przetwornika.

Teraz przechodzimy do kalibracji pomiaru napięcia wyjściowego, polegającej na takim ustawieniu wieloobrotowego potencjometru POMIAR_U, żeby wyświetlacz sterownika wskazywał dokładnie napięcie zmierzone multimetrem na wyjściu zasilacza.

Ostatnią czynnością jest ustawienie poprawnego pomiaru prądu wyjściowego. Układ INA250 mierzy prąd z wystarczającą dokładnością, ale na jego wyjściu mamy napięcie 0,8 V dla natężenia równego 1 A . Należy ten sygnał wzmocnić tak, by przy 1 A na wejściu przetwornika PADC panowało napięcie +3,3 V. Wzmocnienie napięciowe reguluje się wieloobrotowym potencjometrem TRIM I dokładnie ustalającym potrzebne wzmocnienie. Następnie obciążamy zasilacz prądem ok. 500 mA, a w szereg z obciążeniem włączamy amperomierz multimetru i tak ustawiamy TRIM I, aż prąd wyświetlany na ekranie wyświetlacza będzie równy wskazaniom amperomierza.

Tak wyregulowany zasilacz jest gotowy do pracy.



Fotografia 3. Połączenie płytki sekcji analogowej i sterownika

Podsumowanie

Na koniec możemy ponownie spróbować odpowiedzieć sobie na pytanie postawione na początku pierwszej części artykułu: czy warto samodzielnie budować takie urządzenie? Zaprojektowanie, wykonanie i oprogramowanie nawet tak relatywnie prostego urządzenia jak zasilacz warsztatowy, zajmuje mnóstwo czasu. Komercyjny koszt takiego przedsięwzięcia – zważywszy tylko na koszty pracy – jest tak duży, że za tę kwotę można kupić dobry lub nawet bardzo dobry, gotowy zasilacz. Ekonomicznie nie jest to w żaden sposób do obronienia, chyba że projekt miałby być produkowany w większej ilości. Ale w takim przypadku koszty opracowania jeszcze wzrosną. Prototyp trzeba by było pewnie trochę przeprojektować, usunąć drobne błędy, wprowadzić jakieś poprawki. Potem konieczne byłyby testy niezawodności, certyfikaty bezpieczeństwa itp. Do tego kosztowne opracowanie i wyprodukowanie mechaniki.

Jeżeli jednak będziemy rozpatrywać takie projekty w kategoriach zdobywania doświadczeń, szczególnie w projektowaniu urządzeń na styku techniki cyfrowej i analogowej, to może to być dobry poligon doświadczalny. A w kategoriach „Zrób to Sam” dochodzi do tego niemierzalna satysfakcja z własnoręcznie zaprojektowanego i wykonanego urządzenia. Dla sporej części entuzjastów to rzecz, którą trudno przecenić.

Tomasz Jabłoński, EP

Fotografia 4. Ekran wyświetlacza sterownika

Najważniejsze parametry:
- napięcie zasilania: 3,3...5,0 V,
- poziomy logiczne: 3,3...5,0 V,
- zdublowane złącza sygnałowe (gniazdo Grove + listwa goldpin),
- sygnały magistrali wyprowadzone na zaciski sprężynowe.

Projekty pokrewne na stronie www.ep.com.pl

(aktywne linki do artykułów):
- Izolowane moduły pomiarowe prądu i napięcia z interfejsem Grove
- Moduł pomiaru napięcia, prądu i mocy w standardzie Grove

* **Uwaga!** Elektroniczne zestawy do samodzielnego montażu. Wymagana umiejętność lutowania! Podstawową wersją zestawu jest wersja **[B]** nazywana potocznie KIT-em (z ang. zestaw). Zestaw w wersji **[B]** zawiera elementy elektroniczne (w tym **[UK]** – jeśli występuje w projekcie), które należy samodzielnie wlutować w dołączoną płytkę drukowaną (PCB). Wykaz elementów znajduje się w dokumentacji, która jest podlinkowana w opisie kitu. Mając na uwadze różne potrzeby naszych klientów, oferujemy dodatkowe wersje:

- **wersja [C]** – zmontowany, uruchomiony i przetestowany zestaw **[B]** (elementy wlutowane w płytkę PCB),
- **wersja [A]** – płytka drukowana bez elementów i dokumentacji.

Kity, w których występuje układ scalony wymagający zaprogramowania, mają następujące dodatkowe wersje:
- **wersja [A+]** – płytka drukowana **[A]** + zaprogramowany układ **[UK]** i dokumentacja,
- **wersja [UK]** – zaprogramowany układ.

Nie każdy zestaw AVT występuje we wszystkich wersjach! Każda wersja ma załączony ten sam plik PDF! Podczas składania zamówienia upewnij się, którą wersję zamawiasz! http://sklep.avt.pl

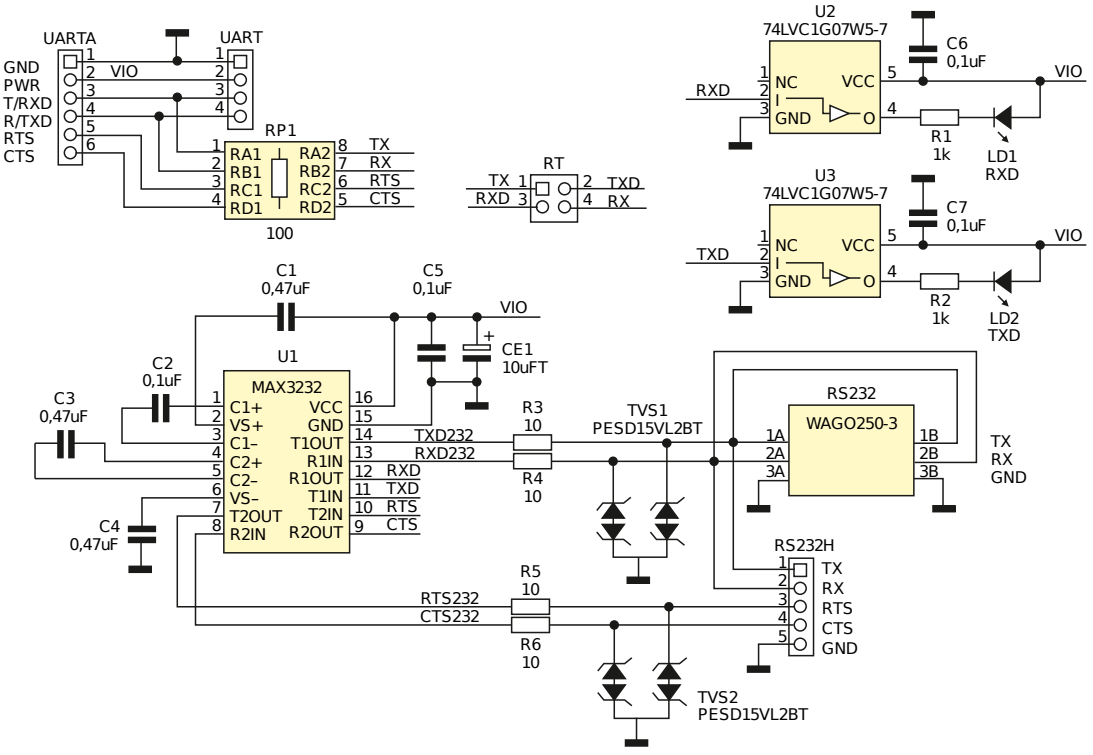
W przypadku braku dostępności na stronie sklepu osoby zainteresowane zakupem płytek drukowanych (PCB) prosimy o kontakt via e-mail: kity@avt.pl

Drivery magistral szeregowych RS232, RS422, RS485 zgodne z Grove

Pomimo postępu technologicznego i wprowadzenia szeregu szybkich i ultraszybkich sposobów komunikacji pomiędzy systemami mikroprocesorowymi, interfejsy RS232, RS485 i RS422 trzymają się dzielnie i nic nie wskazuje, aby nagle miały zniknąć z rynku. Dobrze mieć więc pod ręką kilka modułów ułatwiających szybkie prototypowanie, niezależnie od preferowanej platformy sprzętowej. Każdy z opisanych w artykule modułów może być zasilany napięciem 3,3...5 V, zapewniając przy tym pełną zgodność z systemami 3,3 V (np. Raspberry Pi czy Orange Pi) i 5 V (np. Arduino). Moduły zaprojektowano jako zgodne mechanicznie z systemem Grove, a złącza sygnałowe zostały dodatkowo powielone na listwach szpilkowych. Sygnały magistral RS wyprowadzono na wygodne w użyciu zaciski sprężynowe.

Pierwszym i podstawowym modułem jest driver magistrali RS232, którego schemat przedstawiono na **rysunku 1**.

W module zastosowano typowy driver U1 typu MAX3232, przystosowany do pracy w szerokim zakresie napięć zasilania 3,3...5,0 V. Sygnały interfejsu UART doprowadzone są do złącza UART zgodnego ze standardem Grove i powielonegonazłączuUARTA.U1 zawiera w sobie cztery drivery, dwa z nich (odbiorczy i nadawczy) wyprowadzone są na złącze sprężynowe typu WAGO250. Podstawowa para umożliwia realizację najczęściej używanej transmisji bez sprzętowego potwierdzenia. „Pełny" zestaw sygnałów koniecznych do realizacji transmisji ze sprzętowym potwierdzeniem z CTS/RTS, wyprowadzony jest na listwę szpilkową RS232H. Wszystkie sygnały magistrali RS232 zabezpieczono przed skutkami przepięć za pomocą diod TVS1,2. Zwora RT umożliwia zamianę sygnałów TX/RX,

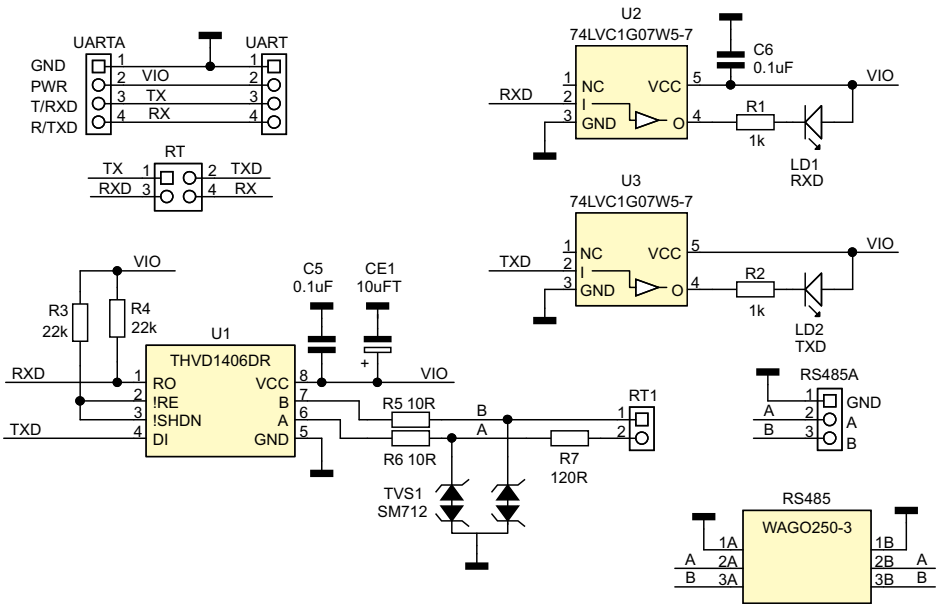


Rysunek 1. Schemat modułu Grove_RS232

co ułatwia podłączenie modułu przy wykorzystaniu gotowych przewodów Grove (nie jest wymagany „przeplot"). Układy U2,3 buforują diody LED sygnalizujące stany sygnałów RXD i TXD.

Drugim modułem jest driver magistrali RS485, którego schemat przedstawiono na **rysunku 2**.

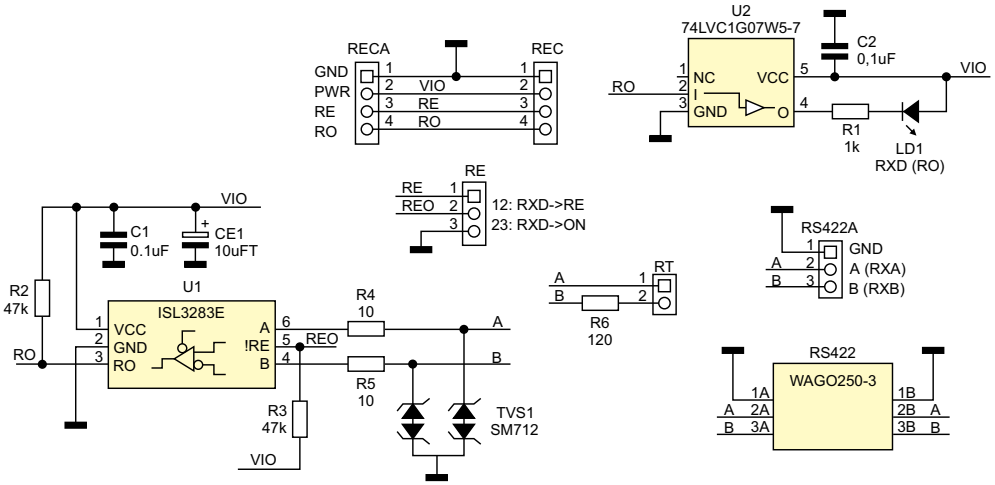
Moduł bazuje na układzie drivera U1 z automatyczną detekcją kierunku transmisji typu THVD1406 (500 kbps) lub szybszym THVD1426 (12 Mbps), co umożliwia rezygnację z sygnału wyboru kierunku DIR, znanego z „klasycznych" układów driverów RS485. Sygnały interfejsu UART doprowadzone są do złącza UART zgodnego z Grove oraz powielone są na złączu szpilkowym UARTA. Zwora RT, podobnie jak w przypadku drivera RS232, umożliwia krosowanie sygnałów RXD/TXD. Interfejs RS485 wyprowadzony jest na złącze sprężynowe RS485 i szpilkowe RS485A. Dioda TVS1 zabezpiecza driver przed skutkami przepięć. Zwora RT1 umożliwia terminację linii różnicowej za pomocą R7, co należy zastosować gdy moduł znajduje się na końcach magistrali RS485. Układy U2,3 buforują diody LED sygnalizujące stany sygnałów RXD, TXD.



Rysunek 2. Schemat modułu Grove_RS485

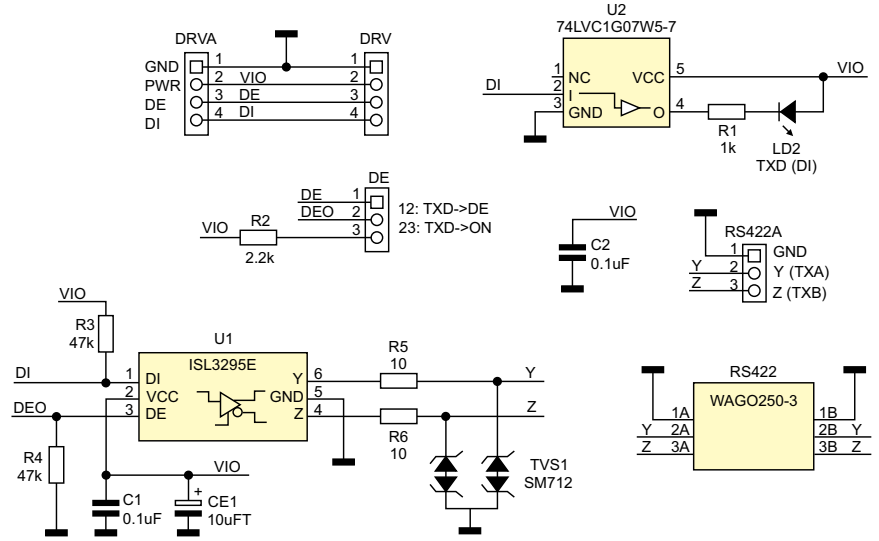
W przypadku, gdy chcemy zastosować magistralę RS422 lub wystarczy nam transmisja sygnału tylko w jednym kierunku, możemy użyć trzeciego i czwartego z opisanych modułów: Grove_RS422R_ISL3283E pełniącego funkcję odbiornika i Grove_RS422T_ISL3295E pracującego jako nadajnik magistrali RS422/485. Oba moduły, przy zastosowaniu szybkich driverów, mogą pełnić także funkcję różnicowych odbiorników/nadajników cyfrowego audio AES/EBU.

Schemat modułu odbiornika Grove_RS422R_ISL3283E przedstawiono na **rysunku 3**.



Rysunek 3. Schemat modułu odbiornika RS422 Grove_RS422R_ISL3283E

Magistrala RS422(485) doprowadzona jest do złącza sprężynowego RS422 oraz powielona na złączu szpilkowym RS422A, a stąd poprzez diodę zabezpieczającą TVS1 do układu odbiornika U1 typu ISL3283E (lub zgodnego MAX3283E). Zwora RT umożliwia podłączenie rezystora R6 terminującego magistralę. Układ U1 ma możliwość konfiguracji wyjścia odbieranych danych RO, co jest realizowane przy pomocy wejścia !RE. Gdy wejście to jest w stanie niskim, bufor wyjściowy pozostaje aktywny, natomiast po ustawieniu go w stan wysoki, bufor przechodzi w stan wysokiej impedancji, co umożliwia podłączenie kilku driverów do jednego portu UART. Za tryb pracy wyjścia RO odpowiada zwora RE. Ustawienie jej w położeniu 2-3 aktywuje wyjście RO na stałe, a po założeniu zworki na piny 1-2 możliwe jest sterowanie wejściem RO przy pomocy zewnętrznego sygnału RE. Wyjściowy sygnał odbiornika RO, sygnał sterujący RE oraz zasilanie wyprowadzone są na złącze REC w standardzie Grove i powielone są na złączu szpilkowym RECA. Układ U2 buforuje diodę LED sygnalizującą stan linii RO.



Rysunek 4. Schemat modułu nadajnika RS422 Grove_RS422T_ISL3295E

Wykaz elementów:

Grove_RS422R_ ISL3283E
Rezystory:
R1: 1 kΩ (SMD 0603, 1%)
R2, R3: 47 kΩ (SMD 0603, 1%)
R4, R5: 10 Ω (SMD 0603, 1%)
R6: 120 Ω (SMD 1206, 1%)

Kondensatory:
C1, C2: 100 nF (SMD 0603, 25 V, X7R)
CE1: tantalowy 10 µF (SMD 3216, 10 V)

Półprzewodniki:
LD1: dioda LED żółta (SMD 0603)
TVS1: transil SM712 (SOT-23)
U1: ISL3283E (SOT-23-6)
U2: 74LVC1G07W5-7 (SOT-25)

Pozostałe:
RE, RS422A: listwa SIP3 (R=2,54 mm)
REC: złącze Grove proste (110990030)
RECA: listwa SIP4 (R=2,54 mm)
RS422: złącze sprężynowe WAGO250-3
RT: listwa SIP2 (R=2,54 mm)

Grove_RS485
Rezystory:
R1, R2: 1 kΩ (SMD 0603, 1%)
R3, R4: 22 kΩ (SMD 0603, 1%)
R5, R6: 10 Ω (SMD 0603, 1%)
R7: 120 Ω (SMD 1206, 1%)

Kondensatory:
C5, C6: 100 nF (SMD 0603, 25 V, X7R)
CE1: tantalowy 10 µF (SMD 3216, 10 V)

Półprzewodniki:
LD1: dioda LED żółta (SMD 0603)
LD2: dioda LED czerwona (SMD 0603)
TVS1, TVS2: transil SM712 (SOT-23)
U1: THVD1406DR (SO8)
U2, U3: 74LVC1G07W5-7 (SOT-25)

Pozostałe:
RS485: złącze sprężynowe WAGO250-3
RS485A: listwa SIP3 (R=2,54 mm)
RT: listwa IDC4 (R=2,54 mm)
RT1: listwa SIP2 (R=2,54 mm)
UART: listwa SIP4 (R=2,54 mm)
UARTA: złącze Grove proste (110990030)

Grove_RS232
Rezystory:
R1, R2: 1 kΩ (SMD 0603, 1%)
R3...R6: 10 Ω (SMD 0603, 1%)
RP1: drabinka rezystorowa 100 Ω (CRA06S08)

Kondensatory:
C1, C3, C4: 470 nF (SMD 0603, 25 V, X7R)
C2, C5...C7: 100 nF (SMD 0603, 25 V, X7R)
CE1: tantalowy 10 µF (SMD 3216, 10 V)

Półprzewodniki:
LD1: dioda LED żółta (SMD 0603)
LD2: dioda LED czerwona (SMD 0603)
TVS1, TVS2: transil PESD15VL2BT (SOT-23)
U1: MAX3232 (TSSOP16_065)
U2, U3: 74LVC1G07W5-7 (SOT-25)

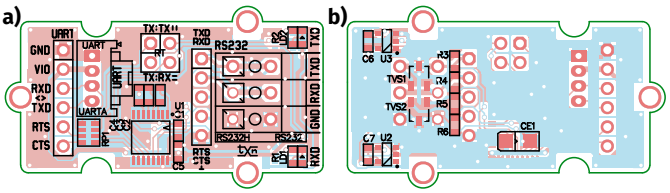
Pozostałe:
RS232: złącze sprężynowe WAGO250-3
RS232H: listwa SIP5 (R=2,54 mm)
RT: listwa IDC4 (R=2,54 mm)
UART: złącze Grove proste (110990030)
UARTA: listwa SIP6 (R=2,54 mm)

Grove_RS422T_ ISL3295E
Rezystory:
R1: 1 kΩ (SMD 0603, 1%)
R2: 2,2 kΩ (SMD 0603, 1%)
R3, R4: 47 kΩ (SMD 0603, 1%)
R5, R6: 10 Ω (SMD 0603, 1%)

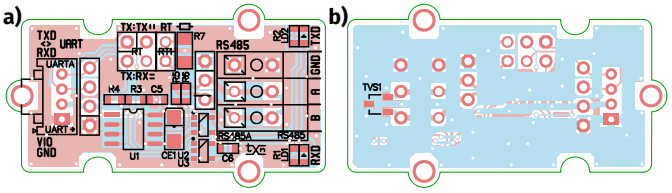
Kondensatory:
C1, C2: 100 nF (SMD 0603, 25 V, X7R)
CE1: tantalowy 10 µF (SMD 3216, 10 V)

Półprzewodniki:
LD2: dioda LED czerwona (SMD 0603)
TVS1: transil SM712 (SOT-23)
U1: ISL3295E (SOT-23-6)
U2: 74LVC1G07W5-7 (SOT-25)

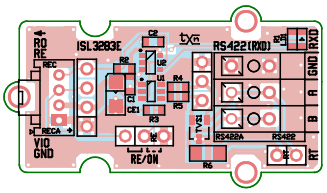
Pozostałe:
DE: listwa SIP3 (R=2,54 mm)
DRV: złącze Grove proste (110990030)
DRVA: listwa SIP4 (R=2,54 mm)
RS422: złącze sprężynowe WAGO250-3
RS422A: listwa SIP3 (R=2,54 mm)



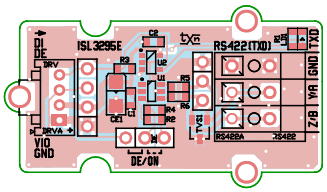
Rysunek 5. Rozmieszczenie elementów modułu Grove_RS232 (a – strona TOP, b – strona BOTTOM)



Rysunek 6. Rozmieszczenie elementów modułu Grove_RS485 (a – strona TOP, b – strona BOTTOM)



Rysunek 7. Rozmieszczenie elementów modułu Grove_RS422R_ISL3283E



Rysunek 8. Rozmieszczenie elementów modułu Grove_RS422T_ISL3295E

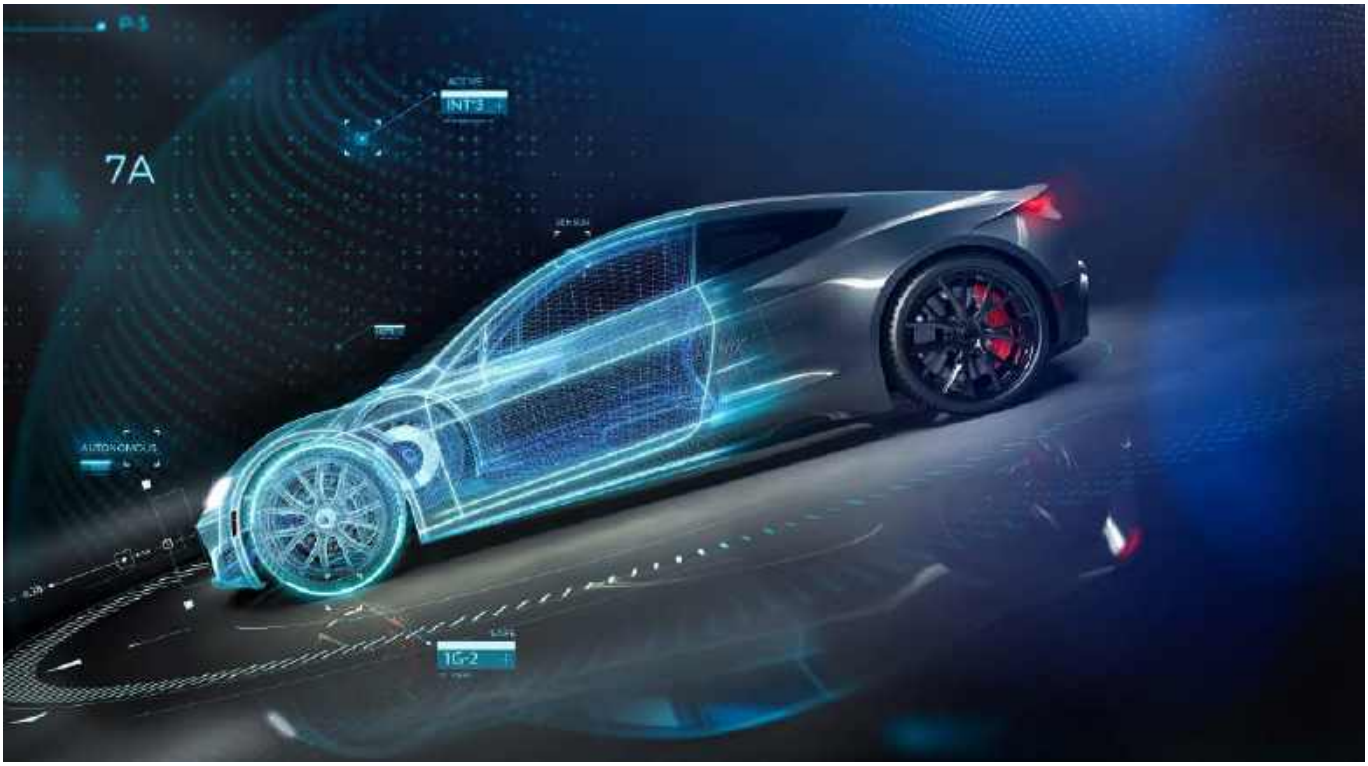
Ostatnim z prezentowanych w artykule modułów jest nadajnik magistrali RS422(485), którego schemat przedstawiono na **rysunku 4**.

W module zastosowano driver U1 typu ISL3295E (lub kompatybilny z nim MAX3295E). Sygnał z interfejsu UART doprowadzony jest do złącza DRV typu Grove i powielony na złączu szpilkowym DRVA. Sygnał transmisji DI doprowadzono bezpośrednio do drivera U1. Sygnał na wejściu DE o aktywnym stanie wysokim, sterujący trybem pracy bufora wyjściowego magistrali RS422 poprzez zworę DE, podłączono do układu U1. Ustawienie zwory w położeniu 2-3 aktywuje na stałe bufor wyjściowy nadajnika, co jest przydatne podczas używania transmisji RS422, gdy nadajnik połączony jest bezpośrednio z jednym lub wieloma odbiornikami. Ustawienie zwory DE w położeniu 1-2 umożliwia sterowanie buforem nadajnika poprzez sygnał DE – ten tryb pracy jest niezbędny, gdy do magistrali RS485 podłączonych jest wiele nadajników. Wyjścia nadajnika zabezpieczono diodą TVS1 i wyprowadzono na złącze sprężynowe RS422 oraz szpilkowe RS422A. Nadajnik pozbawiony jest terminatora magistrali, gdyż w przypadku RS422 wymagany jest on tylko po stronie odbiornika. W przypadku pracy modułu jako ostatniego elementu magistrali RS485, terminacja musi być zrealizowana zewnętrznym rezystorem podłączonym bezpośrednio do zacisków złącza RS422. Układ U2 buforuje diodę LED sygnalizującą stan linii DI.

Wszystkie moduły zmontowane są na miniaturowych, dwustronnych płytkach drukowanych zgodnych pod względem mechanicznym ze standardem Grove. Rozmieszczenie elementów przedstawiono na **rysunkach 5...8**. Montaż jest typowy i nie wymaga opisu. Zmontowane moduły pokazano na fotografii tytułowej.

Moduły nie wymagają uruchamiania, po montażu i poprawnym podłączeniu są od razu gotowe do pracy.

Adam Tatuś, EP



Wydajne mikrokontrolery, zintegrowane peryferia – recepta na wyzwania projektowe nowoczesnych systemów wbudowanych

Systemy wbudowane rozwijają się, obsługując coraz bardziej złożone aplikacje – od automatyki przemysłowej, poprzez inteligentne systemy w samochodach, aż po zaawansowane urządzenia IoT. Projektanci muszą w nich godzić wydajność, elastyczność i niezawodność. Możliwość skalowania rozwiązania i integracja różnorodnych peryferiów stanowią klucz do sprostania tym wyzwaniom i przyszłej rozbudowy projektów.

Wydajne przetwarzanie danych i obsługa zadań czasu rzeczywistego

Współczesne systemy wbudowane coraz częściej muszą przetwarzać dane w czasie rzeczywistym, wykonywać zaawansowane zadania analityczne i jednocześnie obsługiwać rozmaite protokoły komunikacyjne. Wymaga to nie tylko szybkiego rdzenia (na przykład ARM Cortex-M4F pracującego z częstotliwością do 128 MHz), ale również efektywnej architektury pamięci oraz niezawodnej obsługi przerwań.

Niezawodna praca i redukcja ryzyka projektowego

Niezawodność i minimalizacja ryzyka projektowego są krytycznie ważne w aplikacjach przemysłowych i motoryzacyjnych, w których układy muszą działać niezawodnie w szerokim zakresie temperatur i spełniać rygorystyczne normy, takie jak AEC-Q100 Grade 1. Wybór podzespołów i architektury systemu zapewniających stabilne działanie w tych warunkach jest zatem warunkiem koniecznym. Dodatkowo projektowanie toru radiowego wymaga szczegółowych testów i przeprowadzenia procesu certyfikacji, co zwiększa zarówno ryzyko projektowe, jak i koszty.

Zarządzanie złożoną łącznością i wymaganiami interfejsowymi

Rozwiązania nowej generacji często muszą komunikować się za pośrednictwem wielu przewodowych i bezprzewodowych protokołów, takich jak Bluetooth LE, Thread, CAN FD, Ethernet czy USB. Integracja tych interfejsów przy zachowaniu niskiego zużycia energii i wysokiej przepustowości danych stanowi poważne wyzwanie. Poleganie na wielu układach scalonych w celu obsługi różnych standardów zwiększa powierzchnię płytki PCB i podnosi całkowity koszt rozwiązania.

Architektura pamięci jako fundament elastyczności i bezpieczeństwa

Nowoczesne mikrokontrolery oferują znaczną pojemność pamięci wbudowanej, co ma niebagatelne znaczenie dla obsługi zaawansowanych stosów komunikacyjnych i protokołów bezpieczeństwa. Zwiększona pojemność umożliwia obsługę złożonych standardów radiowych, a także przechowywanie danych i funkcji

kryptograficznych dla bezpiecznej komunikacji. Ponadto ułatwia lokalne przetwarzanie danych, zmniejszając zależność od chmury i opóźnienia. Odpowiednio duża pamięć pozwala również obsługiwać aktualizacje oprogramowania metodą OTA, co upraszcza wprowadzanie nowych wersji firmware i poprawek bezpieczeństwa oraz przygotowuje urządzenia na przyszłe zmiany standardów. Bezpieczne składowanie kluczy kryptograficznych i kodu rozruchowego zwiększa bezpieczeństwo urządzeń, co jest szczególnie ważne w rozwiązaniach IoT wymagających wysokiego poziomu zaufania.

Przyspieszenie rozwoju i niezawodne działanie

Rozwiązania oferujące sprawdzone projekty referencyjne, wstępnie certyfikowane moduły radiowe i komponenty o kwalifikacji AEC-Q100 Grade 1 mogą istotnie zredukować ryzyko projektowe w aplikacjach przemysłowych i motoryzacyjnych. Taki pakiet skraca czas wprowadzenia produktu na rynek, ułatwia zapewnienie zgodności z wymaganiami normatywnymi i minimalizuje koszty certyfikacji. Gwarantuje także niezawodną pracę w szerokim zakresie temperatur, co daje producentom pewność spełnienia wymagań stawianych systemom o kluczowym znaczeniu.

Integracja peryferiów dla uniwersalności systemu

Mikrokontrolery o wysokim stopniu integracji łączą w ramach jednego chipu wiele peryferiów, takich jak CAN FD, Ethernet, USB, układy sterowania silnikami (QEI), akceleratory grafiki, obsługę dotyku oraz zaawansowane bloki analogowe (ADC/DAC). Pozwala to uprościć projekt płytki, skrócić listę elementów (BOM) i zapewnić elastyczną konfigurację systemu – a to z kolei umożliwia łatwe dostosowywanie do różnych wariantów produktu lub zmieniających się standardów. W efekcie projektant zyskuje możliwość wydajnego sterowania i monitorowania w czasie rzeczywistym, na przykład poprzez odczyt informacji zwrotnych z enkodera, pozyskiwanie danych z czujników itp. Bogate opcje interfejsów użytkownika z dotykowym sterowaniem i obsługą grafiki są dzięki temu osiągalne nawet w aplikacjach wrażliwych na koszty.

Przyszłość zaczyna się już dziś: zabezpiecz rozwój przyszłych generacji systemów wbudowanych

Wykorzystując skalowalne rozwiązania z obszerną pamięcią i zintegrowanymi peryferiami, projektanci mogą budować platformy, które obsługują szeroki zakres aplikacji i przyszłych aktualizacji, bez konieczności dokonywania zmian sprzętowych. Pozwala to sprostać wymaganiom wydajności i niezawodności w środowiskach przemysłowych i motoryzacyjnych, integrować zaawansowane interfejsy i łączność zgodne z obowiązującymi i nowo pojawiającymi się standardami oraz zwiększać bezpieczeństwo urządzeń przy zachowaniu zgodności z przepisami.

Na przykład jedna platforma mikrokontrolera może posłużyć zarówno do budowy inteligentnego czujnika przemysłowego, jak i modułu komunikacyjnego w samochodzie – wystarczy odpowiednio skonfigurować pamięć, włączyć potrzebne peryferia i zaktualizować oprogramowanie. Taki model upraszcza projektowanie, zmniejsza koszty i gwarantuje długoterminową elastyczność.

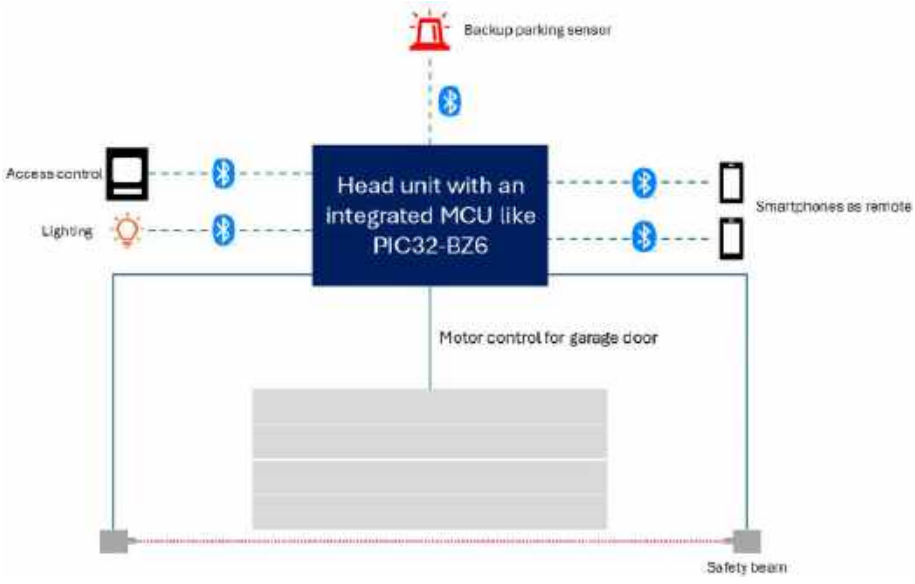
Podsumowanie

Pojemna pamięć i integracja peryferiów to nie tylko parametry produktu – to kluczowe elementy pozwalające sprostać wyzwaniom obecnym w projektowaniu nowej generacji systemów wbudowanych. Dzięki architekturom zapewniającym elastyczność, niezawodność i bezpieczeństwo, projektanci mogą tworzyć rozwiązania spełniające dzisiejsze wymagania i gotowe na jutrzejsze wyzwania.

Ramya Kota
Menedżer marketingu produktowego
Shishir Malav
Menedżer rozwoju biznesu
w grupie rozwiązań bezprzewodowych
firmy Microchip

Przykład: nowoczesny system bramy garażowej

Nowoczesne systemy bram garażowych wymagają bezpiecznej łączności bezprzewodowej, precyzyjnego sterowania silnikiem oraz przyjaznego interfejsu użytkownika, a całość musi mieścić się w kompaktowej i ekonomicznej konstrukcji. Mikrokontroler bezprzewodowy PIC32-BZ6 firmy Microchip odpowiada na te potrzeby dzięki pojemnej pamięci i obsłudze wielu protokołów. Interfejs Bluetooth Low Energy (BLE) umożliwia zdalny dostęp, a pamięci Flash o pojemności 2 MB i RAM o rozmiarze 512 kB pozwalają realizować zaawansowane algorytmy sterowania. Zintegrowane moduły PWM, precyzyjny przetwornik ADC wysokiej rozdzielczości i interfejs QEI zapewniają dokładne sterowanie silnikiem, sprzężenie zwrotne z czujników i niezawodny pomiar położenia. Dodatkowo wbudowane funkcje dotykowe i graficzne umożliwiają konstrukcję intuicyjnych klawiatur i wyświetlaczy. Jednoukładowe rozwiązanie, takie jak PIC32-BZ6, upraszcza projekt sprzętu, zmniejsza powierzchnię PCB i obniża koszt systemu, co czyni je idealnym rozwiązaniem dla nowej generacji bram garażowych.



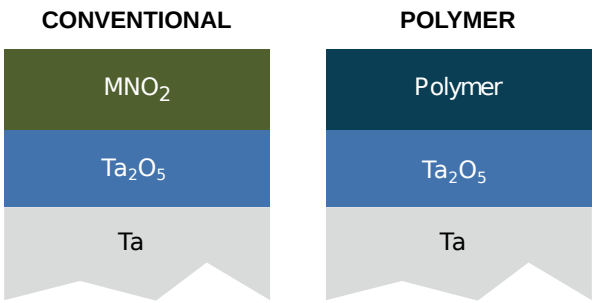
Kondensatory tantalowe

Kondensatory tantalowe – znamy je od lat, ale chyba nie do końca. Mają spore pojemności i zachęcające parametry, ale czy można je stosować bez większego zastanowienia? W tym artykule rozważam blaski i cienie tych popularnych elementów.

Dla uporządkowania faktów: kondensator tantalowy to taki, w którym dielektrykiem jest tlenek tantalu (V). Dzięki znacznie wyższej wartości względnej przenikalności elektrycznej (25…27) w stosunku do tlenku aluminium (III), dla którego wynosi ona 9…10, można budować kondensatory o mniejszych gabarytach w stosunku do typowych „elektrolitów". Na rynku mamy dostępne dwa rodzaje kondensatorów tantalowych: klasyczne, tudzież konwencjonalne (często po prostu bez żadnych dopisków) oraz polimerowe (te producenci wyraźnie już oznaczają). Mają nieco inny układ warstw w swojej strukturze – **rysunek 1** – zaś dokładniej różnią się materiałem katody, czyli elektrody ujemnej. W klasycznych wariantach jest to tlenek magnanu (IV), w polimerowych… właśnie polimer. Anodą, czyli elektrodą dodatnią, w obu wypadkach pozostaje czysty tantal.

Nie chcę się zagłębiać w szczegóły konstrukcji ani historię rozwoju takiego kondensatora, bo nie o tym jest ten artykuł – wolę skupić się na praktycznych aspektach jego jestestwa, czyli na tym, jaki pożytek możemy mieć z niego my, elektronicy. Na pewno w oczy rzucają się mniejsze ich gabaryty w stosunku do zwyczajnych kondensatorów elektrolitycznych, co ma potwierdzenie w twardych danych – **rysunek 2**. Tantalowe odpowiedniki potrafią mieć nawet pięć tysięcy (!) razy większy współczynnik CV, czyli iloczyn pojemności i napięcia w odniesieniu do objętości. Takich rekordzistów nieczęsto spotyka się w hurtowniach – z moich obserwacji wynika, że kondensatory tantalowe SMD (w formie prostopadłościennych kostek, jak na **rysunku 3**) mają objętość co najwyżej kilkukrotnie mniejszą w odniesieniu do kondensatorów elektrolitycznych. Niemniej jednak zawsze to jakiś plus.

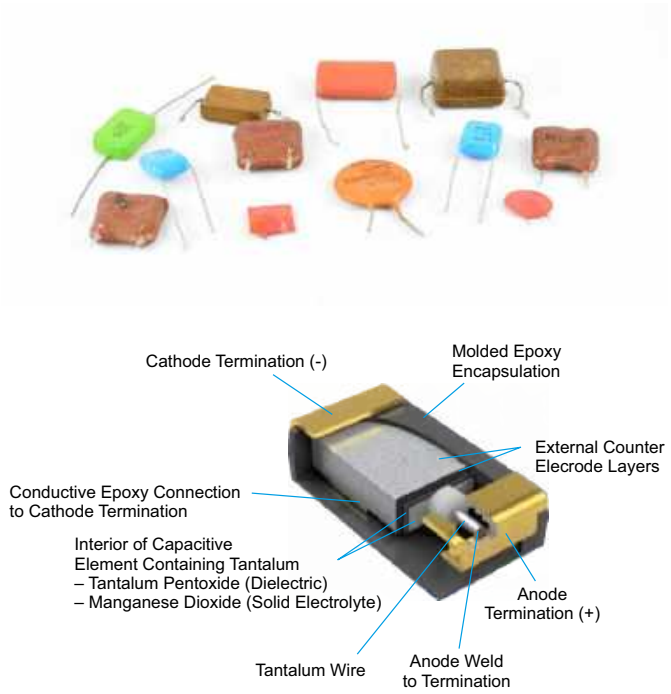
Mówi się o nich, że się nie starzeją. Jako główny powód jest wymieniany suchy elektrolit (nie ma więc co wyschnąć). Potwierdza to producent: na **rysunku 4** mamy zależność między odsetkiem uszkodzonych elementów w funkcji czasu. Po okresie „chorób wieku dziecięcego", kiedy to wychodzą na jaw wady produkcyjne zarówno



Rysunek 1. Układ warstw w tantalowym kondensatorze konwencjonalnym i polimerowym [1]

Capacitor	Package	Max CV
Tantalum Capacitor	SMD	63,0 mFv/mm³
Aluminum Can	Cylindrical	11,8 µFv/mm³
Aluminum Polymer	Stacked SMD	10,5 µFv/mm³

Rysunek 2. Porównanie współczynnika CV kondensatorów elektrolitycznych i tantalowych [1]



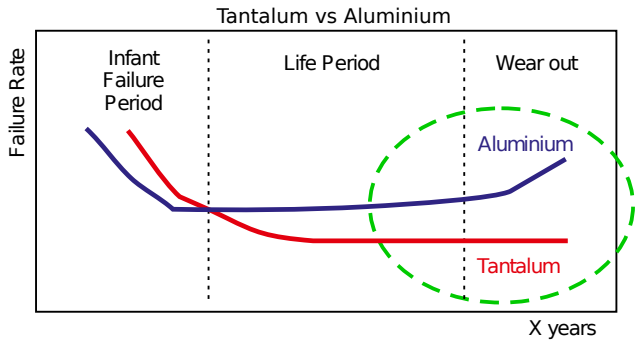
Rysunek 3. Budowa kondensatora tantalowego w obudowie SMD [1]

kondensatorów tantalowych, jak i elektrolitycznych (pierwsza część wykresu), uszkodzenia tych pierwszych zdarzają się później sporadycznie. Z kolei elektrolityczni kuzyni po pewnym czasie zaczynają się masowo „sypać", co widać bardzo dobrze po płytach głównych komputerów albo zasilaczach impulsowych.

Z mojego doświadczenia wynika, że taka zależność dla kondensatorów tantalowych może być zachowana, o ile nie zostaną one przegrzane podczas lutowania. Lutując te kondensatory przy użyciu pasty i gorącego powietrza muszę bardzo uważać na temperaturę oraz czas grzania tych elementów, zdecydowanie bardziej niż przy elementach uznawanych powszechnie za łatwe do przegrzania, jak mikrokontrolery czy pamięci elektroniczne. Jeżeli tego nie dopilnuję, średnio co trzeci kondensator dostaje zwarcie natychmiast, co jest – moim zdaniem – szokująco wysokim odsetkiem. Bywa też, że taki kondensator, który nawet nie odmówił współpracy natychmiast, co objawia się wspaniałym wprost zwarciem, potrafi zrobić zwarcie po kilkunastu lub kilkudziesięciu godzinach pracy. Jeżeli w tym czasie nie zrobi psikusa, to z reguły działa już bezproblemowo. Przez jakiś czas myślałem, że kondensatory w żółtych obudowach (spotykane najczęściej) są w jakiś sposób bardziej wrażliwe od czarnych, ale nie zauważyłem szczególnej różnicy na korzyść którejś ze stron.

Dlatego montując ręcznie prototypy lub niewielkie serie, staram się je lutować przy użyciu zwykłego spoiwa lutowniczego (w formie drutu) i lutownicy kolbowej. Co ciekawe, przy montażu w fabrykach SMD ten problem niemal nie występuje, w każdym razie nie częściej niż uszkodzenia innych podzespołów.

Kondensatory elektrolityczne mają powszechnie znaną, wysoką zależność między pojemnością a napięciem, tudzież między pojemnością a temperaturą. Z tego powodu nie stosuje się ich w układach czasowych, które mają mieć dokładność większą niż budzik wykonany z woskowej świecy. Na **rysunku 5** można zobaczyć – nieco wyidealizowane, ale oddające istotę problemu – porównanie kondensatorów MLCC (czyli najpopularniej występujących dzisiaj „ceramików" z dielektrykiem typu X7R lub podobnym)

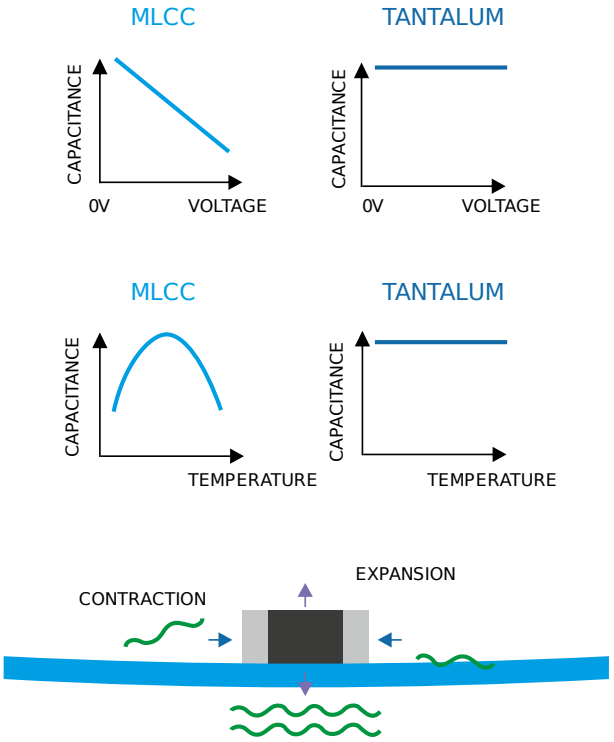


Rysunek 4. Odsetek uszkodzeń w funkcji czasu [1]

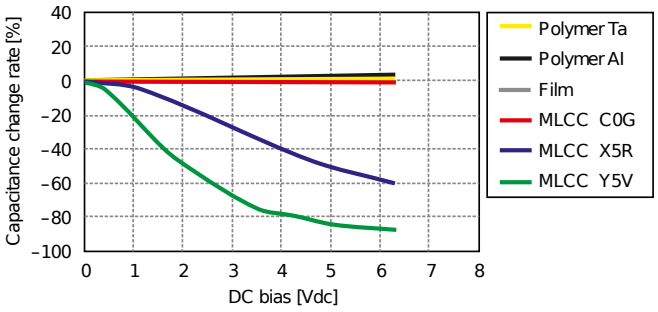
z tantalowymi. Jako największa zaleta jest wskazywana stałość pojemności zarówno w funkcji temperatury, jak i napięcia. Pojemność wielowarstwowych kondensatorów ceramicznych w funkcji temperatury potrafi zmieniać się w różny sposób, zależnie od użytego dielektryka, więc faktycznie taki kondensator tantalowy jest czymś „lepszym" na ich tle. Również pojemność w funkcji napięcia różnie zmienia się w MLCC: dla dielektryka C0G ta zmiana jest praktycznie pomijalna, X5R wykazuje spadek, zaś Y5R już niemal zupełnie traci pojemność po spolaryzowaniu napięciem równym nominalnemu (6,3 V) – **rysunek 6**.

Na rysunku 5 można zobaczyć wizualizację jeszcze jednej zalety kondensatorów tantalowych w stosunku do ceramicznych – brak zjawiska elektrostrykcji. Wynika to z ich odmiennej budowy, ponieważ zamiast wielu cienkich warstw ułożonych naprzemiennie w bardzo regularny sposób, stanowią skupisko wielu nieregularnie ułożonych struktur, co można zobaczyć na **rysunku 7**. Dlatego siły elektrostatyczne oddziałujące między tymi strukturami nie będą parły wszystkie w tym samym kierunku, sumując się – owo chaotyczne ułożenie spowoduje wzajemne zniesienie się odkształceń.

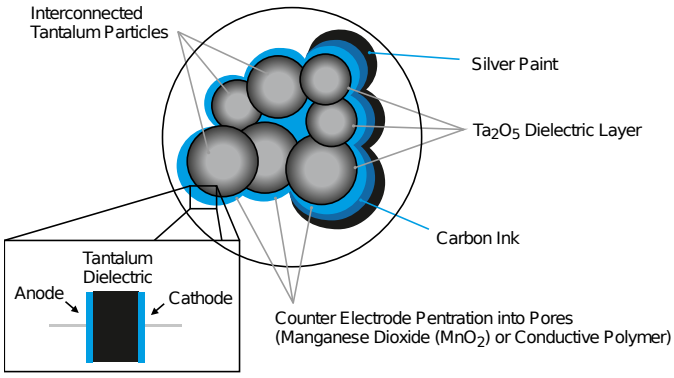
W dokumencie [1] znajduje się tabela podsumowująca wady i zalety kondensatorów elektrolitycznych aluminiowych, polimerowych aluminiowych, ceramicznych i tantalowych. Oprócz wspomnianych już zalet „tantali" przytoczono w niej również to, że kondensatory tantalowe cechują się efektem autoregeneracji, czego ja w mojej



Rysunek 5. Porównanie parametrów kondensatorów MLCC i tantalowych [1]



Rysunek 6. Zależność pojemności w funkcji napięcia dla różnych typów kondensatorów [2]

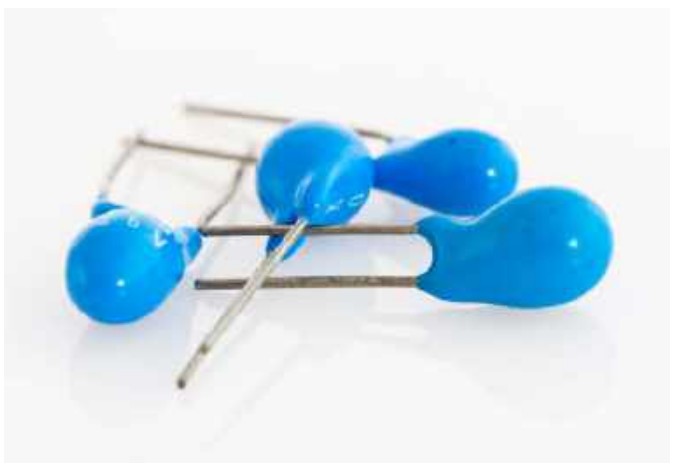


Rysunek 7. Mikrostruktura kondensatora tantalowego [1]

praktyce nie doświadczyłem (lub nie byłem tego świadom) – każde przekroczenie dopuszczalnego napięcia lub zamiana polaryzacji kończyła się nieodwracalnym zniszczeniem elementu na skutek zwarcia. I to jest, moim zdaniem, spora wada kondensatorów tantalowych: o ile zwykłe „elektrolity" zazwyczaj kończą swój żywot utrzymując pojemność rzędu kilku procent nominalnej (z powodu wyschnięcia), ale rzadziej dochodzi w nich do zwarcia, o tyle „tantalom" zdecydowanie częściej zdarza się zewrzeć swoje wyprowadzenia, co może poważnie uszkodzić pozostałe podzespoły w układzie. Dlatego w mojej praktyce urządzenia z kondensatorami tantalowymi pozostawiam dla celów testowych włączone przez kilka godzin pod obserwacją, ponieważ w tym czasie ma miejsce zdecydowanie największa liczba przykrych zdarzeń będących ich udziałem. Po tym okresie z reguły można im już zaufać.

Michał Kurzela, EP

Źródła:
[1] https://www.kyocera-avx.com/docs/techinfo/Tantalum-NiobiumCapacitors/Tantalum-Capacitors-Characteristics-and-Component.pdf
[2] https://article.murata.com/en-eu/article/voltage-characteristics-of-electrostatic-capacitance/

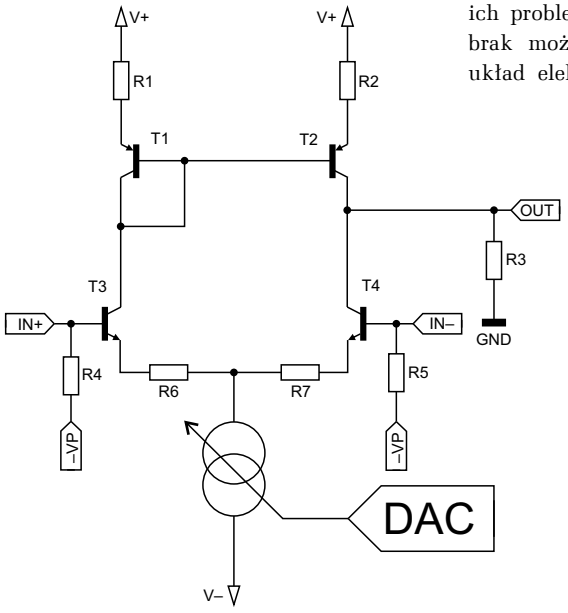


Płynna regulacja poziomu głośności

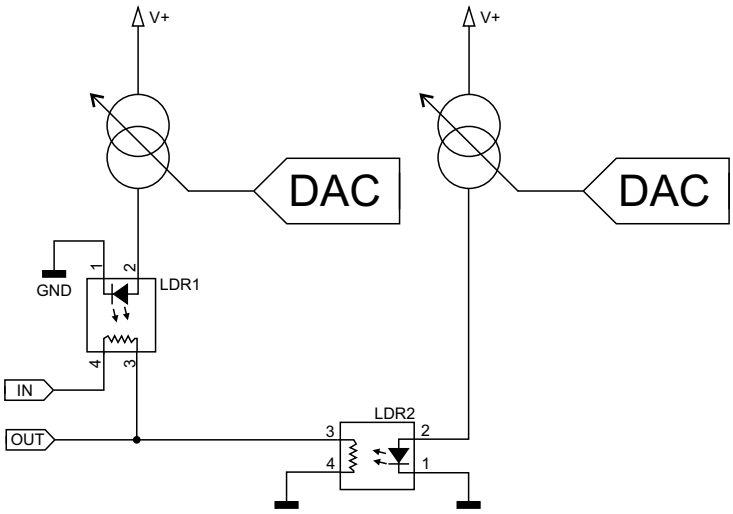
Ze skokową regulacją głośności spotykamy się dzisiaj na co dzień – w telewizorach, telefonach czy odtwarzaczach samochodowych. Niekiedy jednak kwantyzacja poziomów sygnału audio nam przeszkadza – na jednym kroku za cicho, na drugim za głośno, kroki zbyt słyszalne, słowem – stale coś jest nie tak. Niektórym bardziej pasuje stara „gałka" lub inny przyrząd, dający regulację płynną lub quasi-płynną. Co można na to zaradzić w XXI wieku?

Fotografia 1. Potencjometr z silnikiem z serii ALPS RK271 [1]

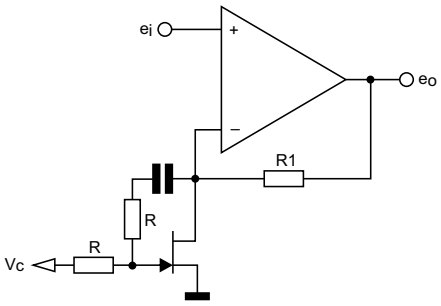
Niemal od początków radiotechniki rolę regulatora poziomu głośności odgrywał potencjometr – czasem tylko zastępowany przez transformator z wieloma odczepami, lecz ten zapewniał regulację skokową. Oczywiście zwykłe potencjometry mechaniczne nadal są dostępne, lecz ich problemem (zresztą nie jedynym) jest brak możliwości sterowania nimi przez układ elektroniczny. Wyjątkiem pod tym



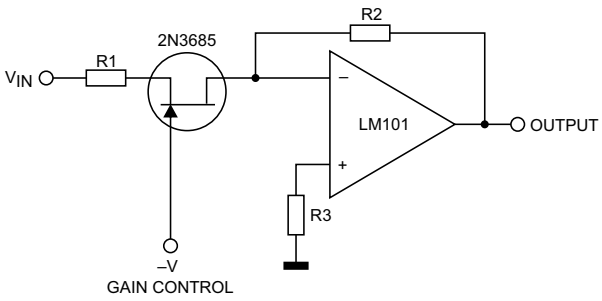
Rysunek 1. Uproszczony schemat regulatora wzmocnienia z układem różnicowym



Rysunek 2. Schemat regulatora głośności z fotorezystorami



Rysunek 3. Wzmacniacz nieodwracający sterowany napięciowo z tranzystorem JFET [2]



Rysunek 4. Wzmacniacz odwracający sterowany napięciowo [3]

względem, całkiem zresztą dobrze działającym, są potencjometry zintegrowane z silnikiem prądu stałego – jak na **fotografii 1**. Ten wynalazek był stosowany w sprzętach z lat osiemdziesiątych i dziewięćdziesiątych, umożliwiając użytkownikowi zarówno zdalną, jak i manualną regulację poziomu głośności. Z uwagi na użycie silnika prądu stałego, możliwe jest ustawienie osi potencjometru w dowolnym położeniu poprzez sterowanie silnikiem za pomocą impulsów o odpowiedniej długości.

Obracające się samoczynnie pokrętło z pewnością robi wrażenie, lecz takie rozwiązanie jest okupione zarówno sporą masą i gabarytami, jak również skończoną trwałością – przede wszystkim samego potencjometru, który przecież jest elementem elektromechanicznym. Warto zatem pójść w stronę rozwiązań czysto elektronicznych, które są tych wad pozbawione. Wprawdzie przy sterowaniu za pomocą urządzeń cyfrowych tytułowa płynność regulacji może nie być idealnie odwzorowana, lecz myślę, że zaproponowane pomysły są w stanie dobrze naśladować ją w wystarczającym stopniu.

Pierwszy pomysł, jaki przychodzi mi do głowy, to regulacja prądu źródła prądowego, które zasila emitery tranzystorów pary różnicowej – szczegóły widać na **rysunku 1**. Ten układ może służyć zarówno do wzmacniania, jak i tłumienia sygnału. Im większy jest prąd źródła prądowego, tym większe wzmocnienie osiąga ten układ i odwrotnie. Przeszkodą są jednak parametry tranzystorów, bowiem zmiana wzmocnienia o 20 dB wymaga dziesięciokrotnej zmiany prądu emiterów (np. w zakresie 1…10 mA), zaś o 40 dB już stukrotnej (chociażby 1…100 mA). Przy niskim prądzie kolektora parametry częstotliwościowe tranzystorów są niezbyt zachwycające, z kolei przy wysokim możemy mieć problem zarówno z chłodzeniem, jak i ze zwiększonym poziomem szumów. Choć można coś dobrać, a samą regulację podzielić na przykład na zakresy. Robiłem próby z tego typu regulacją i efekty były więcej niż zadowalające. Sam sygnał sterujący, w implementacji zaproponowanej na tym schemacie, pochodzi z przetwornika cyfrowo-analogowego, który steruje źródłem prądowym. Daje on skwantowane wartości napięcia na swoim wyjściu, lecz używając konwertera o rozdzielczości 16 lub 24 bitów, można uzyskać regulację niemal pozbawioną słyszalnych kroków. Zwłaszcza, że napięcie sterujące źródłem prądowym można odfiltrować członem RC, co dodatkowo zwiększy płynność przejść między kolejnymi wartościami napięcia.

Druga idea, również przeze mnie przetestowana, polega na zmianie rezystancji fotorezystora w optoizolatorze. Schemat przykładowego rozwiązania znajduje się na **rysunku 2**. Układ ten jest opcją „na bogato”, w której mamy zmienną zarówno rezystancję „górną” naszego „potencjometru” (optoizolator LDR1), jak i „dolną” przy wykorzystaniu optoizolatora LDR2. Budując taki układ trzeba jednak konieczne przewidzieć możliwość jego automatycznej kalibracji, gdyż fotorezystory mają znaczne rozrzuty parametrów. Dodatkową zaletą jest całkowita izolacja galwaniczna między sygnałem analogowym a sterującym. W prototypie, który badałem kilka lat temu, nie było fotorezystora LDR1 (został zastąpiony stałym rezystorem), a dynamika regulacji i tak sięgała 65 dB. Warto jednak ten układ utrzymywać w stałej temperaturze, gdyż przy wysokich wartościach rezystancji wpływ temperatury na parametry fotorezystora jest znaczący. Dodatkowo, z uwagi na szumy, lepiej byłoby go chłodzić niż grzać. Jest to propozycja bardziej dla audiofili, niż dla zwykłego zjadacza chleba, choć z pozornie dziwnych pomysłów czasem wykluwają się kolejne.

Na koniec moja ostatnia propozycja, którą raz zastosowałem w projekcie AVT1729 – czyli zmiana wzmocnienia wykorzystująca tranzystor JFET. W zakresie niskich napięć dren-źródło, ten tranzystor zachowuje się jak zmienna rezystancja, co doskonale sprawdza się w gałęzi ujemnego sprzężenia zwrotnego. **Rysunek 3** zawiera schemat wzmacniacza nieodwracającego, który – z racji swojej topologii – ma wzmocnienie nie mniejsze niż 1 V/V. Rolą szeregowego obwodu RC, znajdującego się między drenem a bramką, jest wprowadzenie ujemnego sprzężenia zwrotnego, które poprawia liniowość i zmniejsza przez to zniekształcenia. Taki układ może mieć dynamikę nawet 60 dB, lecz jego rolą jest wyłącznie zwiększanie amplitudy sygnału wejściowego. Takie umiejscowienie tranzystora JFET jest jedynym możliwym z uwagi na konieczność pracy z niskim napięciem dren-źródło, co zapewnia punkt „wirtualnej masy” między wejściami wzmacniacza operacyjnego – sygnał wejściowy może mieć amplitudę nie większą niż kilka miliwoltów, co można uznać niemal za potencjał masy.

W odmienny sposób działa układ z **rysunku 4** – wprawdzie odwraca fazę sygnału, lecz umożliwia również jego tłumienie, a nie tylko wzmacnianie. Prawe wyprowadzenie tranzystora JFET ma potencjał 0 V, co gwarantuje poprawne działanie wzmacniacza operacyjnego objętego pętlą ujemnego sprzężenia zwrotnego, natomiast lewe wyprowadzenie należy po prostu spolaryzować rezystorem do masy. I tutaj możliwe jest uzyskanie kilkudziesięciodecybelowej dynamiki, zwłaszcza w zakresie bardzo wysokich tłumień (praca tranzystora bliska zatkania), lecz trzeba pamiętać o tym, by amplituda sygnału wejściowego nie była zbyt wysoka, rzędu kilkudziesięciu miliowoltów. W przeciwnym razie grozi to wyjściem tranzystora JFET z „omowego” zakresu pracy.

Michał Kurzela, EP

Źródła:

[1] https://www.ebay.com/itm/122943325712
[2] https://www.onsemi.cn/pub/collateral/an-6603cn.pdf
[3] https://www.ti.com/lit/an/snoa620/snoa620.pdf

Elektronika w systemach płatniczych

Współczesny świat płatności elektronicznych opiera się na złożonym ekosystemie sprzętu, oprogramowania i standardów komunikacyjnych, który pozwala na szybkie i bezpieczne przetwarzanie transakcji. Od kart chipowych po terminale POS, smartfony, biżuterię i zegarki – każdy element infrastruktury jest miniaturowym systemem embedded, w którym wyspecjalizowane układy scalone oraz interfejsy komunikacyjne współpracują w celu zapewnienia niezawodności, bezpieczeństwa i wygody użytkownika.

Elektronika w systemach płatniczych obejmuje zarówno warstwę sprzętową, tj. frontend NFC, układy Secure Element czy mikrokontrolery, jak i oprogramowanie embedded, które realizuje logikę transakcji, generuje kryptogramy i zarządza pamięcią oraz komunikacją. Rola systemów wbudowanych w płatnościach nie ogranicza się jedynie do odczytu kart czy przesyłania danych. Każdy system musi obsłużyć wiele standardów płatniczych, zabezpieczyć klucze kryptograficzne, chronić przed manipulacjami fizycznymi i logicznymi oraz zapewnić kompatybilność z różnymi typami urządzeń końcowych. Jednocześnie oczekiwane przez użytkowników tempo transakcji wymaga realizacji wszystkich operacji w czasie nieprzekraczającym kilkuset milisekund, co stawia wysokie wymagania zarówno przed projektantami układów scalonych, jak i inżynierami embedded odpowiedzialnymi za firmware i aplikacje.

Artykuł ten ma na celu przybliżenie Czytelnikowi tematu elektroniki w systemach płatniczych, zarówno od strony kart i urządzeń mobilnych, jak i terminali POS, bankomatów oraz innych urządzeń wspierających płatności. Omówione zostaną także zagrożenia i ataki, które w ostatnich latach stały się istotnym wyzwaniem dla całego ekosystemu płatniczego [1].

Karty płatnicze i układy embedded

Stos protokołów NFC w kartach płatniczych

Technologia NFC jest rozszerzeniem komunikacji wysokiej częstotliwości (HF RFID) pracującej w paśmie 13,56 MHz. Standardy rządzące tą komunikacją tworzą wielowarstwowy stos protokołów, którego poszczególne warstwy odpowiadają konkretnym normom i specyfikacjom. Zrozumienie tego stosu jest zatem kluczowe zarówno dla projektowania kart płatniczych, jak i terminali obsługujących płatności zbliżeniowe.

Fundamentem całego ekosystemu NFC stosowanego w płatnościach kartowych jest standard ISO/IEC 14443, definiujący parametry komunikacji z kartami zbliżeniowymi. Składa się on z czterech części:

- ISO/IEC 14443-1 – fizyczne właściwości kart: wymiary, odporność mechaniczna i środowiskowa,
- ISO/IEC 14443-2 – interfejs radiowy i sygnałowy: modulacja, kodowanie bitów oraz prędkości transmisji,
- ISO/IEC 14443-3 – inicjalizacja komunikacji i procedury antykolizyjne, pozwalające na jednoznaczną identyfikację i adresowanie karty w polu czytnika,
- ISO/IEC 14443-4 – protokół transmisji danych (T=CL, czyli contactless), zapewniający niezawodną, blokową wymianę danych na poziomie sesji, analogicznie do warstwy transportowej w modelu OSI. [2]

Oprócz ISO/IEC 14443 w ekosystemie NFC funkcjonuje także norma ISO/IEC 18092 (znana też jako NFCIP-1). Jest to fundamentalny standard NFC opisujący komunikację peer-to-peer między dwoma pełnoprawnymi urządzeniami NFC, obsługujący tryby: aktywny i pasywny. Norma ISO/IEC 21481 (NFCIP-2) doprecyzowuje zasady współpracy urządzeń obsługujących jednocześnie ISO 18092 i ISO 14443, co jest istotne w kontekście smartfonów pełniących rolę zarówno czytnika, jak i karty, zależnie od scenariusza użytkowania w danym momencie. [7]

Ponad tymi normami funkcjonują specyfikacje NFC Forum – organizacji zrzeszającej producentów układów i urządzeń, która definiuje

interoperacyjność praktycznych implementacji. NFC Forum publikuje specyfikację cyfrową (*Digital Protocol Specification*) opisującą, jak korzystać ze standardów ISO 14443 i ISO 18092 w produktach. Definiuje ona pięć typów tagów NFC różniących się pojemnością pamięci, prędkością transmisji i obsługiwanymi protokołami:

- Tag Type 1 – oparty na ISO/IEC 14443 Type A, pojemność typowo 96 bajtów (teoretycznie z opcją rozszerzenia do 2 kB),
- Tag Type 2 – oparty na ISO/IEC 14443-3A, bardzo popularny w prostych aplikacjach,
- Tag Type 3 – oparty na japońskim standardzie JIS X 6319-4 (FeliCa), stosowany m.in. w kartach transportowych,
- Tag Type 4 – oparty na ISO/IEC 14443-4 (zarówno typ A, jak i B), obsługujący złożone protokoły APDU; ten typ realizują karty płatnicze EMV,
- Tag Type 5 – oparty na ISO/IEC 15693, przeznaczony do odczytu na większych odległościach. [7]

Na poziomie wymiany danych NFC Forum zdefiniowało format NDEF (*NFC Data Exchange Format*) – lekki format binarny przeznaczony do pakowania różnych typów danych, od adresów URL, aż po rozbudowane struktury binarne. Rekord NDEF zawiera pole nagłówka z typem danych (TNF – *Type Name Format*), długością ładunku (tzw. *payload*) i opcjonalnym identyfikatorem. W komunikacji peer-to-peer nad protokołem NDEF pracuje LLCP (*Logical Link Control Protocol*), który zapewnia niezawodne, dwukierunkowe przesyłanie danych, analogicznie do warstwy łącza danych w modelu OSI.

W płatnościach kartowych kluczową rolę odgrywa warstwa aplikacyjna, czyli standard EMV. Komendy APDU (*Application Protocol Data Unit*), zgodne z normą ISO/IEC 7816-4, są bezpośrednio przesyłane przez kanał NFC (ISO 14443-4) między kartą a terminalem. Na tym poziomie realizowany jest dialog, w którym terminal wybiera aplikację płatniczą (AID – *Application Identifier*), odczytuje dane karty i generuje żądanie autoryzacji. Struktura stosu wygląda zatem następująco: warstwa fizyczna (ISO 14443-1 i 14443-2) dostarcza bity do warstwy inicjalizacji i antykolizji (ISO 14443-3), ta z kolei do warstwy protokołu transmisji (ISO 14443-4), a nad nią pracuje warstwa aplikacji EMV operująca komendami APDU. [2] [7]

Rysunek 1 ilustruje pełny ekosystem standardów rządzących komunikacją w systemach płatności zbliżeniowych. Komunikacja między urządzeniem użytkownika a terminalem sprzedawcy opiera się na standardach ISO/IEC 14443 i ISO/IEC 7816-4, nadzorowanych przez EMVCo i PCI. Zarządzanie Secure Element po stronie urządzenia mobilnego realizowane jest przez protokoły NCI, SWP+HCI i GlobalPlatform, natomiast komunikacja z menadżerem usług zaufanych (TSM) oraz infrastrukturą bankową odbywa się przez GlobalPlatform i standardy EMVCo.

Komunikacja NFC – tryby pracy i parametry

Komunikacja NFC opiera się na sprzężeniu indukcyjnym, w którym anteny obu urządzeń tworzą wspólne pole magnetyczne o częstotliwości 13,56 MHz. Zasięg transmisji w standardowym zastosowaniu wynosi zwykle około 4 cm, choć w kontrolowanych warunkach laboratoryjnych możliwe jest osiągnięcie zasięgu rzędu kilkudziesięciu centymetrów, co, jak zostanie omówione w dalszej części artykułu, stanowi podstawę niektórych ataków. Prędkości przesyłu danych sięgają wartości od 106 kb/s do nawet 848 kb/s, w zależności od trybu i konfiguracji.

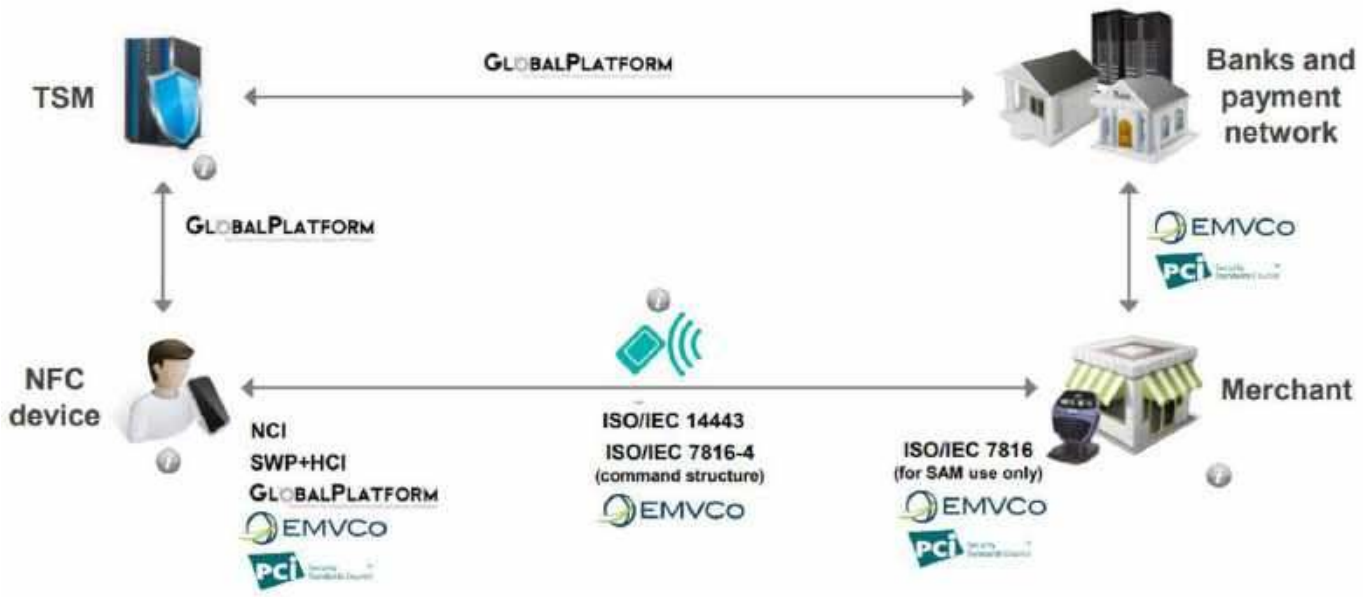
W praktyce NFC wykorzystuje trzy tryby pracy:

- **Reader/Writer** – urządzenie inicjuje komunikację i odczytuje dane z tagów lub kart; terminal płatniczy zawsze pracuje w tym trybie,
- **Peer-to-Peer (P2P)** – umożliwia dwukierunkową wymianę danych pomiędzy dwoma urządzeniami NFC, np. transfer pliku lub danych między smartfonami,
- **Card Emulation** – urządzenie (np. smartfon lub zegarek) zachowuje się jak karta zbliżeniowa, pozwalając na wykonywanie płatności lub autoryzację dostępu.

W warstwie protokołów NFC uwzględnione są mechanizmy antykolizyjne, które umożliwiają bezkonfliktową komunikację, gdy w polu czytnika znajduje się więcej niż jedna karta. Każda karta posiada unikalny identyfikator (UID lub NFCID), dzięki któremu terminal może adresować wybraną kartę. Mechanizmy antykolizji są szczególnie istotne w środowiskach o dużym zagęszczeniu kart – przykładem z życia wziętym może być portfel z wieloma kartami zbliżeniowymi [2] [7].

Układy scalone w kartach

Na rynku dostępne są specjalizowane układy scalone przeznaczone do kart płatniczych, dostarczane przez takie firmy jak STMicroelectronics, Infineon czy NXP. Układy Infineon z rodziny SLE78 i SLE97 integrują funkcje kryptograficzne z obsługą kart chipowych i zbliżeniowych. Mikrokontroler odpowiada za obsługę protokołów płatniczych, w tym EMV i standard ISO/IEC 14443. EEPROM przechowuje dane użytkownika i klucze kryptograficzne, pamięć Flash lub ROM zawiera firmware karty, a RAM służy do buforowania danych i wykonywania obliczeń kryptograficznych w czasie transakcji.



Rysunek 1. Ekosystem standardów NFC/EMV [22]

Secure Element izoluje klucze i mechanizmy kryptograficzne, znacznie utrudniając ich odczyt nawet po uzyskaniu fizycznego dostępu do karty. Układy te implementują akceleratory sprzętowe algorytmów DES, 3DES, AES i RSA, co pozwala na realizację operacji kryptograficznych w czasie nieprzekraczającym kilku milisekund. Całość jest zintegrowana w małym chipie, który czerpie energię z pola elektromagnetycznego terminala (w przypadku kart zbliżeniowych), pobierając typowo do kilku miliwatów mocy [3].

Firmware i aplety płatnicze

Sprzęt w kartach płatniczych realizuje jedynie podstawowe funkcje obliczeniowe i komunikacyjne, a logika płatności oraz zarządzanie bezpieczeństwem leżą po stronie firmware i apletów. Najczęściej stosowanymi systemami operacyjnymi są Java Card i MULTOS. Java Card pozwala na uruchamianie apletów w izolowanym środowisku, umożliwiając weryfikację transakcji EMV, generowanie kryptogramów i zarządzanie pamięcią w sposób deterministyczny. MULTOS oferuje podobne możliwości, z dodatkowymi mechanizmami zarządzania kluczami i obsługi certyfikatów.

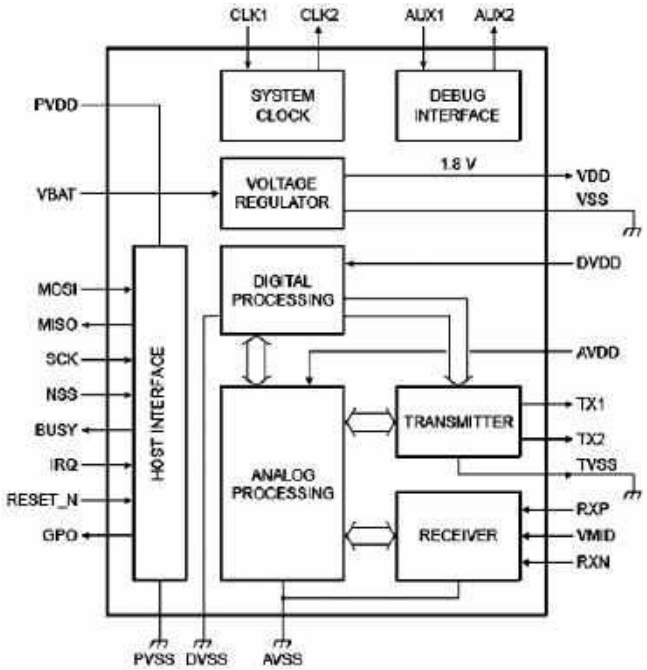
Aplety płatnicze realizują logikę transakcji: generowanie i weryfikację kryptogramów (ARQC – *Authorization Request Cryptogram*, ARPC – *Authorization Response Cryptogram*), obsługę transakcji offline i online oraz tokenizację danych w systemach mobilnych. Niepozorna karta płatnicza jest więc w istocie kompletnym, miniaturowym systemem embedded, w którym MCU przetwarza dane, Secure Element chroni klucze, a aplet odpowiada za logikę transakcji [4] [5].

Terminale płatnicze NFC

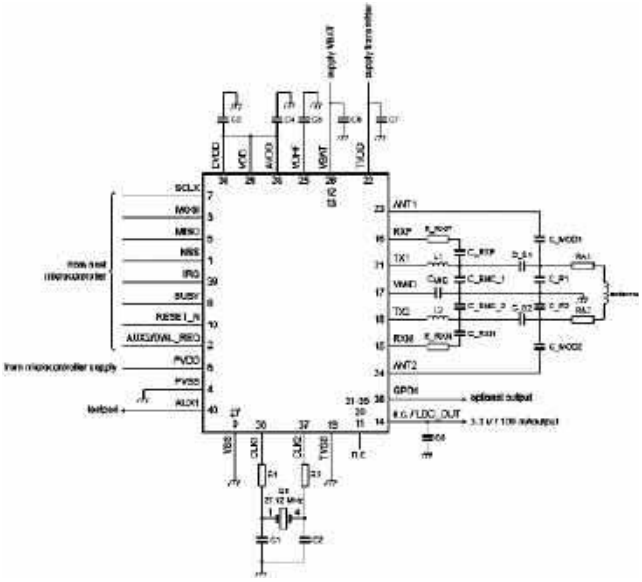
Terminal płatniczy obsługujący płatności zbliżeniowe stanowi złożony system elektroniczny integrujący kilka wyspecjalizowanych bloków funkcjonalnych. Jego podstawowym zadaniem jest komunikacja radiowa z kartą lub urządzeniem mobilnym użytkownika, realizowana zgodnie ze standardami NFC, a także przekazanie danych transakcyjnych do systemu autoryzacyjnego operatora płatności.

Frontend NFC

Kluczowym elementem toru komunikacyjnego terminala płatniczego jest układ frontendu NFC odpowiedzialny za fizyczną warstwę komunikacji radiowej. Układ ten generuje pole elektromagnetyczne



Rysunek 2. Schemat blokowy układu PN5180 [6]



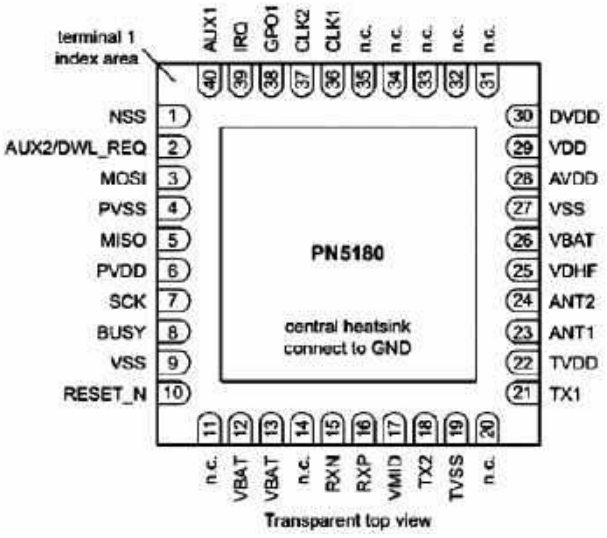
Rysunek 3. Schemat aplikacyjny układu PN5180 [6]

o częstotliwości 13,56 MHz oraz realizuje modulację sygnału nadawczego oraz demodulację sygnałów odbieranych z karty lub urządzenia mobilnego. Przykładem takiego układu jest NXP PN5180 (**rysunki 2...4**) – wysokowydajny frontend NFC obsługujący standardy ISO/IEC 14443 A/B, ISO/IEC 15693 i NFC Forum, z maksymalną mocą nadajnika RF do około 1,5 W i interfejsem SPI o przepustowości do 7 Mbit/s. Układ zawiera wbudowane mechanizmy dynamicznego dopasowania anteny (Dynamic Power Control), które automatycznie dostosowują moc nadajnika do aktualnych warunków odczytu [6].

Podstawowe parametry elektryczne układu zestawiono w **tabeli 1**. Układ zasilany jest napięciem w zakresie 2,7...5,5 V, co pozwala na współpracę zarówno z systemami 3,3 V, jak i 5 V. Nadajnik RF pobiera do 250 mA z szyny TVDD, co przekłada się na moc wyjściową wystarczającą do osiągnięcia zgodności z wymaganiami EMVCo na poziomie RF. W trybie czuwania pobór prądu spada do zaledwie 15 µA, co z kolei czyni układ odpowiednim również do aplikacji bateryjnych.

Antena NFC

Integralną częścią systemu komunikacji NFC jest antena odpowiedzialna za wytworzenie pola elektromagnetycznego oraz sprzężenie indukcyjne z anteną karty lub urządzenia mobilnego.



Rysunek 4. Układ wyprowadzeń układu NXP PN5180 w obudowie HVQFN40 [6]

Tabela 1. Podstawowe parametry elektryczne układu NXP PN5180 [6]

Symbol	Parametr	Min.	Typ.	Maks.	Jedn.
$V_{DD(VBAT)}$	Napięcie zasilania – pin VBAT	2,7	3,3	5,5	V
$V_{DD(PVDD)}$	Napięcie zasilania – pin PVDD	1,65	1,8	1,95	V
		2,7	3,3	3,6	V
$V_{DD(TVDD)}$	Napięcie zasilania – pin TVDD	2,7	5,0	5,5	V
I_{pd}	Prąd w trybie power-down	–	10	–	µA
I_{stb}	Prąd w trybie standby	–	15	–	µA
$I_{DD(TVDD)}$	Prąd zasilania – pin TVDD	–	180	250	mA
		–	–	300	mA
T_{amb}	Temperatura otoczenia	–30	+25	+85	°C
T_{stg}	Temperatura przechowywania	–55	+25	+150	°C

W terminalach płatniczych stosuje się najczęściej anteny w postaci wielozwojowych cewek wykonanych w technologii planarnej (ścieżki na PCB lub na elastycznych laminatach). Projekt anteny ma bezpośredni wpływ na zasięg komunikacji, stabilność transmisji oraz odporność systemu na zakłócenia elektromagnetyczne. Konieczne jest dopasowanie impedancji anteny do układu frontendu NFC za pomocą obwodu rezonansowego z precyzyjnie dobranymi kondensatorami dopasowującymi [7].

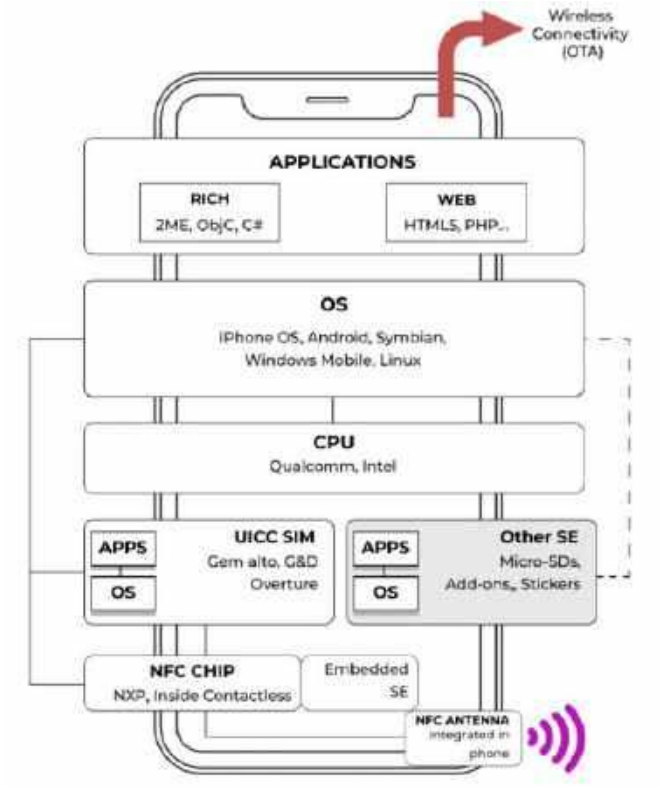
Płatności mobilne i tokenizacja

Współczesne płatności mobilne funkcjonują na zasadzie analogicznej do kart zbliżeniowych, wprowadzając dodatkową warstwę oprogramowania i bezpieczeństwa. Smartfony, zegarki i inne urządzenia mobilne korzystają z wbudowanego układu typu *Secure Element* (SE), *Trusted Execution Environment* (TEE) oraz *Host Card Emulation* (HCE), aby przechowywać i przetwarzać wrażliwe dane.

Secure Element w telefonach to izolowany układ scalony lub obszar mikrokontrolera, w którym przechowywane są klucze kryptograficzne, certyfikaty płatnicze oraz tokeny. Może przyjmować formę wbudowanego SE na płycie głównej, modułu SIM lub karty MicroSD pełniącej funkcję SE. *Host Card Emulation* (HCE) pozwala natomiast na emulację karty płatniczej bez konieczności instalacji fizycznego SE. Dane wrażliwe przechowywane są w chmurze lub systemie tokenizacji, a urządzenie generuje dynamiczne tokeny w momencie płatności. Takie rozwiązanie umożliwia elastyczną integrację z aplikacjami typu wallet i redukuje koszty sprzętowe.

Tokenizacja stanowi kluczowy element bezpieczeństwa w płatnościach mobilnych. Numery kart (PAN – *Primary Account Number*) zastępowane są tokenami, które nie zawierają danych wrażliwych i są powiązane z dynamicznie generowanym kryptogramem, zapewniając autentyczność każdej transakcji. Tokeny mogą mieć charakter jednorazowy lub być przypisane do konkretnego urządzenia, co dodatkowo ogranicza ryzyko nadużyć. Z perspektywy oprogramowania wbudowanego procesory w telefonach lub TEE zajmują się generowaniem kryptogramów i weryfikacją tokenów, Secure Element zapewnia izolację kluczy, a HCE umożliwia elastyczne zarządzanie tokenami w warstwie software [8] [9].

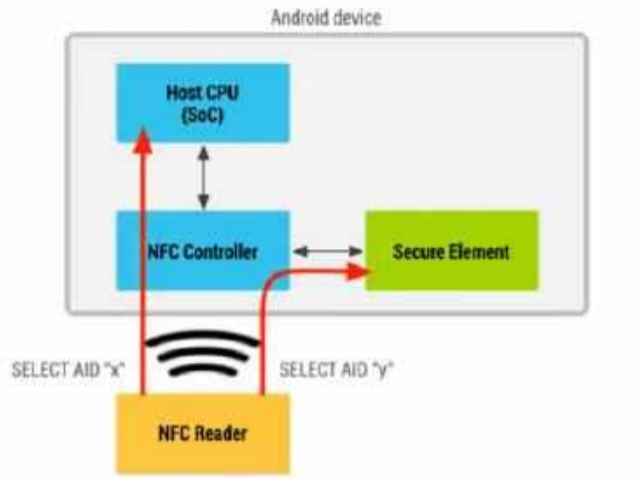
Rysunek 6 ilustruje mechanizm routingu komend NFC w urządzeniu z systemem Android. NFC Controller pełni rolę przełącznika – na podstawie identyfikatora aplikacji płatniczej (AID), zawartego w komendzie SELECT, kieruje komunikację albo do fizycznego Secure Element, albo bezpośrednio do procesora głównego (Host CPU/SoC), gdzie obsługuje ją serwis HCE. Dzięki temu jedno urządzenie może obsługiwać zarówno aplikacje wymagające sprzętowej izolacji kluczy, jak i aplikacje oparte na tokenizacji chmurowej.



Rysunek 5. Architektura urządzenia mobilnego z NFC [24]

Komunikacja i protokoły w systemach embedded

W systemach płatniczych komunikacja między kartą, terminalem i systemami bankowymi stanowi fundamentalny element realizacji transakcji. W przypadku kart zbliżeniowych oraz urządzeń mobilnych wymiana danych z terminalem odbywa się zgodnie ze standardem ISO/IEC 14443, który definiuje komunikację NFC



Rysunek 6. Architektura routingu NFC w systemie Android [8]

typu A i B. Frontend NFC w terminalu odbiera i demoduluje sygnał z karty lub telefonu, a następnie przekazuje dane do mikrokontrolera poprzez interfejs SPI lub I²C. Mikrokontroler przetwarza je zgodnie z logiką transakcji określoną w specyfikacjach EMV i generuje odpowiedź przesyłaną z powrotem do urządzenia użytkownika.

Cały dialog transakcyjny między kartą a terminalem realizowany jest za pomocą komend APDU (*Application Protocol Data Unit*), zgodnych z normą ISO/IEC 7816-4. Komenda APDU ma strukturę złożoną z nagłówka (CLA, INS, P1, P2) oraz opcjonalnego pola danych i oczekiwanej długości odpowiedzi. Terminal inicjuje sesję komendą SELECT, wybierając aplikację płatniczą po jej identyfikatorze AID (*Application Identifier*). Następnie wymieniane są kolejne komendy: GET PROCESSING OPTIONS inicjuje transakcję i pobiera listę plików do odczytu (AFL – *Application File Locator*), READ RECORD odczytuje dane aplikacji, a GENERATE AC (*Application Cryptogram*) jest finalną komendą, w odpowiedzi na którą karta generuje kryptogram ARQC (*Authorization Request Cryptogram*), unikalny dla danej transakcji kod uwierzytelniający, obejmujący kwotę, walutę, datę, losową liczbę terminala i inne parametry [10].

Po stronie backendu komunikacja terminala z systemami bankowymi odbywa się za pośrednictwem szyfrowanych kanałów, najczęściej z wykorzystaniem protokołu TLS (*Transport Layer Security*) czy też połączeń VPN. Do przesyłania informacji o transakcjach stosowane są standardy komunikacyjne ISO 8583 oraz nowszy ISO 20022. ISO 8583 definiuje strukturę wiadomości używanych w transakcjach kartowych, jest to format binarny złożony z pól bitmapy i elementów danych o zmiennej długości, umożliwiający przesyłanie danych o kwocie transakcji, typie karty, identyfikatorze terminala oraz kryptogramach do systemu autoryzacyjnego banku. ISO 20022 to nowszy, oparty na XML i JSON standard komunikacji finansowej, stopniowo zastępujący ISO 8583 w infrastrukturze rozliczeniowej [10] [11].

Architektura komunikacji w systemach płatniczych obejmuje również mechanizmy bezpieczeństwa na poziomie sieci. Terminale płatnicze muszą być certyfikowane zgodnie ze standardami PCI DSS (*Payment Card Industry Data Security Standard*) i PCI PTS (*PIN Transaction Security*), które określają wymagania dotyczące szyfrowania klucza PIN (za pomocą algorytmu Triple DES lub AES), zarządzania kluczami szyfrującymi (PKI, HSM – *Hardware Security Module*) oraz fizycznej odporności urządzeń na manipulacje. Klucze szyfrujące PIN przechowywane są w dedykowanych, odpornych na manipulacje modułach HSM, których obudowy wyposażone są w czujniki fizyczne. Próba otwarcia obudowy powoduje natychmiastowe skasowanie kluczy z pamięci ulotnej [10] [11].

Inne urządzenia płatnicze

Bankomaty

Bankomat stanowi złożony system, który łączy elementy obliczeniowe, interfejsy użytkownika oraz układy mechaniczne odpowiedzialne za obsługę gotówki. Z punktu widzenia architektury urządzenia bankomat można traktować jako komputer przemysłowy wyposażony w specjalne moduły sprzętowe i połączony z systemami bankowymi za pośrednictwem sieci komunikacyjnej.

Głównym elementem sterującym jest płyta zawierająca procesor, pamięć oraz kontrolery komunikacji z pozostałymi komponentami. Do podstawowych elementów bankomatu należą także: czytniki kart (stykowy i zbliżeniowy), szyfrująca klawiatura PIN (EPP – *Encrypting PIN Pad*), ekran LCD z panelem dotykowym lub przyciskami mechanicznymi, kasety z banknotami, mechanizm wydawania i weryfikacji gotówki oraz drukarka paragonów. Czytnik kart odczytuje dane zapisane na pasku magnetycznym lub w układzie chipowym zgodnym ze standardem EMV, który generuje unikalny kryptogram dla każdej transakcji.

Szyfrująca klawiatura PIN (EPP) stanowi jeden z najważniejszych elementów bezpieczeństwa bankomatu z perspektywy systemu embedded. Jest to autonomiczny moduł zawierający własny mikrokontroler, pamięć i układ kryptograficzny, który szyfruje wprowadzony PIN bezpośrednio w momencie naciśnięcia klawisza, zanim dane trafią do głównego komputera bankomatu. Klucze szyfrujące są wstrzykiwane do EPP przez bank podczas procesu inicjalizacji urządzenia i nie mogą być odczytane z zewnątrz. Obudowa EPP wyposażona jest w czujniki antytamper: czujnik otwarcia, czujnik temperatury, czujnik napięcia zasilania i siatkę przewodów wykrywającą wiercenie. Każda próba fizycznego dostępu do wnętrza modułu skutkuje natychmiastowym skasowaniem kluczy.

Mechanizm dystrybucji banknotów pobiera je z odpowiednich kaset i transportuje do podajnika. System detekcji kontroluje grubość i rozmiary banknotów za pomocą czujników optycznych i mechanicznych, aby upewnić się, że wydawany jest pojedynczy, autentyczny banknot. W przypadku wykrycia nieprawidłowości banknot kierowany jest do pojemnika odrzutu, a system wybiera kolejny egzemplarz. Dane transakcyjne są przetwarzane przez główny kontroler bankomatu, a następnie przesyłane do procesora transakcyjnego za pośrednictwem interfejsu komunikacyjnego. System ten przekazuje żądanie do odpowiedniej sieci płatniczej, która kieruje je do banku wydającego kartę w celu autoryzacji operacji [12].

Zagrożenia i ataki na elektroniczne systemy płatnicze

Powszechność systemów płatniczych opartych na elektronice czyni je atrakcyjnym celem dla przestępców. Ataki na te systemy można podzielić na dwie główne kategorie: fizyczne, polegające na manipulacji sprzętem oraz logiczne, wykorzystujące słabości protokołów i oprogramowania. Poniżej omówiono najważniejsze z nich, ze szczególnym uwzględnieniem aspektów technicznych istotnych z perspektywy inżyniera systemów wbudowanych.

Nakładki na klawiatury i czytniki kart (skimming)

Skimming to metoda polegająca na instalacji fałszywych urządzeń w pobliżu lub bezpośrednio na prawdziwym terminalu lub

bankomacie, w celu przechwycenia danych karty i numeru PIN. Z perspektywy embedded ataki te są przykładem wyrafinowanej inżynierii sprzętowej i miniaturyzacji elektroniki.

Skimmer na czytnik kart (ang. *card skimmer*) to cienkie urządzenie montowane nad właściwym czytnikiem bankomatu lub terminala POS. Odczytuje ono dane z paska magnetycznego karty podczas jej wsuwania. Dane są przechowywane w wewnętrznej pamięci Flash lub przesyłane bezprzewodowo, najczęściej przez moduł Bluetooth lub GSM. Skimmery nowej generacji wykonane są z tworzyw sztucznych drukowanych w technologii 3D i pomalowane na kolor obudowy bankomatu, co czyni je praktycznie niewidocznymi dla nieświadomego użytkownika. Równolegle z czytnikiem kart instalowana jest fałszywa nakładka na klawiaturę (ang. *PIN pad overlay*), cienka warstwa elektroniki montowana bezpośrednio na oryginalnej klawiaturze EPP, rejestrująca naciskane klawisze i zapamiętująca wprowadzone kody PIN. Alternatywnie przestępcy montują miniaturową kamerę skierowaną na klawiaturę. Bywa ona umieszczana w listwach ozdobnych bankomatu [15] [16].

Bardziej zaawansowaną odmianą skimmingu jest tzw. shimming, atakujący karty chipowe EMV. Shim to niezwykle cienki, elastyczny obwód drukowany o grubości zaledwie kilkudziesięciu mikrometrów, wsuwany między kartę a styk czytnika. Pasożytniczo pobiera zasilanie z czytnika i przechwytuje komunikację APDU między kartą a terminalem. Choć dane karty chipowej są trudniejsze do sklonowania niż dane z paska magnetycznego, shim może przechwycić wrażliwe informacje wystarczające do przeprowadzenia transakcji w trybie paska magnetycznego (*mag-stripe fallback*) lub ataków na protokół. Organy regulacyjne i sieci płatnicze stopniowo ograniczają możliwość fallbacku do paska magnetycznego, aby zniwelować ten wektor ataku [15] [16].

Ataki na protokół EMV – relay i pre-play

Ataki na warstwę protokołową systemów EMV są bardziej wyrafinowane i wymagają dogłębnej znajomości specyfikacji płatniczych. Badacze zidentyfikowali kilka klas podatności, które – choć teoretycznie są znane od lat – wciąż stanowią realne zagrożenie w praktycznych implementacjach [13].

Atak *relay* (przekaźnikowy) polega na nielegalnym rozszerzeniu zasięgu komunikacji NFC między kartą ofiary a złośliwym terminalem. Atakujący potrzebuje dwóch urządzeń: tzw. *mole* (kreta), urządzenia działającego w pobliżu karty ofiary i emulującego terminal oraz tzw. *ghost* (ducha), urządzenia przy prawdziwym terminalu płatniczym emulującego kartę. Oba urządzenia komunikują się ze sobą przez Internet lub sieć mobilną, przekazując w czasie rzeczywistym komendy i odpowiedzi APDU. Z perspektywy terminala wygląda to jak normalna transakcja z kartą, podczas gdy prawdziwa karta może znajdować się nawet kilkadziesiąt kilometrów dalej. Atak ten jest możliwy, ponieważ standard NFC nie zawiera mechanizmu weryfikacji odległości między kartą a terminalem [13] [14].

Badania potwierdziły praktyczną wykonalność ataku relay przy użyciu powszechnie dostępnych smartfonów z systemem Android i dedykowanych aplikacji NFC. Czas opóźnienia wprowadzany przez łącze internetowe jest na tyle mały, że mieści się w limitach czasowych protokołu EMV. Skuteczną metodą obrony przed atakami relay jest wprowadzenie mechanizmów distance bounding, protokołów kryptograficznych mierzących czas przesyłu sygnału w celu weryfikacji fizycznej bliskości urządzeń. Ich wdrożenie w kartach płatniczych pozostaje jednak wyzwaniem sprzętowym i standaryzacyjnym [13].

Schemat ataku relay przedstawiono na **rysunku 7**. Lewy smartfon znajduje się w pobliżu karty ofiary i emuluje terminal NFC, przechwytując komendy APDU. Dane są przesyłane przez serwer pośredniczący do prawego smartfona, który przy prawdziwym czytniku NFC emuluje kartę płatniczą. Opcjonalny komputer pośredniczący umożliwia dodatkowo modyfikację przesyłanych danych w locie, realizując atak Man-in-the-Middle na poziomie protokołu APDU. Z perspektywy terminala transakcja wygląda całkowicie normalnie. Karta i terminal komunikują się zgodnie ze specyfikacją EMV, choć fizycznie dzieli je dowolna odległość.

Atak pre-play wykorzystuje słabość generatorów liczb losowych w terminalach. W protokole EMV terminal generuje losową liczbę (*Unpredictable Number* – UN), którą karta włącza do obliczenia kryptogramu ARQC. Jeśli generator UN w terminalu jest przewidywalny lub słaby, atakujący może z wyprzedzeniem nakłonić kartę do wygenerowania kryptogramów dla przyszłych wartości UN i użyć ich później do przeprowadzenia fałszywych transakcji. Badania wykazały, że niektóre terminale używają sekwencji liczb pseudolosowych opartych na czasie systemowym lub prostych licznikach, co czyni UN przewidywalnymi [13].

Atak określany mianem *contactless limit bypass* polega na manipulacji danymi transakcji w celu ominięcia limitu kwotowego dla transakcji zbliżeniowych bez weryfikacji PIN. Atakujący modyfikuje dane wymienianych komunikatów APDU, np. walutę transakcji lub flagi konfiguracyjne tak, aby terminal zakwalifikował transakcję powyżej limitu jako mieszczącą się w limicie, akceptując ją bez żądania PIN. Eksperymenty wykazały, że podatność ta dotyczyła zarówno kart Visa, jak i Mastercard, choć sieci płatnicze wydały aktualizacje specyfikacji częściowo adresujące ten problem [13].

Ataki typu Man-in-the-Middle i podsłuch NFC

Podsłuch (*eavesdropping*) komunikacji NFC jest możliwy dzięki temu, że sygnał radiowy 13,56 MHz nie jest kierunkowy i propaguje się dość swobodnie w przestrzeni. Atakujący wyposażony w odpowiednio czułą antenę może rejestrować transmisję NFC z odległości od kilkudziesięciu centymetrów do kilku metrów, w zależności od mocy terminala i charakterystyki środowiska elektromagnetycznego. Przechwycone dane mogą zawierać numer karty (PAN), datę ważności, imię i nazwisko posiadacza oraz inne dane aplikacji, w zależności od konfiguracji karty i sieci płatniczej [14].

Atak Man-in-the-Middle (MITM) w komunikacji NFC jest trudniejszy do wykonania niż pasywny podsłuch, ponieważ wymaga jednoczesnego aktywnego uczestnictwa w obu kierunkach komunikacji, bez ryzyka wykrycia przez żadną ze stron. W kontekście NFC realizowany jest zazwyczaj jako kombinacja ataku relay z modyfikacją przesyłanych danych. Skuteczność ochrony kryptograficznej w postaci dynamicznie generowanych kryptogramów ARQC sprawia, że przechwycone dane transakcji nie mogą być bezpośrednio odtworzone do kolejnej transakcji. Jednak dane statyczne karty (PAN, data ważności) mogą być użyte do transakcji typu *Card Not Present* (CNP), np. zakupów w Internecie, które nie wymagają dynamicznego kryptogramu [13] [14].

Rysunek 7. Nakładkowy skimmer na terminal POS z modułem Bluetooth [23]

Ataki side-channel na układy kryptograficzne

Ataki typu *side-channel* (kanałem bocznym) to klasa ataków, która zamiast łamania algorytmu kryptograficznego wprost, wykorzystuje fizyczne właściwości urządzenia ujawniające informacje o przetwarzanych danych. Są one szczególnie groźne dla układów embedded realizujących operacje kryptograficzne, w tym dla Secure Element w kartach płatniczych i terminalach [17].

Metody *Simple Power Analysis* (SPA) i *Differential Power Analysis* (DPA) polegają na pomiarze poboru prądu układu scalonego podczas obliczeń kryptograficznych. Ponieważ tranzystory CMOS pobierają prąd proporcjonalnie do przetwarzanych danych (w wyniku ładowania i rozładowywania pojemności pasożytniczych), analiza kształtu przebiegu poboru mocy może ujawnić przetwarzane dane, a w konsekwencji klucze kryptograficzne. DPA wykorzystuje statystyczną analizę wielu przebiegów, pozwalając na ekstrakcję kluczy nawet z zaszumionych pomiarów. Badania z użyciem standardowego oscyloskopu i niedrogich sond prądowych wykazały podatność wielu komercyjnych układów kryptograficznych na tego rodzaju „nasłuch" [17].

Metoda *Electromagnetic Analysis* (EMA) jest analogiczna do DPA, lecz zamiast poboru prądu mierzy promieniowanie elektromagnetyczne emitowane przez układ podczas obliczeń. Zaletą jest możliwość lokalizacji konkretnych obszarów układu (np. rejestrów przechowujących klucz) i selektywne podsłuchiwanie ich aktywności. Metoda ta jest szczególnie groźna, ponieważ nie wymaga fizycznego kontaktu z układem ani modyfikacji jego połączeń [17].

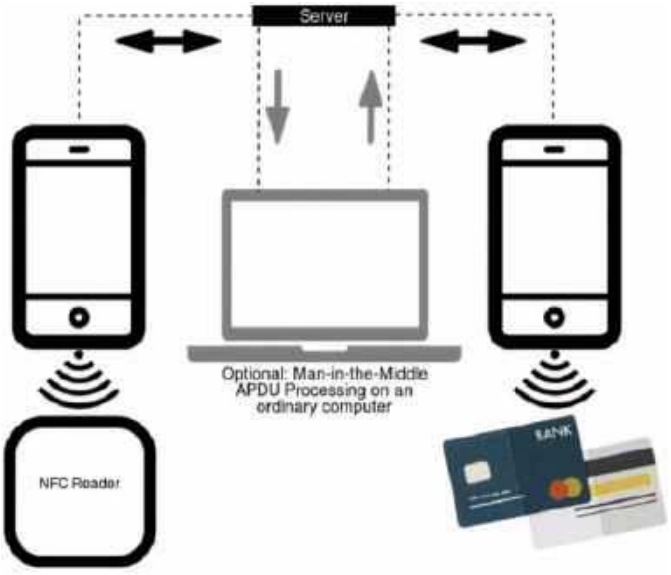
Ataki przez wstrzykiwanie błędów (*fault injection*) polegają na celowym zakłóceniu pracy układu w celu wywołania obliczeniowego błędu, który może ujawnić informacje o kluczu lub ominąć procedurę weryfikacji. Zakłócenia mogą być wprowadzane przez chwilowe zmiany napięcia zasilania (*voltage glitching*), krótkie impulsy elektromagnetyczne (*EM glitching*) lub naświetlenie układu laserem (*laser fault injection*). Producenci chipów kryptograficznych stosują szereg środków zaradczych: losowe maskowanie operacji kryptograficznych, powielanie obliczeń i weryfikację spójności wyników, czujniki anomalii napięcia i częstotliwości zegara oraz fizyczne ekranowanie układu metalową warstwą nad strukturą krzemową [17].

Malware NFC i ataki na aplikacje mobilne

Najnowszą i dynamicznie rozwijającą się kategorią zagrożeń są ataki z wykorzystaniem złośliwego oprogramowania na smartfonach, używające funkcji NFC do oszustw finansowych. W 2024 i 2025 roku badacze i firmy z branży cyberbezpieczeństwa odnotowali gwałtowny wzrost liczby takich incydentów [18] [19].

NGate to złośliwe oprogramowanie dla systemu Android, wykryte przez badaczy z firmy ESET, które umożliwia przekazywanie danych NFC z zainfekowanego urządzenia ofiary do urządzenia kontrolowanego przez przestępcę. Atak przebiega dwuetapowo: w pierwszym etapie ofiara jest nakłaniana (przez phishing, fałszywe SMS-y lub połączenia telefoniczne podszywające się pod bank) do zainstalowania fałszywej aplikacji bankowej zawierającej komponent NGate. W drugim etapie, gdy ofiara zbliży swoją kartę płatniczą do zainfekowanego smartfona, aplikacja przechwytuje dane NFC karty i w czasie rzeczywistym przekazuje je przestępcy. Przestępca używa osobnego urządzenia do emulacji karty ofiary i dokonuje wypłat z bankomatu. Firma ESET odnotowała w 2024 roku 35-krotny wzrost liczby ataków z wykorzystaniem technologii NFC w porównaniu z rokiem poprzednim [18].

SuperCard X to kolejna rodzina złośliwego oprogramowania NFC, zidentyfikowana w 2025 roku, działająca na zasadzie podobnej do NGate, lecz oferująca przestępcom bardziej zaawansowane możliwości operacyjne. SuperCard X jest dystrybuowany w modelu MaaS (*Malware-as-a-Service*), co oznacza, że twórcy udostępniają go innym przestępcom za opłatą abonamentową. Zawiera



Rysunek 8. Schemat ataku typu relay [21]

panel zarządzania kampaniami oraz gotowe szablony fałszywych aplikacji bankowych dla różnych krajów i instytucji. Ataki z wykorzystaniem SuperCard X zostały odnotowane w Polsce. CERT Polska wydał ostrzeżenie po wykryciu incydentów, w których ofiary traciły środki z kont bez świadomości, że ich karta fizycznie nigdy nie opuściła portfela [18] [19].

Z technicznego punktu widzenia zarówno NGate, jak i SuperCard X wykorzystują biblioteki Android NFC API dostępne dla aplikacji działających na nieodblokowanych urządzeniach, a do emulacji karty używają mechanizmu *Host Card Emulation* (HCE) – tego samego, który stosują legalne aplikacje mobilne. Ochrona przed tego rodzaju atakami leży zarówno po stronie systemu operacyjnego (ograniczenia uprawnień NFC, weryfikacja aplikacji), jak i po stronie banków (analiza behawioralna transakcji, weryfikacja geolokalizacji urządzenia podczas transakcji) [18] [19].

Trendy i kierunki rozwoju

Systemy płatnicze rozwijają się w kierunku większej integracji, elastyczności i bezpieczeństwa, przy jednoczesnym zmniejszeniu zależności od dedykowanego sprzętu. Jednym z najważniejszych trendów są terminale typu softPOS, aplikacje płatnicze działające na standardowych urządzeniach mobilnych, takich jak smartfony czy tablety z systemem Android.

SoftPOS umożliwia realizację płatności zbliżeniowych i kartowych bez konieczności posiadania dedykowanego terminala, wykorzystując front-end NFC oraz wbudowane mechanizmy bezpieczeństwa (*Trusted Execution Environment* i *Secure Element*) do generowania tokenów i kryptogramów. Standard *PCI Mobile Payments on COTS* (MPoC) określa wymagania bezpieczeństwa dla takich rozwiązań. MPoC buduje się na wcześniejszych normach SPoC (*Software-based PIN entry on COTS*) i CPoC (*Contactless Payments on COTS*) i obejmuje sytuacje, w których zarówno dane PIN, jak i dane kart zbliżeniowych są przetwarzane na tym samym urządzeniu ogólnego przeznaczenia (COTS – *Commercial Off-The-Shelf*). Standard MPoC zapewnia, że transakcje realizowane w aplikacjach softPOS spełniają wymagania bezpieczeństwa PCI, a klucze kryptograficzne i dane kart są chronione równorzędnie do tradycyjnych terminali [13] [14].

Kolejnym istotnym kierunkiem rozwoju jest integracja biometrii jako warstwy autoryzacji transakcji. Czytniki linii papilarnych, kamery do rozpoznawania twarzy (Face ID, skanery tęczówki) oraz sensory żył dłoni są coraz częściej stosowane zarówno w smartfonach realizujących płatności mobilne, jak i w dedykowanych

terminalach oraz bankomatach. Z perspektywy inżyniera oznacza to konieczność integracji dedykowanych układów przetwarzania biometrycznego z istniejącą architekturą Secure Element i TEE. Dane biometryczne muszą być przetwarzane i przechowywane wyłącznie w izolowanym środowisku, nigdy nie opuszczając chronionego obszaru procesora.

Rosnące znaczenie mają też płatności w ekosystemie IoT. Zegarki, opaski fitness, inteligentne samochody, lodówki czy systemy automatyki domowej stają się pełnoprawnymi urządzeniami płatniczymi. Z perspektywy projektantów oznacza to często konieczność miniaturyzacji frontendu NFC, układów kryptograficznych i Secure Element do rozmiarów i poboru mocy akceptowalnych dla urządzeń ubieralnych zasilanych małymi akumulatorami. Integracja frontendu NFC, MCU i Secure Element w jednym chipie (tzw. SoC – *System on Chip*) upraszcza projektowanie, zwiększa niezawodność i skraca czas wdrożenia nowych produktów [13] [14].

Istotnym trendem jest także stopniowe upowszechnianie się płatności biometrycznych na karcie (*on-card biometrics*). Karty płatnicze wyposażone we wbudowany czytnik linii papilarnych umożliwiają autoryzację transakcji zbliżeniowych bez konieczności wprowadzania numeru PIN, nawet powyżej standardowego limitu zbliżeniowego. Czytnik linii papilarnych jest zintegrowany z chipem karty, a wzorzec biometryczny przechowywany jest w *Secure Element* karty i nigdy nie jest przesyłany poza kartę. Energia potrzebna do odczytu i weryfikacji biometrycznej pobierana jest z pola elektromagnetycznego anteny terminala. Takie rozwiązanie łączy wygodę płatności zbliżeniowych z poziomem bezpieczeństwa właściwym dla weryfikacji biometrycznej [3] [4].

Na poziomie protokołów płatniczych trwa systematyczne wdrażanie do transakcji internetowych standardu EMV 3-D Secure 2.x (3DS2), który wprowadza bogate uwierzytelnianie oparte na danych kontekstowych (geolokalizacji, historii transakcji, danych urządzenia), redukując liczbę przypadków wymagających dodatkowego potwierdzenia przez użytkownika, przy jednoczesnym podwyższaniu poziomu bezpieczeństwa. Z perspektywy inżyniera systemów embedded oznacza to konieczność implementacji zestawów SDK 3DS2 w aplikacjach mobilnych i integrację z TEE urządzenia w celu bezpiecznego przesyłania danych kontekstowych do serwera autoryzacyjnego [8] [9].

Podsumowanie

Systemy płatności elektronicznych stanowią złożony ekosystem, w którym współpracują układy scalone, mikrokontrolery i oprogramowanie embedded, zapewniając zarówno komunikację, jak i bezpieczeństwo transakcji. Wielowarstwowy stos protokołów NFC, od fizycznej warstwy ISO/IEC 14443, przez format NDEF, aż po komendy APDU standardu EMV, tworzy spójną architekturę, w której każda warstwa pełni precyzyjnie zdefiniowaną rolę. Karty płatnicze, terminale POS oraz urządzenia mobilne integrują funkcje NFC, *Secure Element* i mechanizmy kryptograficzne, umożliwiając realizację płatności zbliżeniowych oraz obsługę tokenów.

Elektronika odgrywa kluczową rolę również w bankomatach i systemach samoobsługowych, gdzie mikrokontrolery współpracują z szyfrującymi klawiaturami PIN, czujnikami antytamper i mechanizmami dystrybucji gotówki, zapewniając bezpieczeństwo i niezawodność operacji. Cyberbezpieczeństwo tych systemów jest jednak nieustannie wystawiane na próbę, od fizycznych ataków skimmingowych, przez wyrafinowane ataki na protokół EMV, po złośliwe oprogramowanie NFC nowej generacji, takie jak NGate czy SuperCard X. Zrozumienie zarówno architektury sprzętowej, jak i wektorów ataków, jest zatem niezbędne dla inżynierów projektujących systemy płatnicze.

Kierunki rozwoju, tj. softPOS, biometria na karcie, płatności IoT i integracja SoC, wskazują na dalszą miniaturyzację

i upowszechnienie elektroniki płatniczej, przy jednoczesnym wzroście wymagań w zakresie bezpieczeństwa i certyfikacji. Systemy płatnicze pozostają jednym z najbardziej wymagających i fascynujących obszarów zastosowań nowoczesnej elektroniki embedded, łącząc szybkość, niezawodność i bezpieczeństwo w globalnym środowisku finansowym.

Filip Krzyżański

Literatura:

[1] https://www.emvco.com/emv-technologies/emv-contactless-chip/
[2] https://nfc-forum.org/what-is-nfc/
[3] https://www.infineon.com/cms/en/product/security-smart-card-solutions/security-controllers/sle-78/
[4] https://www.oracle.com/java/java-card/
[5] https://multos.com/technology/multos-smartcard-technology/
[6] https://www.nxp.com/docs/en/data-sheet/PN5180A0XX_C3_C4.pdf
[7] https://nfc-forum.org/build/specifications/
[8] https://developer.android.com/develop/connectivity/nfc/hce
[9] https://www.emvco.com/emv-technologies/payment-tokenisation/
[10] https://www.pcisecuritystandards.org/standards/
[11] https://www.iso20022.org/
[12] https://www.nasatm.com/pages/how-do-atms-work
[13] https://www.pcisecuritystandards.org/standards/mobile-payments-on-cots-mpoc/
[14] https://blog.pcisecuritystandards.org/pci-mobile-payments-on-cots-mpoc-standard-version-1-1-now-available
[15], [16] https://www.knf.gov.pl/knf/pl/komponenty/img/Bankow%C5%9B%C4%87%20elektroniczna%20w%20teorii%20i%20praktyce_60154.%20Materia%C5%82y%20dla%20%C5%9Brodowiska%20szkolnego_60154.pdf
[17] https://arxiv.org/abs/1605.00681
[18] https://www.eset.com/pl/about/newsroom/press-releases/news/oszustwa-wykorzystujace-platnosci-zblizeniowe-35-krotny-wzrost-nowe-dane-eset/
[19] https://www.money.pl/gospodarka/nowe-zlosliwe-oprogramowanie-atakuje-uzytkownikow-polskich-bankow-7218305203550816a.html, https://www.money.pl/gospodarka/ataki-na-klientow-bankow-cert-ostrzega-przed-nowa-akcja-7218208559827616a.html
[20] https://arxiv.org/abs/2504.12812
[21] https://www.welivesecurity.com/en/eset-research/ngate-android-malware-relays-nfc-traffic-to-steal-cash/
[22] https://www.themobileknowledge.com/wp-content/uploads/2017/05/NFC-Standards.pdf
[23] https://krebsonsecurity.com/2017/02/more-on-bluetooth-ingenico-overlay-skimmers/
[24] https://rfid4u.com/nfc-device-architecture-and-secure-element/

Si vis pacem, para bellum cum intelligentia artificiali

Jeśli chcesz pokoju, szykuj się do wojny z użyciem AI

Roboty walczące z ludźmi to klasyczny motyw w powieściach i filmach SF. Zwykle jednak roboty wymykają się spod ludzkiej kontroli i atakują swoich twórców. W rzeczywistości jednak to człowiek wskazuje cel maszynie, pozostawiając jej jedynie możliwość wyboru drogi do tego celu.

Wojna na Ukrainie trwa już ponad cztery lata. Codziennie kraj jest atakowany setkami, jeśli nie tysiącami dronów i pocisków rakietowych, broniąc się własnymi systemami antydronowymi i kontratakując także z użyciem dronów. Pod koniec lutego USA i Izrael zaatakowały Iran, na co ten kraj odpowiedział własnym kontratakiem dronowym i rakietowym. Na tyle skutecznym, że USA zmuszone były poprosić Ukrainę o pomoc w zwalczaniu używanych przez Iran dronów opartych na rosyjskich modyfikacjach serii Shahed. Tymczasem nasz kraj w ramach programu SAFE planuje zakupić od Ukrainy technologię antydronową, a nasze wojsko nawiązuje współpracę z wojskiem ukraińskim, by lepiej zrozumieć walkę na drony. Wszystko to wskazuje na duży potencjał rynku bojowych bezzałogowców, szczególnie jeśli te rozwiązania będą znacząco tańsze od broni konwencjonalnej, jak rakiety Patriot czy tradycyjne myśliwce i bombowce.

W Polsce już działa szereg firm produkujących drony i systemy antydronowe, ale według różnych źródeł do niedawna łatwiej im było sprzedawać swoje produkty w innych krajach, niż polskiemu wojsku czy innym służbom. W obecnej sytuacji geopolitycznej, gdy USA jest nieobliczalnym sojusznikiem, a Rosja od lat dąży do konfliktu z krajami NATO, Polska musi się sama szykować do obrony nie tylko swoich granic, ale też do obrony (wraz z innymi krajami) granic UE. Zagrożenie ze strony Rosji jest realne, eksperci wskazują na rosnącą liczbę cyberataków, próby ingerencji w wyniki wyborów w różnych krajach, a także niedawne incydenty z dronami nad europejskimi lotniskami. W związku z tym zagrożeniem UE w trakcie polskiej prezydencji zaczęła przygotowywać program SAFE, zapewniający krajom unijnym korzystne, długoterminowe pożyczki na zbrojenia. Polska w ramach tego programu miała otrzymać 186 miliardów złotych, do wykorzystania już od kwietnia br. Jednym z planowanych wydatków był zakup technologii obrony antydronowej od Ukrainy.

Ze względu na to, jak bardzo zmieniło się pole bitwy w ostatnich latach i jak dużą rolę obecnie odgrywają drony, warto przyjrzeć się bliżej stosowanym rozwiązaniom. Czytelnika zaskoczyć może, jak wiele elementów tych systemów to części prosto ze zwykłego sklepu dla elektroników-hobbystów. Systemy sterowania lotem bywają oparte o 32-bitowe mikrokontrolery ARM oraz żyrokompasy

Fotografia 1. Rosyjski dron-pocisk Geran-5

Fotografia 2. Rosyjski dron Geran-2. Występuje też w wersji czarnej za sprawą farby absorbującej sygnały radarowe

i akcelerometry MEMS, a zarówno operator, jak i wbudowany system AI używają do obserwacji terenu komercyjnych modułów kamer, które produkowane są do systemów monitoringu (mają one bowiem większe sensory niż w kamerach do smartfonów i są mniej wymagające od sensorów stosowanych w aparatach cyfrowych). Same drony i płatowce wykonywane są technikami spotykanymi zarówno w modelarstwie RC, jak i w produkcji maszyn wyczynowych. Branża zbrojeniowa może zatem zaoferować w przyszłości posady nie tylko dla inżynierów lotnictwa, ale też programistów systemów embedded, specjalistów od AI i widzenia maszynowego, projektantów systemów FPV i komunikacyjnych. Przyjrzyjmy się zatem dronom, które toczą wojnę za naszą wschodnią granicą.

Rosyjskie drony i roboty na polu walki

Rosyjska filozofia uzbrojenia jest dość tradycyjna – wszystkie drony produkowane są według konkretnych specyfikacji i do realizacji konkretnych zadań. Pozwala to na łatwe skalowanie produkcji. Na początku wojny trzon uzbrojenia dronowego stanowiły konstrukcje irańskie serii Shahed, ale w ostatnich latach Rosja przerzuciła się na własne modyfikacje tych dronów, czasami na tyle zaawansowane, że dostają własne oznaczenia. Produkcja znajduje się daleko poza linią frontu, w kilku dużych ośrodkach. W ten sposób Rosja redukuje ryzyko ataku na fabryki, ale z drugiej strony transport i logistyka są dużo kosztowniejsze. Przyjrzyjmy się zatem na początek dronom latającym.

Geran-5 (**fotografia 1**) to dron-pocisk przeznaczony do ataków kamikaze, a wykonany został z włókna węglowego na stalowym szkielecie. Napęd stanowi chiński silnik turboodrzutowy Telefly TJ200 zapewniający prędkość do 600 km/h i zasięg 950 km. Również chiński jest moduł łączności (Xingkai Tech XK-F358), który pozwala na przesyłanie obrazu, dźwięku i innych danych w obie strony, tworząc z innymi modułami samoorganizującą się sieć mesh. Co ciekawe, takie moduły można kupić na AliExpress za około 9 tysięcy złotych. System nawigacji jest za to produkcji rosyjskiej i rzekomo wykazuje odporność na zagłuszanie. Używa bowiem zestawu 6...12 anten połączonych w jeden system pozwalający odróżnić bliskie sygnały zakłócające od odległych sygnałów satelitów. Za to zupełnie nierosyjskie okazały się takie komponenty, jak mikrokontroler DSP TMS320C6748 od firmy Texas Instruments, z której fabryk pochodzi też kilka innych komponentów. Infineon Technologies i CTS Corporation również produkują części stosowane w Geranie-5. W innych dronach (głównie w systemach sterowania) można znaleźć mikrokontrolery z serii STM32F4, ale te powoli są zastępowane rosyjskimi układami ARM 1986VE1AT produkowanymi przez Milandr. No, ale czy Czytelnik spodziewałby się obecności modułów Nvidia Jetson Orin Nano i TX2 w dronach Geran-2Y i Geran-5? Moduły te Rosja zakupuje w innych krajach za pomocą różnych pośredników, omijając w ten sposób sankcje nałożone przez kraje UE i USA. Teoretycznie przynajmniej moduły od firmy Nvidia mają numery seryjne i prawdopodobnie dałoby się zidentyfikować ścieżki przemytu oraz pośredników, śledząc po numerach drogę modułów od fabryki do szczątków drona. Nic nie wskazuje jednak na to, by były prowadzone poważne działania w celu ukrócenia tego procederu przemytu.

W rosyjskich dronach znaleziono też układy od Analog Devices, Infineon, czy moduły łączności satelitarnej Iridium 9603N. Te ostatnie pozwalają na przesyłanie krótkich komunikatów przez sieć satelitarną Iridium, a w dronach są używane do śledzenia położenia tychże oraz przesyłania informacji o zmianie celu. Serwomechanizmy z kolei wzięte zostały z rynku modelarskiego – są to produkty firm Hitec i Savöx. Telefly, jak wspomniano, produkuje silniki odrzutowe dla rosyjskich dronów, ale część bezzałogowców używa silników klasycznych, a dokładniej czterocylindrowego, dwusuwowego modelu Limbach L550E. Silnik ten to chłodzony powietrzem boxer o mocy 50 KM, produkowany głównie przez chińską filię niemieckiego Limbacha. Ta sama firma produkuje też tańsze klony wspomnianego silnika o niższej trwałości. Warto dodać jeszcze występowanie komputerów jednopłytkowych Raspberry Pi 4 i 5 w połączeniu z modemami LTE – pozwalają one na budowę dodatkowego kanału śledzenia położenia dronów i na przekazywanie telemetrii. Karty SIM, najczęściej ukraińskich sieci, Rosja pozyskuje nielegalnie.

Najpopularniejszą serią rosyjskich dronów kamikaze jest Geran-2 (**fotografia 2**). Maszyny te przypominają formą klasyczne samoloty z układem skrzydeł typu delta, mają masę startową około 200...240 kg i zasięg 1000...2500 km. Kadłub wykonano z kompozytu włókna szklanego i węglowego z wypełnieniem poliuretanowym, a najnowsze modele dodatkowo są malowane farbą absorbującą sygnały radarowe. Te bezzałogowce mają długość ok. 3,5 m i rozpiętość skrzydeł 2,5 m. Silniki MD550 to wspomniane wyżej kopie L550E. Prędkość przelotowa dochodzi do 150...185 km/h. Mimo że system nawigacji Kometa-M jest rzekomo odporny na zagłuszanie, drony są wyposażane w układy nawigacji inercyjnej oparte na układach firm Murata i Analog Devices. Najnowsze modele korzystają z modułów Nvidia Jetson Orin Nano w połączeniu z kamerą w nosie statku, przeznaczoną do wykrywania i klasyfikowania potencjalnych celów – Geran-2 może dokonać wyboru przy braku łączności z operatorem, po czym samodzielnie w ten cel trafić. Spotykane są trzy rodzaje głowic: standardowe o masie 50 kg, wzmocnione o masie 90 kg (z mniejszym zbiornikiem paliwa, co obniża też zasięg) oraz głowice termobaryczne. Te ostatnie działają przez wytworzenie chmury wybuchowego aerozolu, który jest niemal natychmiastowo detonowany. Siła takiego wybuchu jest znacznie większa, ale rozproszona na większej przestrzeni. Wariant E ma pocisk rakietowy powietrze-powietrze, rosyjski operator może go odpalić, gdy zobaczy na obrazie z kamery ukraiński śmigłowiec lub myśliwiec przechwytujący.

Rosja używa szeregu latających dronów zwiadowczych. Dron Orłan-10 to podstawowy model obserwacyjny o zasięgu do 120 km i czasie

Fotografia 3. NRTK Kuryer

Fotografia 4. Uran-9, czyli z dużej lufy mały ogień. Źródło: MAXIM SHIPENKOV /PAP/EPA

lotu nawet 16 godzin. Ma on system nawigacji Kometa M, a jego głównym zadaniem jest naprowadzanie ognia artylerii. Bliźniaczy model Orłan-30 ma na pokładzie oświetlacz laserowy pozwalający zaznaczyć cele dla pocisków precyzyjnych 2K25 Krasnopol. Pociski te wystrzeliwane są z dział kalibru 152 mm lub 155 mm i potrafią korygować lot by trafić tam, gdzie wskazuje plamka oświetlacza. Rosja używa ich do ataków na przemieszczające się pojazdy. Oba modele Orłana są relatywnie prostymi płatowcami, co pozwala na tanią, masową produkcję (250...350 sztuk miesięcznie według obecnych szacunków). Wadą konstrukcji jest głośny silnik spalinowy pozwalający na łatwe namierzenie i zestrzelenie tych dronów.

Inną konstrukcją, znacznie nowocześniejszą, jest model Zala 421-16E produkowany przez koncern Kałasznikow. Dron ten posiada napęd elektryczny, co ogranicza jego zasięg do 70 km, a profil „latającego skrzydła" dodatkowo utrudnia wykrycie i klasyfikację przez systemy radarowe. Dron w najnowszej wersji ma zaawansowany układ optyczny ze stabilizacją obrazu, pozwalający na rozpoznawanie twarzy z wysokości 1,5 km. Zała współpracuje z rosyjskimi pociskami z serii Lancet. SA to pociski naprowadzane nurkujące, które potrafią krążyć nad polem walki przez długi czas, zanim uderzą w wybrany cel. Najnowsza rodzina Lancetów posiada własne systemy wizualnej identyfikacji celu za pomocą AI. Lancet ma układ skrzydeł typu X, co znacznie zwiększa jego manewrowość i stabilność w locie nurkowym do celu, a sam pocisk rozwija prędkość nurkowania do 300 km/h. Kadłub tego pocisku wykonany jest z kompozytu węglowego i tworzyw sztucznych, co dodatkowo utrudnia jego wykrywanie. W połączeniu z kamerą termowizyjną drona Zała pociski Lancet potrafią być doprawdy groźne, zwłaszcza w atakach nocnych. Według danych wywiadowczych Rosja produkuje 80...120 sztuk dronów Zała miesięcznie.

Trzecim dronem zwiadowczym stosowanym przez Rosję jest Supercam S350. Płatowiec ten jest wyjątkowo groźny ze względu na doskonałą optykę, pułap do 5 km oraz napęd elektryczny z baterią pozwalającą na lot przez 4...5 godzin. Dron o rozpiętości skrzydeł 3,5 m startuje z katapulty pneumatycznej (podobnie jak Orłany), a do lądowania używa spadochronu. Prędkość przelotowa 65...120 km/h oraz zasięg do 100 km, w połączeniu z zaawansowanym systemem łączności odpornym na zagłuszanie, czynią tę maszynę szczególnie problematycznym celem dla Ukrainy. Bezzałogowiec ten współpracuje z Lancetami i Krasnopolami i może działać autonomicznie za sprawą automatycznego rozpoznawania celów. Supercam S350 potrafi też tworzyć sieć Mesh celem zwiększenia zasięgu łączności i jej odporności na zagłuszanie. Wewnątrz znaleźć można chińskie silniki elektryczne Tiger Motors, sensory optyczne z Korei Południowej i mikrokontrolery z USA czy Europy. Wobec tej maszyny Ukraina stosuje dwa rodzaje ataków: drony przechwytujące oraz ataki na miejsca, z których drony startują.

Rosja ma też pojazdy naziemne. Są to różnej wielkości platformy bojowe o rozmaitych funkcjach. NRTK Kuryer to uzbrojony dron bojowy przeznaczony do atakowania pozycji ukraińskich i do osłony w razie odwrotu. Posiada napęd elektryczny, dzięki czemu jest cichy, ale za to powolny. Jest też podatny na ataki dronów FPV i potrafi ugrzęznąć w błocie lub w leju po bombie. Najnowsza seria używa modułów Jetson Orin Nano do lepszej nawigacji w terenie. Nie pomaga to w rozwiązaniu problemu polegającego na tym, że gdy Kuryer przyjmuje pozycję do ataku, sam staje się łatwym celem. Dron ten występuje też w wersjach do transportu sanitarnego lub do prowadzenia walki radioelektronicznej (WRE). Przykładowy wariant bojowy prezentuje **fotografia 3**. Warto dodać, że drony Kuryer są na tyle tanie w produkcji, iż mimo wad stanowią główne „mięso armatnie" pośród lądowych maszyn bezzałogowych, a możliwość pracy jako retransmitery poprawia ich zasięg operacyjny.

Innym pojazdem tego typu jest Uran-9 wyposażony w armatę 30 mm. Z tego też powodu napędza go silnik diesla. W propagandzie rosyjskiej miał być „rewolucją" na polu walki. Okazało się jednak (na szczęście), że na froncie jest kompletnie bezużyteczny, ale za to drogi. Armata 30 mm może dobrze wyglądać na papierze, ale brak jakiejkolwiek stabilizacji ognia sprawia, że jest niecelna. Przy dużej masie własnej (12 ton) Uran-9 ma ogromne problemy z awaryjnością zawieszenia, a silnik diesla potrzebny do jego napędzania czyni go łatwym celem dla dronów wyposażonych w termowizję. Dodajmy faktyczny zasięg łączności w terenie zrujnowanym (dawniej zabudowanym), który wynosi 300 metrów, zamiast deklarowanych 3 km i mamy obraz pięknej katastrofy. Przed manewrami Zapad-2021 pokazano te drony opinii publicznej – do obejrzenia na **fotografii 4**.

Spójrzmy jeszcze na dwa pojazdy, które Rosjanom wyszły w miarę dobrze: Ulan-2 i Omich. Ulan-2 to dron logistyczny o nośności 200...500 kg ładunku lub dwóch rannych żołnierzy z noszami. Skuteczność ewakuacji medycznej z jego użyciem wynosi 30%, co jest bardzo wysokim wynikiem, jak na rosyjskie wojsko. Ulan-2 używa napędu hybrydowego, co pozwala mu cicho podjechać pod linię frontu. Omich jest mniejszym dronem o napędzie elektrycznym, stosowanym głównie jako dron kamikaze i transporter do dowożenia niedużych ilości zapasów krytycznych, jak woda czy baterie do radiostacji. Oba pojazdy używają łączności światłowodowej, przy czym dla Omicha to jedyna opcja.

W kwestii rosyjskiej obrony antydronowej, głównymi metodami są różnego rodzaju pancerze, klatki, siatki i tym podobne fizyczne bariery, które mają zatrzymać lub odbić drony ukraińskie. Rosja łączy te proste rozwiązania z systemami zakłócania łączności (WRE), jak na przykład montowane na magnes do pojazdów urządzenia Volnorez, które omiatają pasmo radiowe od 400 MHz do 6 GHz. Jedną z ciekawszych broni w tym arsenale są ręczne „pistolety WRE", które pozwalają żołnierzom na „ostrzeliwanie" nadlatujących dronów FPV (*First Person View*). Gładkolufowe strzelby strzelające amunicją śrutową też są skuteczną bronią na froncie walki z dronami – przy odrobinie szczęścia

i zręczności zwinny dron da się trafić choćby częścią chmury śrutu. Warto tu zaznaczyć, że wbrew temu, co pokazują amerykańskie filmy akcji, rozproszenie śrutu nie jest aż tak wielkie. Rosja używa też systemów przeciwlotniczych, w tym także pamiętających czasy drugiej wojny światowej. Systemy takie wymagają odnowienia i wymiany układu celowniczego na współczesny celownik optoelektroniczny.

Do wykrywania ukraińskich dronów Rosja stosuje też systemy oparte o AI i sieć mikrofonów, gdyż małe i zwinne drony FPV mają znikomy ślad radarowy. Aktywną formą obrony są też własne drony FPV, oparte na komercyjnych konstrukcjach wyścigowych, tylko ze wzmocnionym szkieletem ramion, które strącają ukraińskie drony przez zderzanie się z nimi. Inne drony (Volk-12, Volk-18) dysponują wyrzutniami kevlarowych sieci, którymi miotają z odległości 3...5 metrów w stronę rotorów dronów ukraińskich, co je skutecznie strąca. Volk-18 ma celownik optyczny sprzężony z AI, które asystuje w celowaniu. Ostatnią grupę stanowią drony wyposażone w broń gładkolufową kalibru 12/70, strzelającą śrutem lub specjalnymi pociskami odłamkowymi. Wadą tego rozwiązania jest spory odrzut i konieczność jego kompensacji. Na początku 2026 roku rosyjskie drony przechwytujące okazały się na tyle skuteczne, by stworzyć strefy, do których drony ukraińskie nie mogły wlecieć. Ukraina dość szybko wdrożyła jednak taktykę wysyłania własnych „interceptorów" wraz z dronami zwiadowczymi i atakującymi, co prowadzi do walk lotniczych przypominających czasy pierwszej wojny światowej. Warto zaznaczyć, że wszystkie te drony są relatywnie prostymi konstrukcjami opartymi o komercyjne modele, głównie chińskie.

Ukraińskie drony i roboty

Ukraina w obliczu ograniczeń w ilości żołnierzy dość szybko wdrożyła własne systemy dronowe i antydronowe do walki. Dużą przewagą Ukrainy jest brak ograniczeń w dostępie do komponentów i gotowych dronów, a także duże wsparcie ze strony krajów UE (i USA). Ukraina zastosowała też inną taktykę projektowania i produkcji dronów: zamiast skupiać się na kilku modelach (jak Rosja), produkują setki różnych platform, od zupełnie amatorskich konstrukcji, aż po bardzo zaawansowane systemy bojowe od dużych firm. Dzięki temu Ukraina może w krótkim czasie przetestować różne rozwiązania, wybrać najlepsze i wdrożyć je do użycia, a w razie zmiany sytuacji na froncie, równie szybko się dostosować. Nowe rozwiązania pojawiają się nawet i co tydzień, z czym Rosja nie jest w stanie konkurować. Takie podejście oznacza też, że nie ma jednej, centralnej fabryki dronów, tylko setki małych manufaktur rozproszonych po całym kraju. Tymczasem rosyjska produkcja skupiona jest w kilku dużych fabrykach, jak choćby Ałabuga. Ukraina posiada też największą na świecie siatkę farm drukarek 3D i używa ich do masowej produkcji różnych komponentów, w tym obudów i ram dla dronów czy stabilizatorów lotu, które można przyczepić do granatu zrzucanego z drona niczym małą bombę.

Spójrzmy zatem na jeden z dronów latających, odpowiedzialny za ataki na rosyjskie rafinerie i składy amunicji Lyutyi (**fotografia 5**).

Fotografia 5. Ukraiński dron latający dalekiego zasięgu Lyutyi, odpowiedzialny za niszczenie rosyjskiej infrastruktury i składów amunicji

Fotografia 6. Uj-26 Bober – dron latający w układzie kaczki, oferujący dzięki temu lepsze parametry lotu. Ze względu na mniejszy rozmiar głowicy z ładunkiem wybuchowym, zwykle jest stosowany do precyzyjnych ataków

Jest to dron w formie klasycznego samolotu o rozpiętości skrzydeł 6,7 m i długości prawie 4,4 m. Napęd stanowi czterosuwowy silnik benzynowy o mocy 50...60 KM, który zamontowany jest z tyłu i pcha samolot. Zbiornik paliwa w kadłubie pozwala na 10...12 godzin lotu i zasięg 1000...1200 km (zależnie od masy głowicy bojowej). Konstrukcja wykonana jest z włókna szklanego, dzięki czemu jest wystarczająco sztywna i wytrzymała, a przy tym zostawia mniejszy ślad radarowy. Głowica bojowa o masie 50...75 kg może nie jest duża, ale wystarczy do niszczenia infrastruktury krytycznej. Przy ataku na rafinerię wystarczy przebić kolumnę rektyfikacyjną i detonować taki ładunek, by wywołać pożar znacznej części rafinerii. Remont po takim ataku trwa miesiącami, bo komponenty w wielu przypadkach pochodzą od firm zachodnich i – o ile Rosja może przemycić kilka skrzynek modułów Nvidia Jetson – to mierząca kilkanaście metrów długości stalowa kolumna rektyfikacyjna może być nieco kłopotliwa dla przemytników. Lyutyi posiada dość rozbudowany system nawigacji, oparty na wieloelementowych antenach GPS, które są mniej podatne na zagłuszanie (analogiczne rozwiązanie do rosyjskich systemów Kometa-M), ale dzięki dostępowi do zachodnich komponentów posiada też bardzo rozbudowany system nawigacji inercyjnej, pozwalający na utrzymanie kursu przez kilkadziesiąt kilometrów. W końcowej fazie lotu dron używa prostego systemu widzenia maszynowego, by rozpoznać cel (np. wspomnianą kolumnę rektyfikacyjną) i skorygować kurs z dokładnością do 1...2 m.

Innym ciekawym dronem latającym jest Uj-26 Bober (**fotografia 6**) firmy UkrJet, czyli mniejsza maszyna latająca o konstrukcji tzw. kaczki (*Canard*). W tym układzie ster wysokości znajduje się z przodu płatowca, a skrzydła bliżej jego tyłu. Maszyna uzyskuje większą siłę nośną, dzięki czemu może latać wolniej. W razie utraty siły nośnej (przeciągnięcie – stall), przód naturalnie opadnie pierwszy, a płatowiec wejdzie w lot ślizgowy odzyskując stabilność wraz ze wzrostem prędkości. Maszyna też jest bardziej zwrotna dzięki temu układowi. Jednym z powodów, dla których w zwykłych samolotach układ kaczki spotykany jest rzadko wynika właśnie z tej zwrotności – zbyt gwałtowny manewr prowadzi do ogromnych przeciążeń. Dron pozbawiony „wkładki mięsnej" może sobie pozwolić na gwałtowniejsze manewry. Bober, mimo mniejszych wymiarów (2,5 m × 2,5 m), może unieść głowicę o masie 20 kg i dostarczyć ją na odległość 800...1000 km. Kadłub o opływowym kształcie wykonany jest z włókna węglowego, a silnik z tyłu zapewnia prędkość przelotową 120...150 km/h, zaś prędkość maksymalna to 200 km/h. Najnowsze modele implementują kilka unikalnych rozwiązań technologicznych, radykalnie podnoszących ich wartość bojową. Bober, poza standardową nawigacją satelitarną i inercyjną, używa też nawigacji wizualnej. Ukraina posiada dostęp do dokładnych map satelitarnych i wgrywając taką mapę do maszyny, ta może rozpoznać rzeki, drogi i lasy wizualnie, a następnie wykorzystać te informacje

do ustalenia pozycji i kursu. System FPV i łączność satelitarna pozwalają operatorowi wybrać dokładnie, w co dron uderzy – bez problemu można naprowadzić go na konkretne okno lub otwarty właz pojazdu opancerzonego. Głównym zastosowaniem tego drona są zatem precyzyjne ataki na instalacje wojskowe, czy nawet budynki rządowe i prywatne rezydencje rosyjskich oligarchów.

Ciekawą grupę dronów UAV stanowi rodzina Baba Jaga, czyli ciężkie heksakoptery i oktokoptery używane przez Ukrainę do nocnych nalotów bombowych. Drony te oparte są na komercyjnych konstrukcjach dronów rolniczych, jak DJI Agras T40, ale poddane licznym modyfikacjom. Rama wykonana jest z włókna węglowego i aluminium lotniczego, a 6...8 użych silników elektrycznych napędza proporcjonalnie duże śmigła. Wprawdzie zasięg wynosi tylko 16 km, a prędkość przelotowa to marne 40 km/h (z ładunkiem) lub 80 km/h (bez), ale opisywany model ma za to kamerę termowizyjną z zoomem 20×/30× oraz system wsparcia celowania, co pozwala zrzucić minę przeciwczołgową lub inny ładunek precyzyjnie na cel. Drony Baba Jaga często mają terminale Starlink, a od niedawna zaczęły być używane jako „nosiciele" mniejszych dronów FPV i jako latające wieże łączności dla nich. Mimo że są duże, powolne i głośne, drony te sieją spustoszenie wśród rosyjskiego sprzętu wojskowego.

Również w przypadku dronów FPV Ukraina opracowała szereg zróżnicowanych rozwiązań. Ramy o różnej wielkości (6, 8 i 10 cali) wykonane są z włókna węglowego. Obudowy elektroniki coraz częściej są drukowane z PET-G (to jeden z moich ulubionych filamentów) lub z nylonu z dodatkiem włókna szklanego. Za napęd służą silniki BLDC takich firm, jak Emax, choć Ukraina ma też własne kopie. Kontrolery lotu oparte są na układach STM32F4 lub F7, z mocno zmodyfikowanym firmware Betaflight. Drony FPV często też dysponują systemami AI opartymi na modułach Nvidia Jetson Orin Nano, albo na chińskich alternatywach, które są sporo tańsze. Operator może dzięki temu wskazać cel z odległości 500 metrów, a dron w niego trafi, nawet jak całkowicie utraci łączność. Drony z serii „Vandal" stosują jeszcze ciekawsze rozwiązanie: cienki jak włos światłowód rozwijany przez drona za sobą, dający zasięg 10 km i krystalicznie czysty obraz wysokiej rozdzielczości. Drony te są odporne na zagłuszanie, a operator cały czas zachowuje nad nimi kontrolę.

Ukraińskie drony FPV stosują trzy rodzaje ładunku bojowego:

- opisane wcześniej **bomby termobaryczne**, stosowane do walki z żołnierzami w bunkrach i piwnicach. Fala uderzeniowa w zamkniętej przestrzeni jest zabójcza;

Fotografia 7. Dron Ratel S, którego zadaniem jest podjechać pod pojazd wroga i wysadzić go w powietrze. Źródło: X/Mychajło Fiodorow

- **ładunki odłamkowe**, detonowane 2...3 metry nad głowami żołnierzy i rozrzucające setki kulek na dużym obszarze;
- przeciw pojazdom Ukraińcy stosują specjalne **pociski formowane**, które odpalane są z odległości 2...3 metrów – niweluje to stosowane przez Rosję siatki i klatki jako fizyczne bariery antydronowe.

Pewną ciekawostką jest zastosowanie w dronach FPV najnowszych przetworników optycznych Sony Starvis 2. Sensory te oferują lepszą jakość obrazu w warunkach słabego oświetlenia oraz w paśmie bliskiej podczerwieni, dlatego stosowane są głównie w kamerach monitoringu i wideorejestratorach.

Podobnie jak Rosja, Ukraina też używa lądowych pojazdów bezzałogowych. Kraj posiada trzy podstawowe typy pojazdów bojowych: Ratel S, Lyut i Ironclad. Ratel S (**fotografia 7**) to kołowy dron kamikaze przenoszący dwie miny przeciwpancerne. Jego niski profil pozwala mu podjeżdżać pod pojazdy wroga, zanim zdetonuje swój ładunek. Odnotowano przypadki, gdy ten robot był parkowany pod konstrukcją mostu celem jego zburzenia. Relatywnie prosta i tania konstrukcja oznacza, że konieczne jest zdalne sterowanie przez cały czas. Jako wsparcie łączności używane są zmodyfikowane drony latające, najczęściej DJI Mavic 3 i Autel EVO II. Do podwozia

Fotografia 8. Lyut 2.0, pojazd wsparcia ogniowego wyposażony w CKM oraz jego operator. Źródło: Brygada Azova, Telegram

Fotografia 9. Dron Ironclad

drona montowany jest wojskowy moduł retransmittera, po czym dron wznosi się na wysokość 300...500 metrów nad obszarem działań. Kamera drona wykorzystywana jest przy okazji do zwiadu. Problemem tego rozwiązania jest cena samych dronów, dlatego w październiku 2025 ukraiński MON zdecydował się na tańszą, dedykowaną platformę Kolibri 13 FR1 firmy TAF Industries. Alternatywnie drony Baba Jaga i proste płatowce są również używane w tej roli. Baba Jaga z modułem Starlink oferuje zasadniczo nielimitowany zasięg łączności, ograniczony jedynie ilością energii w akumulatorach.

Drony z serii Lyut (**fotografia 8**) oferują wsparcie ogniowe żołnierzom piechoty. Wyposażone są w ciężki karabin maszynowy kalibru 7,62 mm oraz system automatycznego śledzenia celów. Zadanie to ułatwia kamera wysokiej rozdzielczości z zoomem 30× i termowizją. Drony te mają relatywnie stabilną bazę oraz dobrą dzielność terenową i często występują na froncie w pierwszej linii, gdzie mogą prowadzić długi ostrzał. Czasami są wręcz zostawiane, by zasadzić się na atakujące wojska rosyjskie i znienacka je ostrzeliwać.

Ironclad (**fotografia 9**) to najcięższy dron bojowy Ukrainy. Jest to opancerzona maszyna składająca się z dwóch części: przedniej i tylnej, połączonych przegubem. Napęd realizowany jest za pomocą silników elektrycznych zasilanych za pomocą akumulatorów i generatora spalinowego. Takie rozwiązanie hybrydowe (stosowane też przez Rosję) ma szereg zalet: może cicho poruszać się na linii frontu z małym śladem termicznym, ale poza frontem oferuje większy zasięg i moc. Ironclad radzi sobie lepiej w terenie od dronów rosyjskich dzięki budowie przegubowej – każda z par kół może lepiej dopasować się do ukształtowania terenu poprawiając przyczepność w trudnych warunkach. W Internecie nie ma zbyt wielu szczegółów na temat tego drona, poza masą (1800 kg), zasięgiem (130 km) i prędkością maksymalną (20 km/h na drodze i 15 km/h w terenie). Uzbrojenie stanowić może granatnik automatyczny albo ciężki karabin maszynowy 7,62 mm lub 12,7 mm. Masa ładunkowa dla amunicji i uzbrojenia wynosi 300 kg. Ciekawą informacją jest fakt, że Ironclad może samodzielnie przemieszczać się dzięki nawigacji satelitarnej, a użycie AI pozwala na automatyczne wyśledzenie celów – operator musi wydać jedynie polecenie strzału.

Sirko-S1 firmy SkyLab UA używany jest przez ukraińskie wojsko jako dron logistyczny. Jest dość tani (kosztuje tylko 8 tysięcy dolarów), ale w zamian oferuje relatywnie niską konstrukcję i nośność do 200 kg, co jest wykorzystywane w transporcie amunicji i zapasów. Posiada też funkcję automatycznego podążania za żołnierzem. Istnieje też wariant z masztem z kamerą, dzięki któremu ten dron staje się mobilnym punktem obserwacyjnym. Do ewakuacji rannych żołnierzy Ukraina stosuje od niedawna dedykowane drony FoxTac o bardzo niskim profilu. Tak niskim, że ranny żołnierz znajduje się zaledwie kilkanaście centymetrów nad ziemią. Drony te mają niewielki zasięg zdalnego sterowania, tylko 700 metrów, ale potrafią samodzielnie wrócić do bazy.

Z powodu ciągłych, nieustannych ataków rosyjskich na cele cywilne i wojskowe, Ukraina zmuszona była opracować najskuteczniejszy na świecie, wielowarstwowy system antydronowy (który Polska zamierza od nich zakupić). Cały kraj znajduje się pod Pokrovą, systemem spoofingu nawigacji satelitarnej, który wprowadza w błąd rosyjskie drony i rakiety. Drugim elementem strategicznej warstwy obrony jest sieć czternastu tysięcy czujników akustycznych montowanych na wieżach telefonii komórkowej (i nie tylko), które w połączeniu z AI potrafią zidentyfikować i namierzyć nisko przelatujące drony rosyjskie niewidoczne dla radarów. Drugim elementem obrony są systemy WRE. Mniejsze „kopuły” (system Piranha) zapewniają zagłuszanie rosyjskich dronów FPV w promieniu kilkuset metrów wokół urządzenia. Większe systemy (Bukovel-AD), montowane na pick-upach, mające zasięg wykrywania 70 km, a aktywnego zagłuszania 20 km – przeznaczone są do ochrony celów stacjonarnych. Ukraina używa też przenośnych urządzeń WRE, które mają chronić pojedyncze oddziały oraz systemów wyrzutni siatki, które mogą „usidlić” dron FPV z odległości 25 metrów. Siatka ma wymiary 3×3 metry i nie wymaga aż tak dokładnego celowania, jak strzelba gładkolufowa.

Przeciw dużym dronom rosyjskim Ukraina stosuje szereg własnych dronów. Model Sting, kosztujący poniżej trzech tysięcy dolarów, strąca rosyjskie drony Shached/Geran równie skutecznie, co o wiele droższe rakiety systemu Patriot. Od maja 2025 roku drony te strąciły ponad 40 tysięcy wrogich bezzałogowców. Z kolei drony P1-Sun atakują głównie drony zwiadowcze i robią to z prędkością do 450 km/h. Rama tych pojazdów, wraz z opływową skorupą, wykonane są w technologii druku 3D. Drony Sting-II z kolei wykorzystują większą baterię i cyfrową kamerę nocną do patrolowania przestrzeni powietrznej przez kilkanaście minut, by zaatakować wykryty cel. Drony Bullet to chyba najciekawszy twór Ukrainy w tej kategorii: quadrocoptery z silnikiem turboodrzutowym. Tradycyjne wirniki pozwalają na pionowy start i manewrowanie, podczas gdy silnik odrzutowy nadaje im wystarczającą prędkość by przechwycić cel w locie. Ukraina ma też dron płatowy przeznaczony do obrony powietrznej o nazwie Salyut. Może on latać dużo dłużej, niż typowy quadrocopter. Trzeba jednak pamiętać, że wysoka skuteczność obrony powietrznej Ukrainy wynika też z użycia AI do wykrywania nadlatujących dronów oraz w końcowej fazie lotu przechwytującego. Interceptor nie musi też uderzyć we wrogi dron, wystarczy że detonuje swój ładunek wystarczająco blisko, by odłamki zniszczyły pojazd.

Wojna maszyn

Z tego krótkiego przeglądu wyłania się jeden wniosek: przyszłość pola walki należy do AI. Zarówno w kwestii wykrywania i namierzania celów, jak i realizacji samego ataku, automatyzacja i sztuczna inteligencja w coraz większym stopniu ograniczają udział człowieka w walce. Teoretycznie można by zbudować całkowicie autonomicznego robota, który ruszyłby na umocnienia wroga, automatycznie wykrył żołnierzy (termowizja) i prowadził skuteczny ogień. Dla przykładu można rozważyć konstrukcję ciężkiego oktokoptera, wyposażonego w szybki komputer z AI i stabilizowany gimbalami karabin – maszyna taka mogłaby lecieć tuż nad ziemią, unikając przeszkód dzięki LIDARom i kamerom, by następnie ostrzelać każdy cel rozpoznany przez system AI jako sprzęt wojskowy oraz każdy obiekt wielkości i kształtu człowieka i o temperaturze ludzkiego ciała. Dyskusje na temat takich rozwiązań trwają już od dekad, a ich intensywność wzrosła wraz z atakiem Rosji na Ukrainę i zwiększeniem użycia AI na froncie przez obie strony. Generalnie

na Zachodzie panuje opinia, że powinno się wprowadzić ogólnoświatowy zakaz tak dalece posuniętej „automatyzacji zabijania". W praktyce jednak należy rozważyć, czy warto rezygnować ze skutecznej broni na rzecz wyższości moralnej nad wrogiem, który do takich zakazów raczej nie będzie się stosował? Pokrewny problem pojawił się właśnie w trakcie konfliktu w Ukrainie. Rosja nie ratyfikowała zakazu stosowania min przeciwpiechotnych, więc rozstawia je na okupowanych terenach. Ukraina traktat ratyfikowała i sama nie może chronić swoich ziem przed szturmem agresora.

Czy zatem powinno się „wyciąć" człowieka z pętli kontroli nad bronią autonomiczną? Na to pytanie Czytelnik sam musi sobie odpowiedzieć, choć zdaniem Autora nie tylko nie powinno się tego robić, a w praktyce jest to jeszcze niewykonalne. W przypadku opisanego wyżej drona bojowego to człowiek podejmuje decyzję o wysłaniu go na misję, więc nadal mamy element kontroli. Drugim elementem może być nakaz przerwania ataku i powrotu do bazy. Ale gdy wiemy, że dron znajduje się u celu, nie potrzeba odpowiadać za każdy strzał. Zresztą nawet teraz obie strony wojny w Ukrainie pozwalają swoim dronom na przeprowadzenie ataku po tym, jak cel został wskazany lub zidentyfikowany automatycznie. Pragmatyzm na polu walki jest ważniejszy od względów moralnych, szczególnie dla strony broniącej się przed wrogiem, który za nic ma wszelkie traktaty i prawa człowieka. Polskie wojsko również musi być gotowe na produkcję i używanie dalece zautomatyzowanych dronów i systemów antydronowych opartych na AI, szczególnie jeśli główny sojusznik Polski, USA, może być zaangażowany w konflikt na Bliskim Wschodzie (Iran, ale też organizacje Hamas i Hezbollah) lub w Azji z Chinami (potencjalna wojna o Tajwan) i w razie agresji ze strony Rosji nie być w stanie zaangażować się w Europie.

Wszystko wskazuje na to, że kolejne dekady przyniosą znaczny rozwój w branży zbrojeniowej i wzrośnie wykorzystanie w niej systemów AI. Istotnymi kierunkami będą zarówno: produkcja dronów krótkiego zasięgu w ogromnych ilościach, jak i tworzenie rozwiązań pozwalających atakować cele daleko poza linią frontu. Sytuacja Ukrainy pokazuje też, jak ważna jest decentralizacja produkcji oraz rozproszona sieć detekcji. Spoofing nawigacji satelitarnej w razie ataku to też dobra taktyka, ale nie będzie działać zbyt długo, bo coraz łatwiej będzie zbudować system nawigacji wizualnej, odporny na zagłuszanie. I tak, jak powstają autonomiczne systemy ataku, tak też powinny powstawać zautomatyzowane systemy obronne. W czasach drugiej wojny światowej powstały pierwsze systemy radarowego kierowania ogniem przeciwlotniczym, ale drony są celami trudniejszymi do wykrycia, a radary dodatkowo nie radzą sobie dobrze przy ziemi. Co można użyć w zamian? Detektory akustyczne, jak w Ukrainie, ale też LIDARy i pasywne detektory optyczne (kamera + AI). Systemy takie, w formie modułów można by, wzorem Ukrainy, montować na masztach telefonii komórkowej, słupach energetycznych i na dachach budynków. Zaprojektowanie takiego systemu wymagać będzie sporej kadry specjalistów, zarówno od systemów embedded jak i od AI, projektowania elektroniki i konstrukcji mechanicznej. Przy czym całość musiałaby być tania w produkcji i łatwa w instalacji.

Innym dobrym kierunkiem rozwoju jest projektowanie tanich płatowców bezzałogowych. Zarówno Rosja, jak i Ukraina używają „zwiadowców" i „wabików" zrobionych ze styropianu i tektury. Ten pierwszy materiał spotyka się dość często w latających modelach RC. Zrobienie dobrej maszyny latającej to spore wyzwanie, gdyż wymaga zachowania odpowiedniego balansu między rozpiętością skrzydeł (większa siła nośna, ale i większe opory powietrza), wielkością silnika (dostępny ciąg i maksymalna prędkość lotu) oraz masą całej konstrukcji (która wpływa na osiągi i ładowność). Zaletą budowania bezzałogowców jest to, że prototyp nie musi być wykonany tak solidnie, jak prototyp samolotu załogowego, skala może być (sporo) mniejsza, a dodatkowo na rynku nie brakuje części dla modelarzy. Można się pokusić o wzięcie konstrukcji RC o dobrych właściwościach lotnych i przeskalowanie jej do wielkości drona wojskowego – amatorzy przetestowali każdą typową i nietypową konstrukcję płatowca. Gotowe modele latające (bez elektroniki) można nabyć w Chinach w cenie od niespełna trzystu do kilku tysięcy złotych.

Przy prototypowaniu jakiegokolwiek drona latającego czy naziemnego (o dronach wodnych nie wspominając) pojawi się pytanie o modele AI i moduły do nich. Nie każdy może sobie pozwolić na zakup modułu Nvidia Jetson, nawet starszej generacji, by ryzykować jego zniszczenie lub zagubienie wraz z modelem. Na szczęście są tańsze alternatywy, choć może nie tak potężne, jak amerykańskie. Firma Sipeed z Chin ma w swojej ofercie tanie płytki MaixCAM, MaixCAM Pro i MaixCAM2 specjalnie stworzone do pracy z modelami VLM, w cenie 2...10 razy niższej od oferty marki Nvidia. Wygenerowanie prostego modelu klasyfikującego obiekty dla tej płytki zajmuje godzinę (zarówno czas generowania, jak i rezultat zależą od wielkości i jakości zestawu danych szkoleniowych). Ponoć praca z tymi płytkami jest tak łatwa, że każdy może stworzyć własny model i aplikację. Moduły te mają kilka rdzeni RISC-V: główny realizuje funkcje związane z obsługą modelu VLM (model wizualno-językowy, ang. Vision Language Model), ale dodatkowy, z systemem RTOS, może zostać oddelegowany do obsługi I/O. Wystarczy jeszcze podłączyć moduł IMU (inercyjna jednostka pomiarowa, ang. Inertial Measurement Unit) i prosty kontroler serwomotorów, by zintegrować ze sobą kontrolę lotu oraz jego stabilizację. A to otwiera też drogę do budowy drona, który naturalnie jest niestabilny w locie, co w połączeniu z – przykładowo – konfiguracją kaczki znacznie zwiększa manewrowość.

Zakończenie

Wojna przyszłości dzieje się już teraz i nie wygra jej ten, kto ma większą liczebność wojska, lecz ten, kto ma przewagę technologiczną. Tę przewagę należy wypracowywać już teraz, także jako narzędzie odstraszania. W końcu od dawna wiadomo, że „Si vis pacem, para bellum".

Paweł Kowalczyk, EP

Moduły SoC i SoM w elektronice

Obecnie mamy do dyspozycji wielordzeniowe, bardzo wydajne mikrokontrolery i procesory, miniaturowe pamięci półprzewodnikowe o gigabajtowych pojemnościach oraz cały wachlarz interfejsów przewodowych i bezprzewodowych – technologie, które sprostają niemal każdemu wyzwaniu. Jednak zaprojektowanie i zbudowanie miniaturowego i wydajnego systemu elektronicznego, który połączy te wszystkie nowoczesne układy, jest zadaniem bardzo trudnym – wymaga wiedzy, doświadczenia i czasu. Dlatego powstały komponenty, które zastępują te najbardziej skomplikowane sekcje w wielu projektach elektronicznych i są dostępne jako gotowe moduły.

Rysunek 1. Popularny układ SoC typu ESP32 od Espressif (https://www.mouser.pl/datasheet/2/891/Espressif_Systems_01292021_esp32-1991551.pdf)

Każdy bardziej zaawansowany system elektroniczny wymaga wydajnego procesora (CPU), szybkiej i pojemnej pamięci operacyjnej (RAM), nieulotnej pamięci danych (NVM) oraz odpowiednich interfejsów przewodowych i bezprzewodowych. Zastąpienie tych elementów kompaktowym, przetestowanym modułem diametralnie przyspiesza prace projektowe i uruchomieniowe. Jednak różnorodność zastosowań wymusza przynajmniej kilka typów rozwiązań. Dlatego obecnie wyróżniamy kilka kategorii produktów tego typu.

SoC, SiP, MCM i PoP

Pierwsza grupa to komponenty, które są dostępne jako pojedyncze układy scalone. Ich parametry i funkcje mogą się bardzo różnić, a budowa wewnętrzna jest realizowana na kilka sposobów. Poniżej zostały opisane najczęściej stosowane technologie.

SoC (*System on Chip*)

Moduł SoC integruje wszystkie komponenty niezbędne do działania systemu w postaci układu scalonego, czyli na pojedynczym kawałku krzemu. Układy scalone typu System on Chip mają wiele zalet – są wydajne, kompaktowe i ekonomiczne w produkcji. Znajdują zastosowanie w systemach zorientowanych na małe wymiary i niskie zużycie energii, takich jak urządzenia IoT, smartfony czy systemy wbudowane.

Standardowy SoC może zawierać procesor CPU, akcelerator graficzny GPU (*Graphics Processing Unit*), akcelerator AI/NPU (*Neural Processing Unit*), pamięci RAM i/lub ROM, interfejsy zewnętrzne USB/HDMI/Ethernet, interfejs bezprzewodowy Wi-Fi/Bluetooth/5G oraz inne komponenty, takie jak przetworniki analogowo-cyfrowe czy układy zasilania. Pomimo kompaktowych rozmiarów, układy scalone SoC są niezwykle wydajne i często przewyższają parametrami systemy zbudowane z kilku oddzielnych układów. Z drugiej strony są kosztowne w projektowaniu i produkcji oraz mogą być trudne w implementacji, ponieważ:

- wymagają skomplikowanych płytek PCB dla doprowadzenia wielu sygnałów do jednego niewielkiego układu scalonego,
- mogą wymagać bardzo wydajnego i precyzyjnego układu zasilania,
- mogą generować duże ilości ciepła,
- brak możliwości modyfikowania zasobów sprzętowych sprawia, że zmiana lub dodanie nawet jednego bloku wymaga wyprodukowania nowego układu scalonego.

Popularnym układem SoC jest ESP32 od Espressif. W rozbudowanej wersji zawiera dwurdzeniowy procesor Xtensa, pamięci RAM/ROM/Flash, blok komunikacji radiowej Wi-Fi/Bluetooth, akcelerator kryptograficzny, rdzeń ULP oraz cały szereg interfejsów I/O (**rysunek 1**). Niski koszt tego układu oraz łatwość implementacji, dzięki bogatym zbiorom przykładów, bibliotek i tutoriali sprawiły, że jest on jednym z najczęściej stosowanych układów w aplikacjach IoT.

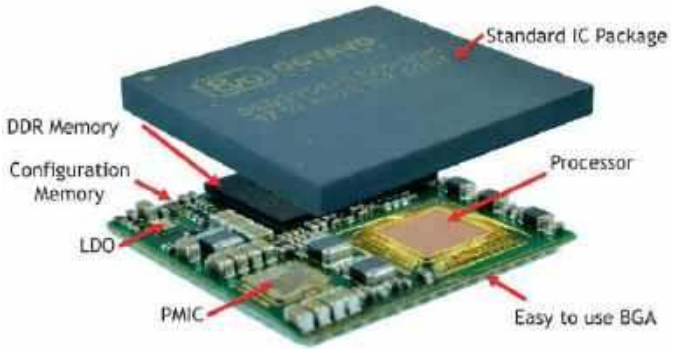
W kontekście układów SoC należy wyjaśnić również pojęcie **ASIC** (*Application Specific Integrated Circuit*). Układy scalone tej klasy są zaprojektowane specjalnie do jednego, konkretnego zastosowania, które wykonują bardzo wydajnie. Elementem układu SoC często jest struktura ASIC realizująca np. funkcje akceleratora AI/NPU czy kalkulatora sum kontrolnych SHA.

SiP (*System in Package*)

Moduł SiP łączy różnorodne komponenty – procesory, pamięci, moduły RF, moduły zarządzania energią, czujniki i dyskretne elementy pasywne – w jedną, kompaktową jednostkę (**rysunek 2**). Poszczególne bloki mogą być wykonane w różnych technologiach i rozmieszczone zarówno w płaszczyźnie 2D, jak i jako struktura 3D (tzw. 3D stacking) – wtedy uzyskuje się większą gęstość upakowania. Połączenia wykonywane są różnymi technikami, m.in. wire bonding, flip-chip albo za pomocą ich kombinacji.

Interesującym układem SiP jest procesor Apple M1, który zawiera zaawansowany i super wydajny układ SoC (8-rdzeniowy CPU, 8-rdzeniowy GPU, 16-rdzeniowy silnik neuronowy i kontroler interfejsu Thunderbolt) połączony z pamięciami LPDDR4X SDRAM o pojemności 8/16 GB (**fotografia 1**). Układ ten jest jednostką centralną niektórych komputerów MacBook.

W porównaniu do układów SoC, SiP wyróżniają się dużą elastycznością oraz krótkim cyklem projektowania i relatywnie niskim kosztem rozwoju. Produkcja gigantycznych, monolitycznych



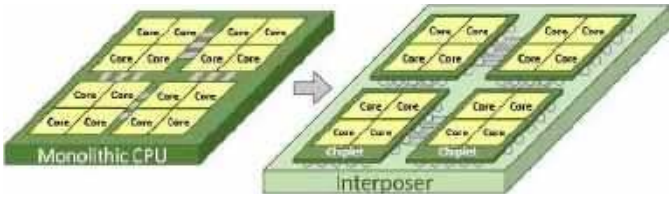
Rysunek 2. Budowa układu SiP (https://elektronikab2b.pl/biznes/53134-przyszlosc-rynku-modulow-sip)

Fotografia 1. Zaawansowany układ SiP typu M1 od Apple (https://en.wikipedia.org/wiki/Apple_M1)

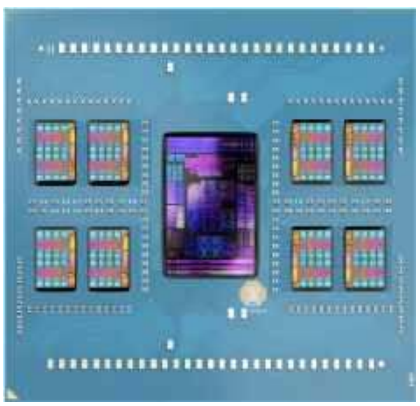
struktur półprzewodnikowych typu SoC w technologii 2…3 nm jest niesamowicie skomplikowana i obarczona dużym ryzykiem błędów. Łatwiej jest zbudować kilka mniejszych bloków i połączyć je w jednej obudowie. Dodatkowo SiP pozwala na integrację nowoczesnych układów mieszanych – cyfrowych i analogowych – w ich optymalnie skonfigurowanych, starszych strukturach. Możliwe jest również łączenie różnych materiałów półprzewodnikowych – Si, GaAs, GaN lub integracja układów MEMS, elementów optycznych i różnych czujników. Natomiast układy SiP ustępują SoC pod względem energooszczędności i w niewielkim stopniu także pod względem wydajności.

MCM (*Multi-Chip Module*)

Technologią podobną do SiP jest MCM. W tym przypadku mamy do czynienia z układem, który składa się z kilku oddzielnych struktur scalonych (tzw. chipletów – **rysunek 3**). Chiplety są projektowane



Rysunek 3. Porównanie struktur układów SoC i MCM (bazującej na chipletach) (https://tasmayshah12.medium.com/the-hidden-wiring-challenge-why-connecting-chiplets-is-becoming-techs-next--big-problem-4548d4d3f232)



Fotografia 2. Procesor AMD EPYC Bergamo, wykonany z użyciem chipletów, który ma aż 128 rdzeni (https://wccftech.com/amd-epyc-bergamo-cpu-die-detailed-16-zen-4c-vindhya-cores-per-ccd-35-percent-smaller-core-area/)

jako komponenty większego układu scalonego lub układy SoC i mogą być dowolnie dobierane. Podział na mniejsze, niezależne jednostki przekłada się na większą elastyczność, wydajność i skalowalność. Chiplety są połączone za pomocą interposera – krzemowego bloku połączeń, który odgrywa kluczową rolę w utrzymaniu wysokiej integralności sygnałów i zmniejszeniu opóźnień. Ta struktura zwiększa wydajność i energooszczędność systemów bazujących na chipletach oraz umożliwia efektywne współdzielenie zasobów. Technologia MCM utorowała drogę dla SiP, a w ostatnim czasie przeżywa swój renesans w najpotężniejszych procesorach. Na **fotografii 2** został pokazany procesor AMD EPYC Bergamo, wykonany z użyciem technologii chipletów i oferujący aż 128 rdzeni.

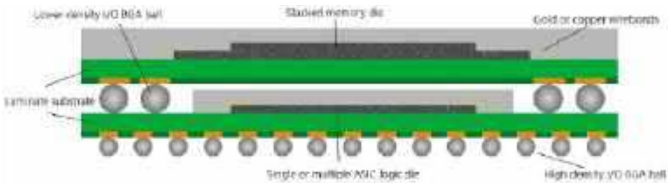
PoP (*Package-on-Package*)

Istnieje jeszcze jedna technologia ściśle związana z SoC i SiP. *Package-on-Package* to sprytne rozwiązanie konstrukcyjne, które pozwala zaoszczędzić miejsce poprzez układanie jednego gotowego układu scalonego na drugim. W branży smartfonów i nowoczesnych SBC jest to najczęstszy sposób łączenia procesora SoC z pamięcią RAM (**rysunek 4**) i pozwala na wyższe taktowanie pamięci. Zasadniczą wadą tego rozwiązania jest utrudnione odprowadzanie ciepła. Grzejący się układ SoC jest osłonięty układem pamięci, co skutecznie pogarsza efektywność jego chłodzenia. Niektóre procesory do Raspberry Pi korzystały właśnie z technologii PoP – **fotografia 3**.

Producenci SoC/SiP

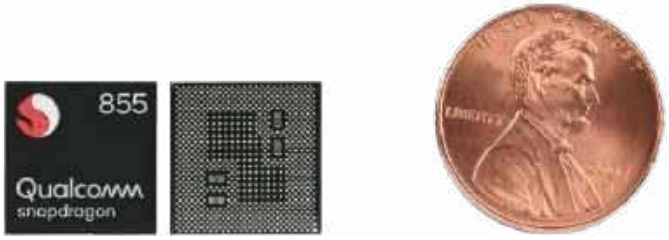
Najwięksi producenci SoC/SiP koncentrują się na produkcji układów do smartfonów, komputerów przenośnych i zaawansowanej elektroniki motoryzacyjnej. Do takich zastosowań wymagana jest przede wszystkim wysoka wydajność oraz integracja akceleratorów graficznych i jednostek AI/NPU. Liderami w branży są:

- **Apple** – układy z serii M i A. Apple jest pionierem w branży SoC i zrewolucjonizował rynek laptopów oferując układy, które osiągają wydajność komputerów desktopowych, zużywając zarazem wielokrotnie mniej energii. Niedawno



Rysunek 4. Sposób montażu układów w technologii Package-on--Package (https://www.pcbcart.com/assembly-capability/package--on-package-assembly.html)

Fotografia 3. Procesor BCM2835 na płytce Raspberry Pi, wyposażony w pamięć SDRAM zamontowaną w technologii PoP (https://de.wikipedia.org/wiki/Package-on-Package)

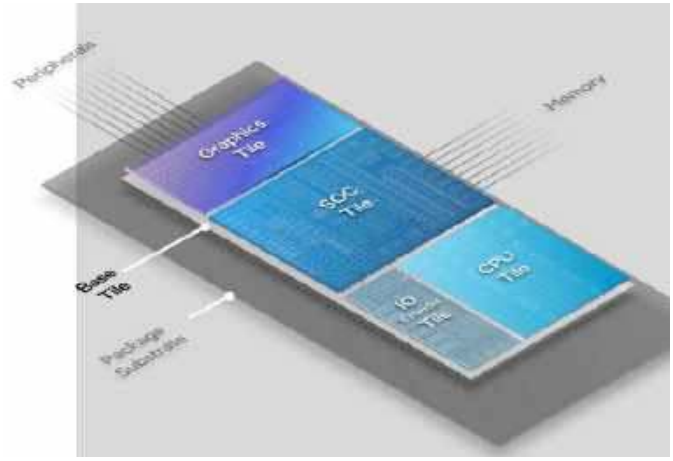


Fotografia 4. Miniaturowy układ SoC Qualcomm Snapdragon 855, który zapewnia wydajność nawet do 100 TOPS (https://mobiili.fi/2018/12/06/qualcomm-paljasti-snapdragon-855n-yksityiskohdat-android-huippupuhelimiin-jopa-45-prosenttia-lisaa-suorituskykya/)

Apple zaprezentowało nową generację układów – M5 Pro i M5 Max, które po raz pierwszy bazują na technologii o nazwie Fusion Architecture, pozwalającej na połączenie dwóch oddzielnych matryc (dies) w jeden wspólny system SoC przy użyciu zaawansowanych technologii produkcyjnych. Dzięki temu układy te oferują do 18 rdzeni CPU (w tym nowe super rdzenie) i do 40 rdzeni GPU, zachowując zunifikowaną architekturę pamięci o przepustowości do 614 GB/s.

- **Qualcomm** – układy Snapdragon napędzają większość urządzeń z systemem Android. Są wyposażone w wielordzeniowe CPU oraz zaawansowany silnik AI typu Hexagon o wydajności nawet do 100 TOPS (bilion operacji na sekundę) – patrz **fotografia 4**. Natomiast w tym roku zaprezentowano układy Snapdragon X2 Elite/Plus przeznaczone do komputerów przenośnych z systemem Windows, które dorównują tradycyjnym procesorom x86 lub je przewyższają.
- **NVIDIA** – układy Tegra/Drive/Thor. Marka jest kojarzona przede wszystkim z procesorami do kart graficznych, jednak produkuje również najbardziej zaawansowane SoC dla robotyki i autonomicznych samochodów. Najnowsze układy z serii Thor oferują potężną moc obliczeniową do 2000 TFLOPS i są przeznaczone do pojazdów, gdzie będą realizowały zarówno funkcje jazdy autonomicznej, jak i cały system Infotainment (**fotografia 5**).
- **MediaTek** – układy Dimensity to SoC zoptymalizowane do flagowych smartfonów. Producent przyjął architekturę All Big Core (brak małych rdzeni o niskiej wydajności), ponadto integruje w swoich układach jednostki wspomagające generowanie obrazów AI, autorskie akceleratory NPU oraz modemy 5G.

Fotografia 5. Moduł z układem SoC Nvidia Thor. Na płytce widać niezwykle rozbudowany blok zasilania, ponieważ układ Thor może pobierać moc nawet 130 W (https://designer.antmicro.com/library/devices/nvidia-900-13834-0080-000)



Rysunek 5. Budowa układów firmy Intel w technologii Tile-Based Design (odpowiednik MCM) – https://www.komputerswiat.pl/komputery-i-laptopy/laptopy/rewolucja-w-swiecie-komputerow-test-procesora-intel-core-ultra-7-155h/ldd134x

- **Intel** – układy SoC z serii Core Ultra. Intel dokonał ogromnej transformacji, przechodząc z klasycznych procesorów na układy typu SoC. Opracował technologię Tile-Based Design (odpowiednik MCM), w której różne bloki układu mają swoje osobne struktury krzemowe – tzw. kafelki (Tiles). Kafelki są ułożone obok siebie na wspólnej krzemowej tafli (Base Tile), realizującej matrycę połączeń (**rysunek 5**). Układy Core Ultra, oprócz rdzeni CPU i GPU, zawierają silnik NPU, tory radiowe obsługujące łączność Wi-Fi 6 i 7 oraz kontrolery nowoczesnych interfejsów PCI-Express 5.0, Thunderbolt 4 i USB4.

Przemysłowe SoC/SiP

Liderzy rynku przemysłowego projektują układy do zastosowań w komputerach SoM i SBC, czy też urządzeniach IoT, gdzie ważniejsze od wydajności są: niezawodność układów, odporność na temperaturę i zakłócenia, bezpieczeństwo danych oraz długi cykl życia produktu. Oto najważniejsi producenci rozwiązań z tej klasy.

NXP Semiconductors

Charakterystyka rodziny układów i.MX od NXP to droga ewolucji od klasycznych mikrokontrolerów do potężnych procesorów aplikacyjnych z akceleracją AI. Oto główne grupy układów.

- **i.MX RT** – nie są typowymi procesorami SoC, lecz mikrokontrolerami typu Crossover, czyli nowoczesnymi układami łączącymi cechy tradycyjnych MCU (prostota obsługi, niski pobór energii, krótki czas reakcji, łatwość programowania, niski koszt) z wysoką wydajnością procesorów aplikacyjnych MPU (taktowanie rzędu 600 MHz…1 GHz, rdzeń Cortex-M7). Aby uzyskać taką specyfikę układu, zamiast zintegrowanej pamięci Flash, która ogranicza prędkość działania, zastosowano interfejsy zewnętrznej pamięci Flash oraz ogromną ilość (kilka MB) zintegrowanej, szybkiej pamięci RAM (SRAM).
  Układy RT są przeznaczone do aplikacji Real-time audio, do prostych interfejsów graficznych, do układów sterowania silnikami itp. Są oferowane w 4 wersjach:
  – jedno-rdzeniowe MCU – RT101x…RT106x (Cortex-M7);
  – klasyczne MCU 2-rdzeniowe – RT116x…RT118x (Cortex-M7, Cortex-M33);
  – nowoczesne MCU z ogromną ilością pamięci RAM (5 MB) oraz dodatkowym zaawansowanym, konfigurowalnym rdzeniem Cadence Tensilica – RT500, RT600 (Cortex-M33, Cadence Tensilica);

Rysunek 6. Struktura blokowa procesora SoC typu i.MX 95 od NXP (https://www.nxp.com/products/i.MX95)

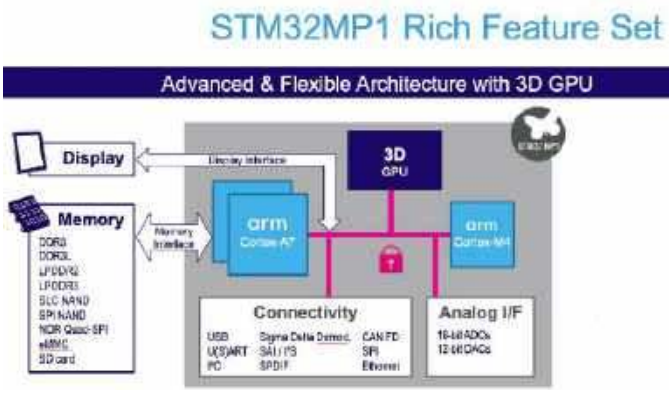
– podwójny zestaw MCU + Cadence Tensilica oraz 7,5 MB pamięci RAM i silnik AI/ML eIQ Neutron NPU – RT700 (Cortex-M33 + Cadence Tensilica Hi-Fi 4; Cortex-M33 + Cadence Tensilica Hi-Fi 1).

- **i.MX 6** – podstawowe procesory aplikacyjne, które zbudowały potęgę NXP w branży przemysłowej. Dostępne z wersjach z 1, 2 lub 4 rdzeniami Cortex-A7/Cortex-A9, akceleratorem grafiki 2D/3D (Vivante GPU), pojedynczym lub podwójnym interfejsem Ethernet 1 Gb, interfejsem PCIe oraz w wersji dla branży automotive. Są przystosowane do warunków przemysłowych i odpowiednie do pracy w reżimie 24/7. Modele o mniejszej wydajności, obniżonym poborze energii i niskiej cenie to m.in.: 6ULZ, 6ULL, 6UltraLite, 6SLL, 6Solo, 6SoloLite. Modele o większej wydajności z rdzeniami dual-core i quad-core to: 6SoloX, 6DualLite, 6Dual, 6DualPlus, 6Quad, 6QuadPlus.
- **i.MX 7** – charakteryzują się heterogeniczną architekturą, łączącą wydajny rdzeń Cortex-A7, na którym może działać system Linux, z energooszczędnym rdzeniem Cortex-M4 do mniej wymagających zadań. Dodatkowo układy i.MX 7 są wyposażone w zaawansowane moduły bezpieczeństwa oraz w interfejs wyświetlacza MIPI/równoległy/EPD, dlatego doskonale nadają się do urządzeń przenośnych, zasilanych bateryjnie i zapewniających bezpieczeństwo w świecie IoT. Model przeznaczony do aplikacji ultra low power to 7ULP, model zrównoważony to 7Solo, natomiast model o wysokiej wydajności to 7Dual.
- **i.MX 8** – oferują ogromny skok wydajnościowy dzięki przejściu na architekturę 64-bitową i wielordzeniową, zawierającą jednostki Cortex-A72/A53/A35, Cortex-M4F/M33/M7, DSP/NPU/GPU, w różnych konfiguracjach. Oferują wirtualizację sprzętową, czyli możliwość uruchomienia dwóch systemów (np. Android i RTOS) na jednym procesorze, w całkowitej izolacji pomiędzy obydwoma systemami. Ponadto obsługują wyświetlacze do 4K, kamery oraz kodeki obrazu i dźwięku. Przeznaczone są do zaawansowanych zastosowań graficznych, wizji maszynowej, sterowania głosowego, analizy wideo i systemów nadzorowania bezpieczeństwa. Modele o mniejszej wydajności to 8XLite, 8X, 8ULP, modele o dużej wydajności to 8M Plus, 8M Nano, 8M Mini, 8M, zaś najbardziej wydajny przedstawiciel tej rodziny to i.MX 8 (2×A72 + 4×A53 + 2×M4F + DSP + 2×GPU).
- **i.MX 9** – najnowsza generacja układów i.MX przeznaczona do aplikacji Edge AI i Edge Lock. Wprowadzono nowoczesne jednostki przetwarzania neuronowego NPU typu Ethos-U, dzięki czemu takie funkcje, jak rozpoznawanie głosu czy gestów odbywa się lokalnie przy minimalnym zużyciu energii. Wewnątrz układu znajduje się wydzielona, sprzętowa twierdza (*Secure Enclave*), która zarządza funkcjami bezpieczeństwa i kryptograficznymi. Ponadto zastosowano technologię Energy Flex odpowiadającą za precyzyjne zarządzanie energią – kontroler może wyłączyć niemal wszystkie bloki i pozostawić aktywny tylko jeden sensor. Najbardziej podstawowy model to 91, wyposażony w jeden rdzeń Cortex-A55. Modele 93, 94, 95 i 952 to wydajne, wielordzeniowe układy z interfejsami wyświetlaczy, kamer i PCIe (**rysunek 6**).

ST Microelectronics

ST Microelectronics ma w ofercie dwa rodzaje popularnych układów SoC. Pierwszy z nich stanowią rozbudowane mikrokontrolery STM32MP1 i STM32MP2, druga grupa obejmuje mikrokontrolery zintegrowane z uniwersalnym torem radiowym 2,4 GHz – STM32WB.

- **STM32MP1** – układy, które umożliwiły przejście mikrokontrolerów do świata systemów operacyjnych typu Linux. Firma ST Microelectronics nie próbowała konkurować z procesorami do smartfonów, zamiast tego opracowała rozbudowane, niezawodne i energooszczędne mikrokontrolery z solidnym wsparciem programowym. Pierwsze modele (MP131, MP133, MP135) dysponują jednym rdzeniem Cortex-A7 o taktowaniu do 1 GHz. Kolejne układy (MP151, MP153, MP157) mają 1 lub 2 rdzenie Cortex-A7 oraz rdzeń Cortex-M4, a najlepiej wyposażona wersja MP157 zawiera dodatkowo silnik graficzny 3D OpenGL ES 2.0 (**rysunek 7**).
- **STM32MP2** – druga generacja procesorów aplikacyjnych otwiera drzwi do wyższej wydajności dzięki platformie 64-bitowej i nowoczesnym rdzeniom Cortex-A35/Cortex-M33. Dodatkowo, dzięki akceleratorowi NPU wbudowanemu w procesory MP25x i MP23x, a także za sprawą ekosystemu ST Edge



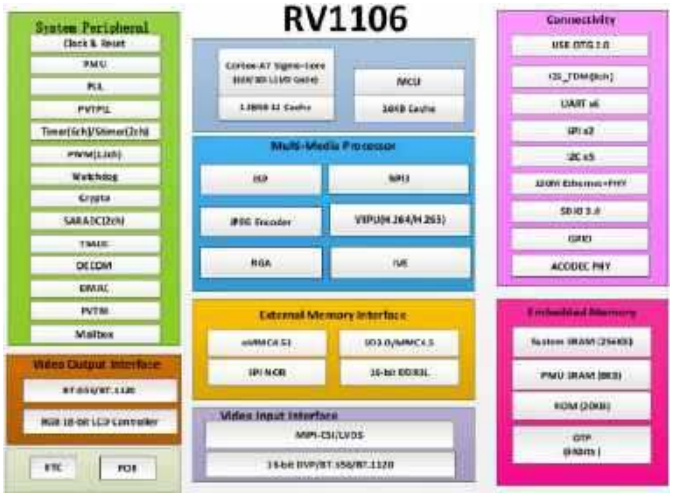
Rysunek 7. Struktura blokowa układów STM32MP1 (https://embeddedcomputing.com/technology/processing/stmicroelectronics-releases-its-stm32mp1-microprocessor-series)

Rysunek 8. Struktura blokowa układów STM32WB (https://ep.com.pl/rynek/temat-miesiaca/14912-od-mikrokontrolerow-do-ukladow-radiowych-bluetooth-z-ukladami-stm32wb)

AI, można łatwo wybierać, trenować i optymalizować aplikacje AI. Układy wyposażone są także w zaawansowane, certyfikowane funkcje bezpieczeństwa.

- **STM32WB** – układy z tej rodziny bazują na rdzeniu Cortex-M4, który działa jako procesor aplikacji oraz na drugim rdzeniu Cortex-M0+, który realizuje zadania związane z komunikacją radiową w paśmie 2,4 GHz (**rysunek 8**). Zapewniają obsługę technologii Bluetooth LE zgodnej ze specyfikacją Bluetooth Core 5.4, a także standardów: IEEE 802.15.4 ZigBee, Thread i innych współbieżnych standardów bezprzewodowych. Dodatkowo układy STM32WB zawierają szereg standardowych zasobów: pamięć Flash do 1 MB, liczniki, interfejsy komunikacyjne, zasoby analogowe, peryferia interfejsu użytkownika oraz bloki funkcjonalne zwiększające bezpieczeństwo aplikacji.

Fotografia 6. Komputer SBC typu ROCK 4C+ zbudowany na bazie układu SoC Rockchip RK3399 (https://www.keyestudio.com/products/rock-4-model-c-4gb-single-board-computer-rockchip-rk3399-t-arm-cortex-a72)

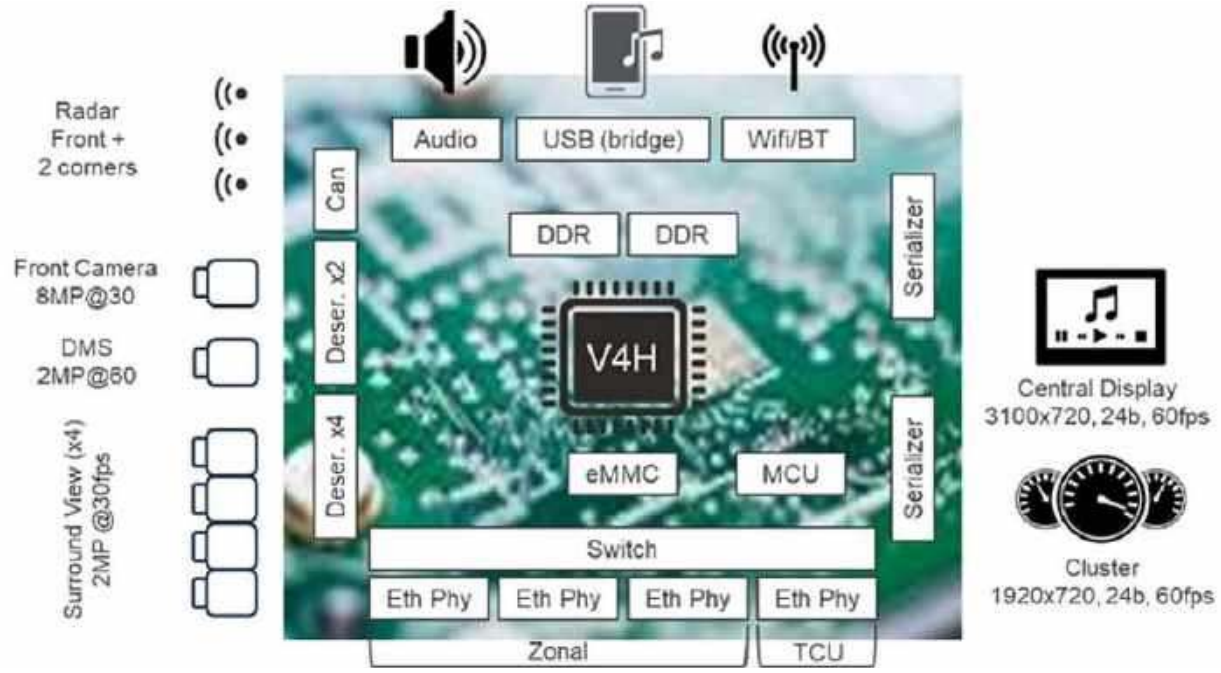


Rysunek 9. Struktura blokowa układu RV1106 (https://www.scensmart.com/general-description-of-soc/rockchip-rv1106-soc-for-pic-ai/)

Rockchip

Układy Rockchip w ostatnich latach stały się bazą dla najwydajniejszych komputerów jednopłytkowych (SBC) i zaawansowanych urządzeń IoT. NXP czy ST stawiają na certyfikacje i stabilność przemysłową, podczas gdy firma Rockchip postawiła na dużą moc obliczeniową i multimedia.

- **RK3399** – to wydajny procesor SoC zbudowany w architekturze sześciordzeniowej Big.LITTLE – 2×Cortex-A72 + 4×Cortex-A53. Jest on wyjątkowo popularny w świecie komputerów jednopłytkowych SBC, takich jak Pine64 czy Rock 4C (**fotografia 6**), ze względu na świetny stosunek ceny do możliwości. Oferuje układ graficzny Mali-T860 MP4 ze wsparciem dla 4K/60 fps, USB-C z DisplayPort, szybkie interfejsy PCIe i jest wspierany przez niemal każdą dystrybucję Linuksa na ARM.
- **RK3566/RK3568** – układy o średniej wydajności, ale nowoczesne i energooszczędne. Zastąpiły starsze jednostki w tanich tabletach, TV Boxach i budżetowych SBC (np. Orange Pi 3B). Oferują cztery rdzenie Cortex-A55 oraz prostą jednostkę NPU (ok. 1 TOPS), a także szeroką gamę interfejsów – SATA, PCIe 3.0, Dual Gigabit Ethernet, co czyni je idealnymi bazami dla tanich serwerów domowych (NAS) i routerów.
- **RK3588/RK3588S** – to flagowe układy SoC nowej generacji, wykonane w procesie technologicznym 8 nm i przeznaczone do zaawansowanych zastosowań w AI, Edge IoT oraz do złożonego przetwarzania danych. Układy te konkurują z procesorami Intela i Qualcomma w świecie systemów embedded. Ośmiordzeniowa architektura big.LITTLE składa się z 4 wydajnych rdzeni Cortex-A76 (2,4 GHz) oraz 4 energooszczędnych rdzeni Cortex-A55 (1,8 GHz). Zintegrowany układ graficzny Mali-G610 MP4 wspiera zaawansowane renderowanie 3D, wymagające interfejsy graficzne – 8K/60 fps oraz możliwość podłączenia do 4 wyświetlaczy jednocześnie. Całość uzupełnia wbudowany akcelerator AI o wydajności 6 TOPS, wspierający operacje mieszane (INT4/INT8/INT16/FP16) i popularne frameworki, takie jak TensorFlow, PyTorch czy Caffe.
- RV1103/RV1106 – to wysoce zintegrowany procesor SiP z serii AI Vision, zaprojektowany z myślą o urządzeniach IoT, inteligentnych kamerach IP oraz systemach brzegowych wymagających wsparcia dla sztucznej inteligencji. Zawiera jednordzeniowy procesor Cortex-A7 taktowany zegarem 1,2 GHz, zintegrowaną pamięć RAM DDR3L 128/256 MB oraz sprzętowy blok przetwarzania obrazu ISP 3, obsługujący wejście wideo do 5 MP/30 fps. Wspiera technologie HDR, WDR, 2D/3D noise reduction oraz funkcje korekcji obrazu (np. defogging, fisheye correction). Umożliwia sprzętowe kodowanie w formatach



Rysunek 10. Zasoby sprzętowe układu V4H od Renesas (https://www.renesas.com/en/blogs/exploring-entry-fusion-application-architecture-and-cost-effective-solution-utilizing-r-car-v4h?srsltid=AfmBOop_zsvMCSVPGKWPVYES5Kr9hcnT-SB8FkSCd7qQsDiuqgN5Vq4a)

H.264 i H.265 (do 5 MP/30 fps) oraz snapshoty JPEG do 16 MPx. Charakterystyczne cechy tego mikrosystemu to bardzo krótki czas startu – Fast Boot, możliwość przechwycenia obrazu w 250 ms i rozpoznawania twarzy w mniej niż 1 sekundę.

Renesas

Renesas to japoński gigant, który wyspecjalizował się w produkcji układów SoC dla branży automotive. Układy Renesas są fundamentem systemów wspomagania kierowcy (ADAS) oraz krytycznej infrastruktury przemysłowej.

- **Seria R-Car** (V4M/V4H) – układy zaprojektowane tak, aby zarządzały zarówno systemem rozrywki (Infotainment), jak i systemami bezpieczeństwa (ADAS) oraz jazdy autonomicznej na poziomach 2+ i 3 (**rysunek 10**). To absolutna czołówka procesorów w świecie elektroniki dla motoryzacji, wyposażonych w potężne jednostki Cortex-A76/A55, rdzenie czasu rzeczywistego Cortex-R52 i dedykowane akceleratory deep learning. Zintegrowany procesor graficzny AXM-8-256 osiąga wydajność ponad 150 GFLOPS, a procesor sygnałowy obrazu (ISP) obsługuje kamery o wysokiej rozdzielczości – do 8 MP.
- **Seria RZ/G** – układy z grupy Mainstream, stanowiące bezpośrednią konkurencję dla i.MX od NXP czy STM32MP1. Są to procesory aplikacyjne przeznaczone do paneli HMI i rozwiązań IoT. Wyposażone w rdzenie GPU Mali-G31, oferują świetny balans między estetyką interfejsu a niskim poborem prądu.
- **Seria RZ/V** – najbardziej innowacyjna grupa układów Renesas, która wprowadza autorską technologię akceleracji sztucznej inteligencji – DRP-AI (Dynamically Reconfigurable Processor). To unikalne podejście stanowi połączenie tradycyjnego procesora z układem FPGA. DRP-AI potrafi skonfigurować swoje bloki logiczne w locie, aby idealnie dopasować się do konkretnego algorytmu sieci neuronowej. W efekcie uzyskiwana jest ekstremalnie wysoka wydajność AI na każdy wat pobieranej energii. Rodzina RZ/V doskonale nadaje się do aplikacji wymagających wizji 3D i rozpoznawania obiektów (**fotografia 7**).
- **Seria RZ/N i RZ/T** – układy przeznaczone do sterowników PLC i robotyki, gdzie liczy się każda mikrosekunda opóźnienia (**rysunek 11**). Architektura bazuje na rdzeniach Cortex-R, które gwarantują przewidywalny czas odpowiedzi systemu. Ponadto układy oferują sprzętową obsługę zaawansowanych protokołów przemysłowych (EtherCAT, PROFINET, EtherNet/IP). Nowsze jednostki, jak RZ/N2L, wspierają technologię Time-Sensitive Networking (TSN), niezbędną w nowoczesnych fabrykach Przemysłu 4.0.

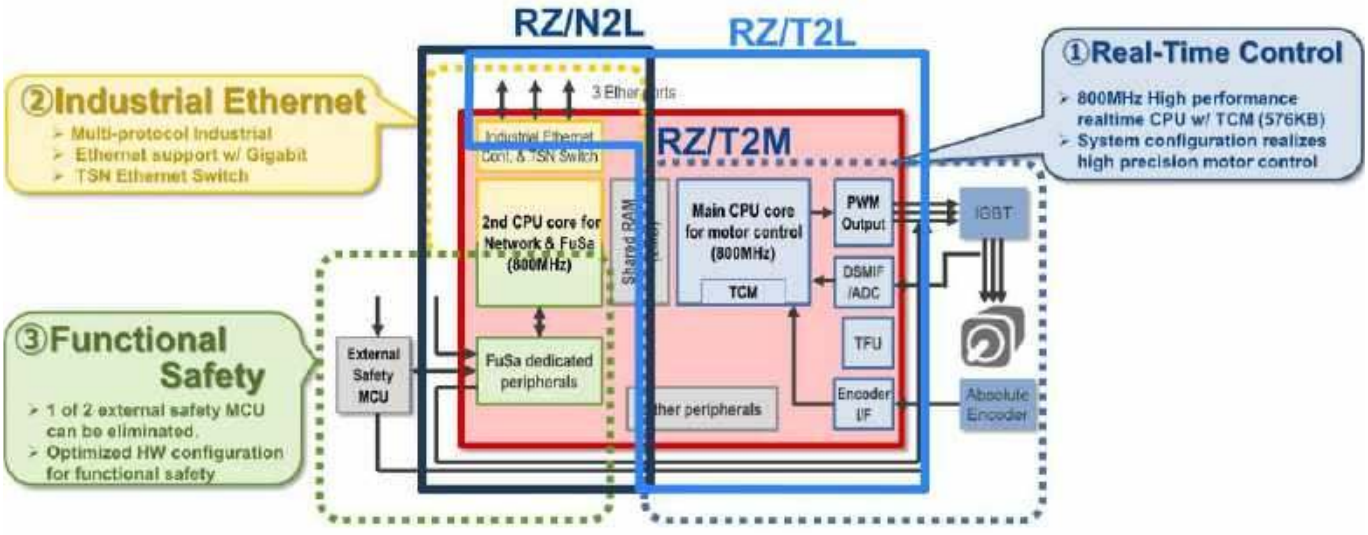
Fotografia 7. Płytka uruchomieniowa z układem RZ/V2H do testowania aplikacji typu 3D vision (https://deepvisionconsulting.com/a-realtime-3d-application-on-the-renesas-rz-v2h/)

Moduły SoM

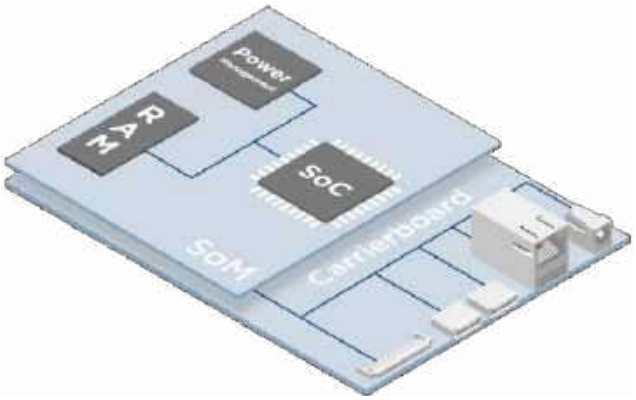
Moduły SoC/SiP mają wiele zalet, ale mogą też sprawić wiele trudności:

- często wymagają zewnętrznej pamięci Flash lub dodatkowej szybkiej pamięci RAM,
- do stabilnej pracy potrzebują precyzyjnego i wydajnego układu zasilania,
- niektóre interfejsy, w tym Ethernet, muszą być połączone z zewnętrznym układem szybkiego transceivera, np. Ethernet PHY,
- interfejs bezprzewodowy wymaga implementacji skomplikowanych obwodów antenowych lub kompletnego modułu radiowego.

W efekcie, skoncentrowane w układzie SoC nowoczesne funkcjonalności i tak wymagają zaprojektowania złożonych obwodów współpracujących. Moduły SoM (*System on Module*) powstały po to, aby rozwiązać ten problem.



Rysunek 11. Typowa aplikacja układów Serii RZ/N i RZ/T (https://www.redeweb.com/is/li%C3%B0veisla/notkun-rz-t2l-ethercat-serv%C3%B3-m%C3%B3torsins/)



Rysunek 12. Idea modułów SoM (https://www.baslerweb.com/it-it/learning/embedded-processing-platforms/)

SoM to niewielka płytka drukowana, która integruje w sobie najbardziej skomplikowane w implementacji elementy systemu wbudowanego: procesor SoC, pamięć RAM, pamięć NVM – Flash/eMMC, układ zarządzania zasilaniem – PMIC, układy interfejsów przewodowych i bezprzewodowych. Czasami określana jako CoM (Computer on Module), jednak w przeciwieństwie do gotowych komputerów SBC, moduł SoM przeważnie nie zawiera złączy, np. USB, HDMI, Ethernet, dostępnych bezpośrednio dla użytkownika (rysunek 12). Zamiast tego ma wielostykowe złącza (zwykle krawędziowe lub typu Mezzanine – przyp. red.), które wyprowadzają wszystkie kluczowe sygnały na zewnątrz. Zalety modułów SoM to przede wszystkim:

- **skalowalność** – można zaprojektować jedną płytę bazową i w zależności od budżetu lub wymagań projektu, dołączyć do niej moduł z 1-rdzeniowym lub 8-rdzeniowym procesorem;
- **szybkość projektowania** – wszystkie krytyczne połączenia, takie jak szybkie interfejsy i szeroka magistrala pamięci, są już wykonane i przetestowane. Płytka bazowa jest zatem niezbyt rozbudowana i łatwa w projektowaniu;
- **łatwość programowania** – producenci modułów SoM udostępniają skonfigurowane i gotowe do użycia systemy operacyjne oraz pakiety oprogramowania BSP (Board Support Package), biblioteki, frameworki, przykłady programów;
- **długowieczność** – gdy procesor stanie się przestarzały lub któryś element ulegnie uszkodzeniu, wystarczy wymienić niewielki moduł SoM. Cała płyta bazowa ze specjalistycznymi złączami i układami wykonawczymi nie musi być nawet demontowana na czas serwisu;
- **niezawodność** – moduły SoM są zwykle testowane i/lub certyfikowane, co gwarantuje wysoką niezawodność i wydajność produktów końcowych. Może to mieć kluczowe znaczenie w przypadku zastosowań w urządzeniach medycznych, systemach motoryzacyjnych i automatyce przemysłowej.

Podział modułów CoM

Moduły CoM to przede wszystkim rozbudowane i zaawansowane minikomputery, które zwykle są dostosowane do jednego z kilku otwartych standardów. Dzięki temu istnieje możliwość wymiany modułu na wyższy model lub na produkt innej marki. Moduły CoM najczęściej produkowane są w jednym z 3 standardów.

SMARC (*Smart Mobility ARChitecture*)

Obecnie najpopularniejszy standard kompaktowych, energooszczędnych komputerów modułowych CoM z procesorami ARM i x86. Główne cechy standardu SMARC:

- stosowany przez wielu producentów,
- dwa zdefiniowane rozmiary: 82×50 mm oraz 82×80 mm,
- zdefiniowane rozmieszczenie punktów mocowania,
- złącze krawędziowe 314-pinowe o rastrze 0,5 mm,
- obsługa procesorów ARM oraz x86,
- obsługa systemów o niskim poborze mocy, rzędu kilku watów.

Dzięki interfejsom graficznym do wyświetlaczy i kamer, dźwiękowym, sieciowym i komunikacyjnym (**rysunek 13**), moduły SMARC nadają się nie tylko do systemów mobilnych, ale także do platform multimedialnych, urządzeń IoT i wielu wymagających aplikacji o niskim poborze mocy.

Rysunek 13. Budowa modułów SoM w standardzie SMARC oraz wykaz interfejsów i sygnałów, które mogą być dostępne na złączu krawędziowym (https://www.module-store.de/de/smarc/)

Rysunek 14. Budowa modułów SoM w standardzie Qseven oraz wykaz interfejsów i sygnałów, które mogą być dostępne na złączu krawędziowym (https://www.congatec.com/en/technologies/qseven/)

Qseven

Otwarty standard komputerów modułowych CoM, przeznaczony do systemów wbudowanych o niskim poborze mocy i niewielkich wymiarach (**rysunek 14**). Główne cechy standardu Qseven to:

- kompaktowy rozmiar – moduły występują w dwóch formatach: standardowym 70×70 mm (stąd nazwa Q od quadratic i seven) oraz mniejszym µQseven o wymiarach 40×70 mm,
- niski pobór mocy – moduły są zoptymalizowane pod kątem chłodzenia pasywnego, a maksymalny współczynnik TDP zazwyczaj nie przekracza 12 W,
- złącze krawędziowe 230-pinowe, które eliminuje potrzebę stosowania drogich złączy typu board-to-board,
- obsługa wielu architektur – wspiera zarówno procesory x86, jak i architekturę Arm.

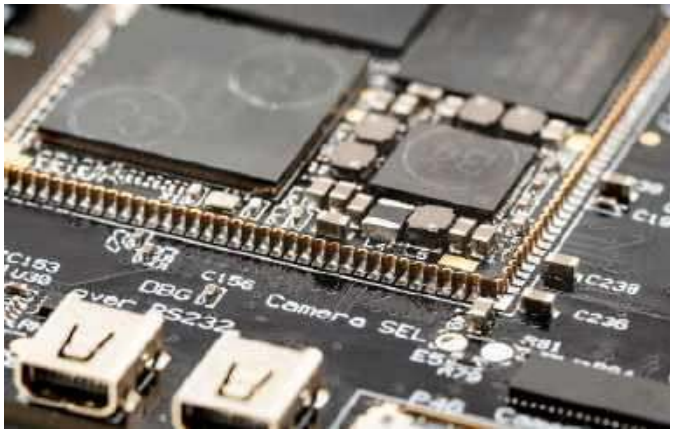
COM Express

Standard przemysłowy dla komputerów typu CoM. Wysoce zintegrowany, kompaktowy moduł obliczeniowy, wyposażony w jedno lub dwa niskoprofilowe, 220-stykowe złącza typu Board-to-Board umieszczone na spodzie płytki, które umożliwiają połączenie z płytą bazową (carrier board). Standard definiuje cztery główne rozmiary modułów (**rysunek 15**) oraz różne konfiguracje styków (Type). Jest zarezerwowany dla najbardziej wymagających zastosowań przeznaczonych do pracy w trudnych warunkach przemysłowych, medycznych i militarnych.

Podział modułów SoM

Moduły SoM są dostępne jako zaawansowane, miniaturowe płytki PCB, zwykle w formacie charakterystycznym dla danego producenta. Wymiana modułu jest możliwa, ale najczęściej tylko w obrębie jednej grupy produktów tego producenta. Dostępne są wtedy

Rysunek 15. Budowa modułów SoM w standardzie COM Express wraz z rozmieszczeniem złączy (https://en.wikipedia.org/wiki/COM_Express#/media/File:COM_Express_form_factor_comparison.jpg)



Fotografia 8. Lutowany moduł SoM zamontowany na płycie bazowej (https://www.compulab.com/blog/advantages-of-using-smt-solder-down-system-on-modules/)

wersje o różnym rodzaju i ilości pamięci, z różnymi wersjami procesora SoC, np. jedno- i wielordzeniowym.

Głównym zastosowaniem modułów SoM są systemy embedded oraz IoT, gdzie sprawdziły się 3 różne formaty:

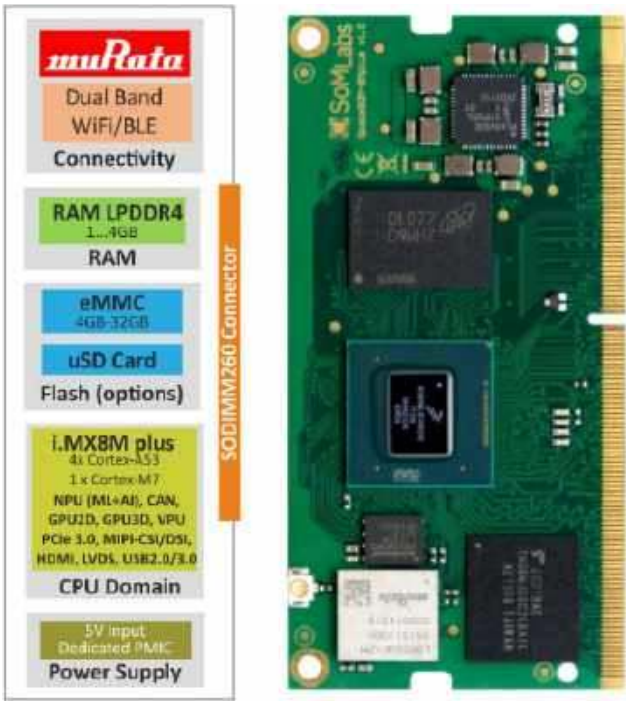
- **SODIMM Style** – zawiera złącze krawędziowe, przez co moduły wyglądają jak moduły pamięci RAM do laptopa. Bardzo popularne, łatwe w wymianie i konkurencyjne cenowo.
- **B2B** (*Board-to-Board*) – wyposażone w niskoprofilowe, wielostykowe złącza typu Mezzanine. Pozwalają na budowę bardzo kompaktowych systemów (np. Raspberry Pi Compute Module 4/5).
- **Solderable SoM** (LGA, QFN) – moduły, które wlutowuje się na stałe na płytę bazową (**fotografia 8**). Są najbardziej odporne na wstrząsy i wibracje, zajmują najmniej przestrzeni, ale są trudne w serwisowaniu (raczej nie przewiduje się możliwości ich wymiany).

Poniżej znajduje się lista wybranych producentów i najnowszych modeli modułów SoM.

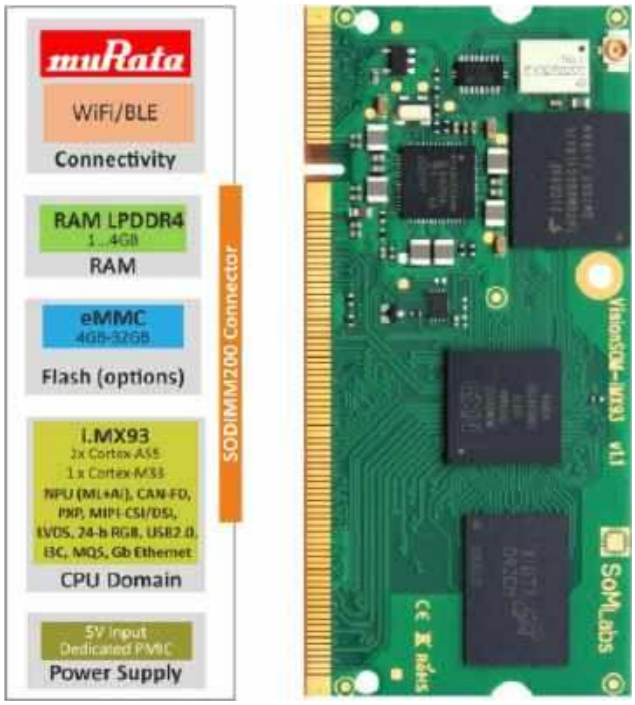
SomLabs

SoMLabs jest niezależną polską firmą skupiającą się na rozwoju i produkcji szerokiej gamy platform wbudowanych, takich jak System on Module (SoM) i Carrier Board (CB) dla projektów wbudowanych. Jest oficjalnym partnerem firm NXP, ST Microelectronics oraz Renesas i dlatego oferta obejmuje moduły z układami tych właśnie producentów.

Fotografia 9. Moduł StarSOM-STM32H757 typu Board-to-Board z procesorem STM32H757XI, zamontowany w płytce bazowej (https://somlabs.com/product/starsom-stm32h757-sls05-dual-core-arm-cortex-m7-cortex-m4/)



Rysunek 16. Moduł SpaceSOM-8Mplus z procesorem NXP i.MX8M Plus Quad (https://wiki.somlabs.com/index.php?title=SpaceSOM-8Mplus_Datasheet_and_Pinout)



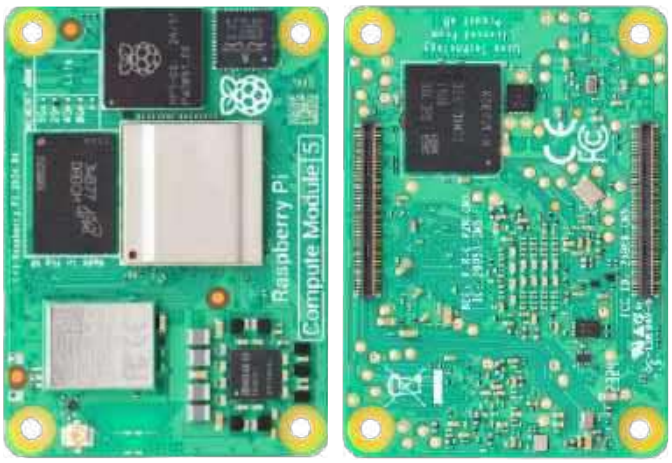
Rysunek 17. Moduł VisionSOM-iMX93 z nowym procesorem NXP i.MX9352 (https://wiki.somlabs.com/index.php?title=VisionSOM-iMX93_Datasheet_and_Pinout)

- **StarSOM-STM32H757** – moduł typu B2B z dwoma miniaturowymi złączami o 100 stykach każde (typu Hirose DF40C100DP04V51) – **fotografia 9**. Przeznaczony do aplikacji wymagających niskiego zużycia energii oraz funkcjonalności systemu czasu rzeczywistego. Zawiera dwurdzeniowy procesor SoC STM32H757XI (Cortex-M7 480 MHz + Cortex-M4 240 MHz), który jest połączony z pamięcią SDRAM 32 MB oraz pamięcią Flash QSPI 32 MB. Oferuje kompletny interfejs Ethernet 100 Mb, interfejs radiowy 802.11b/g/n Wi-Fi/Bluetooth 5.1, równoległy (24-bitowy) interfejs wyświetlacza oraz MIPI-DSI, akcelerator graficzny Chrom-ART GPU, zaawansowane funkcje bezpieczeństwa oraz szeroki wachlarz klasycznych interfejsów.
- **SpaceSOM-8Mplus** – moduł typu SODIMM z 260-stykowym złączem krawędziowym (**rysunek 16**). Zaprojektowany do aplikacji multimedialnych i AI klasy przemysłowej, wymagających wysokiej mocy obliczeniowej i działających na systemach Linux oraz Android. 5-rdzeniowy (4×Cortex-A53 1,8 GHz + Cortex-M7 800 MHz) procesor aplikacyjny SoC i.MX8M Plus Quad, ze zintegrowanym akceleratorem NPU, jest połączony z energooszczędną pamięcią RAM typu LPDDR4 o pojemności do 4 GB i szybką pamięcią eMMC o pojemności do 32 GB. Nowoczesny SoC oferuje interfejs komunikacyjny PCIe 3.0, interfejs USB 2.0/3.0, interfejs wyświetlacza HDMI/LVDS i MIPI-DSI, a na płytce znajduje się miejsce na opcjonalny moduł radiowy Murata obsługujący dwupasmowe Wi-Fi 2,4/5 GHz, 802.11a/b/g/n/ac oraz i Bluetooth 5.1.
- **VisionSOM-iMX93** – moduł typu SODIMM z 200-stykowym złączem krawędziowym (**rysunek 17**). Zawiera jeden z najnowszych procesorów SoC zaprojektowanych przez NXP – i.MX9352 (2×Cortex-A55 1,7 GHz + Cortex-M33 250 MHz), który jest zintegrowany z zaawansowaną jednostką przetwarzania grafiki 2D (PXP) i energooszczędnym koprocesorem AI/ML NPU (Ethos U-65 microNPU). Ma wszystkie standardowe, jak i nowocześniejsze interfejsy: CAN-FD, I3C, Ethernet 1 Gb MIPI-DSI, MIPI-CSI. Moduł jest przeznaczony do aplikacji IoT, Edge AI, interfejsów HMI i automatyki, gdzie wymagana jest energooszczędność i elastyczność przy zrównoważonych kosztach.

Raspberry Pi

W ofercie Raspberry Pi gotowym komputerom SBC od dawna towarzyszyły moduły typu SoM nazywane modułami obliczeniowymi – Compute Module (CM). Są to warianty flagowych komputerów jednopłytkowych Raspberry Pi przeznaczone do zastosowań przemysłowych i komercyjnych. Oprócz tego, że mają kompaktową konstrukcję, są wyposażone w pamięć NVM typu eMMC i dostępne w różnych wariantach.

- **RPi Compute Module 5 (CM5)** – moduł typu B2B z dwoma miniaturowymi złączami na spodzie płytki (**fotografia 10**). Jest wyposażony w 4-rdzeniowy, 64-bitowy procesor Cortex-A76 typu Broadcom BCM2712, taktowany z częstotliwością dochodzącą do 2,4 GHz, który zapewnia wysoką wydajność, zwłaszcza w aplikacjach multimedialnych. Zamontowana szybka pamięć RAM typu LPDDR4 może mieć pojemność od 2 do 16 GB (z obsługą korekcji błędów ECC), natomiast pamięć eMMC może mieć pojemność 0 (wersja Lite)/16/ 32/64 GB. W zakresie komunikacji CM5 oferuje interfejs Gigabit Ethernet oraz wbudowane Wi-Fi 6 i Bluetooth 5.2.



Fotografia 10. Moduł SoM Raspberry Pi Compute Module 5 (https://www.raspberrypi.com/news/compute-module-5-on-sale-now/)

Fotografia 11. Moduł RPi Compute Module 4S (CM4S) typu SO-DIMM ze złączem krawędziowym, zgodny z formatem DDR2 stosowanym we wcześniejszych wersjach: CM1, CM3 i CM3+ (https://www.raspberrypi.com/products/compute-module-4s/)

Fotografia 13. Moduł SoM SAMA5D27 od Microchip (https://www.microchip.com/en-us/product/atsama5d27-som1)

- **RPi Compute Module 4S (CM4S)** – moduł typu SODIMM ze złączem krawędziowym (**fotografia 11**), zgodny z formatem DDR2 stosowanym we wcześniejszym wersjach: CM1, CM3 i CM3+. Wyposażony w czterordzeniowy procesor Cortex A72 (1,5 GHz), do 8 GB pamięci LPDDR4-3200 SDRAM z ECC oraz do 32 GB pamięci eMMC. Moduł obsługuje szereg interfejsów, takich jak USB 2.0, HDMI 2.0 (do 4K przy 60 fps), MIPI DSI i CSI oarz umożliwia dekodowanie wideo 4K w standardach H.265 (HEVC) i H.264. Ponadto, dzięki 46 pinom GPIO, moduł oferuje duże możliwości możliwości rozbudowy, a zgodność z Raspberry Pi OS czyni go rozwiązaniem łatwym w uruchomieniu.

Microchip

Znany producent mikrokontrolerów skoncentrował się na produkcji modułów SoM typu *solderable*, czyli montowanych w płytach bazowych poprzez bezpośrednie lutowanie na docelowej PCB. Takie rozwiązanie ma pewne ograniczenia, ale jednocześnie jest nieporównywalnie kompaktowe (wlutowany moduł praktycznie nie jest wyższy od innych elementów na płytce bazowej) oraz najbardziej ekonomiczne i najłatwiejsze w produkcji seryjnej.

- **SAM9X75D2GN4** – bardzo kompaktowy moduł o wymiarach 35×30 mm ze stykami umieszczonymi na krawędziach płytki (174 piny, raster 0,65 mm), przeznaczonymi do lutowania maszynowego lub ręcznego (**fotografia 12**). Zawiera procesor SAM9X75 (ARM926EJ-S) o częstotliwości taktowania do 800 MHz, 256 MB pamięci DDR3L SDRAM oraz 512 MB pamięci NAND Flash. Komunikacja może być realizowana poprzez interfejs Ethernet 1 Gb oraz wiele klasycznych interfejsów i wyprowadzeń I/O. Zintegrowana jednostka zarządzania energią (Power Management Unit) dba o prawidłowe zasilanie komponentów. Seria modułów SOM SAM9X75 jest wspierana przez darmową dystrybucję systemu Linux oraz przykłady w języku C.
- **SAMA5D27** – bardzo kompaktowy moduł o wymiarach 40×38 mm ze stykami umieszczonymi na krawędziach płytki (176 pinów, raster 0,8 mm) przeznaczonymi do lutowania maszynowego lub ręcznego (**fotografia 13**). Zawiera procesor SAMA5D27 (Cortex-A5) o częstotliwości taktowania do 500 MHz, 128 MB pamięci DDR2 SDRAM oraz 8 MB pamięci QSPI Flash. Komunikacja może być realizowana poprzez interfejs Ethernet 100 Mb oraz wiele klasycznych interfejsów i wyprowadzeń I/O. Zintegrowana jednostka zarządzania energią typu MIC2800 (*Power Management Unit*) pozwala na elastyczne zarządzanie poborem energii.

Fotografia 12. Moduł SoM SAM9X75 od Microchip (https://www.microchip.com/en-us/product/sam9x75d2gn4)

Podsumowanie

Klasyczne procesory i mikrokontrolery to dziś w elektronice za mało. Wyraźnym kierunkiem rozwoju stały się technologie z zakresu AI i cyberbezpieczeństwa, co widać po analizie budowy najnowszych układów SoC. Wynika to z ciągłego udoskonalania i poszerzania funkcjonalności urządzeń, np. w zakresie rozpoznawania obrazów i dźwięków, a także z przesunięcia ciężaru przetwarzania danych z centralnej chmury na lokalne jednostki.

Aby nadążyć za tym postępem, trzeba być gotowym na zmiany. Moduły SoM stanowią pod tym względem doskonałe rozwiązanie, ponieważ można je łatwo zmienić w projekcie, a ich producenci przejmują na siebie cały proces zaadaptowania i uruchomienia nowoczesnych układów SoC. Gotowość na zmiany jest ważna również w innym kontekście. Nie minęło wiele czasu, od kiedy udało się przywrócić ciągłość produkcji i ustabilizować łańcuchy dostaw po tzw. kryzysie półprzewodników, a już musimy mierzyć się z kolejnym wyzwaniem – dużym wzrostem cen i problemami z dostępnością pamięci półprzewodnikowych. Jak sobie z tym radzić? Można optymalizować aplikacje tak, by działały z mniejszą ilością pamięci lub zastosować starsze typy pamięci DDR4/LPDDR4 bądź DDR3/LPDDR3 zamiast najnowszych generacji, na które jest największe zapotrzebowanie. Jeśli projekt bazuje na SoM-ie, jest to niesamowicie łatwe – wystarczy zamontować inny moduł.

Damian Sosnowski, EP

Bibliografia:
- https://www.mouser.pl/datasheet/2/891/Espressif_Systems_01292021_esp32-1991551.pdf
- https://pl.wikipedia.org/wiki/Apple_M1
- https://www.researchgate.net/figure/Comparison-among-SOC-System-On-Chip-MCM-Multi-Chip-Module-SIP-System-In-Package_fig1_228870734
- https://pcbsync.com/sip/
- https://elektronikab2b.pl/opinie/52663-chiplet-nowy-sposob-na-stare-problemy
- https://www.cadence.com/en_US/home/explore/chiplets.html
- https://www.pcbcart.com/assembly-capability/package-on-package-assembly.html
- https://www.purepc.pl/procesor-chip-apple-m5-pro-max-specyfikacja
- https://www.toptal.com/developers/ios/apple-m1-processor-compatibility-overview
- https://www.purepc.pl/qualcomm-snapdragon-x2-elite-wydajnosc-w-grach
- https://mobiili.fi/2018/12/06/qualcomm-paljasti-snapdragon-855n-yksityiskohdat-android-huippupuhelimiin-jopa-45-prosenttia-lisaa-suorituskykya/
- https://smartfonstudio.pl/blog/327_nvidia-jetson-agx-thor-nowy-mozg-robotow-2025.html
- https://nanoreview.net/en/soc/mediatek-dimensity-9500s
- https://www.komputerswiat.pl/komputery-i-laptopy/laptopy/rewolucja-w-swiecie-komputerow-test-procesora-intel-core-ultra-7-155h/ldd134x
- https://www.nxp.com/products/processors-and-microcontrollers/arm-processors/i-mx-applications-processors:IMX_HOME
- https://www.nxp.com/docs/en/brochure/IMXRTPORTBR.pdf
- https://www.st.com/en/microcontrollers-microprocessors/stm32mp1-series.html
- https://ep.com.pl/rynek/temat-miesiaca/14912-od-mikrokontrolerow-do-ukladow-radiowych-bluetooth-z-ukladami-stm32wb
- https://www.st.com/en/microcontrollers-microprocessors/stm32wbx5.html
- https://www.keyestudio.com/products/rock-4-model-c-4gb-single-board-computer-rockchip-rk3399-t-arm-cortex-a72
- https://www.tabletmaniak.pl/212356/rockchip-rk3399/
- https://www.renesas.com/en/about/newsroom/renesas-leads-adas-innovation-power-efficient-4th-generation-r-car-automotive-socs?srsltid=AfmBOopybukXixA5Bz6i-Zx65ChGaXlxg2cO7-uzwUzUSqdPb07K3SJw
- https://www.renesas.com/en/blogs/exploring-entry-fusion-application-architecture-and-cost-effective-solution-utilizing-r-car-v4h?srsltid=AfmBOop_zsvMCSVPGKWPVYES5Kr9hcnT-SB8FkSCd7qQsDiuqgN5Vq4a
- https://deepvisionconsulting.com/renesas-rz-v2h-embedded-vision-platform/
- https://www.electropages.com/blog/2021/05/what-system-module
- https://www.ezurio.com/resources/blog/system-on-module-vs-system-on-chip-what-s-the-difference?srsltid=AfmBOoovk81tBtqGdjEB8jug2zpuMrCh4U8a5ZQZE6oqqzVf6fcwtR7F
- https://www.baslerweb.com/it-it/learning/embedded-processing-platforms/
- https://www.module-store.de/de/smarc/
- https://en.wikipedia.org/wiki/Qseven
- https://www.compulab.com/blog/advantages-of-using-smt-solder-down-system-on-modules/
- https://somlabs.com/
- https://www.raspberrypi.com/documentation/computers/compute-module.html
- https://www.microchip.com/en-us/products/microprocessors/32-bit-mpus/sip-and-som/system-on-module

Słownik cyberbezpieczeństwa (6). Sprzętowa kotwica zaufania: Trusted Platform Module (TPM) i Hardware Security Module (HSM)

Sprzętowe kotwice zaufania, określane po angielsku jako hardware root of trust, to dedykowane układy scalone zaprojektowane do bezpiecznego generowania, przechowywania i użytkowania danych kryptograficznych w izolowanym środowisku sprzętowym, z którego klucze nigdy nie są pobierane w postaci jawnej. Dwa dominujące standardy w tej kategorii, Trusted Platform Module (TPM) oraz Hardware Security Module (HSM), różnią się skalą i przeznaczeniem, lecz wzajemnie się uzupełniają. [1]

Trusted Platform Module to koprocesor kryptograficzny zdefiniowany przez standard ISO/IEC 11889, opracowany przez konsorcjum Trusted Computing Group (TCG). Specyfikacja TPM 2.0 z 2014 roku standaryzuje elastyczniejszy model hierarchii kluczy i algorytmów, wspiera też kryptografię krzywych eliptycznych ECC [1]. Wewnątrz układu znajdują się: sprzętowy generator liczb losowych, silnik kryptograficzny, nieulotna pamięć NV oraz rejestry PCR, czyli rejestry konfiguracji platformy przechowujące skróty kolejnych etapów procesu rozruchowego. Mechanizm pieczętowania, po angielsku sealing, pozwala zaszyfrować dane tak, że ich odszyfrowanie jest możliwe wyłącznie przy niezmienionej konfiguracji platformy, a modyfikacja UEFI, bootloadera lub jądra skutkuje odmową ujawnienia klucza. Stanowi to fundament pomiaru integralności rozruchu, sealingu i zdalnego zaświadczenia integralności, określanego jako remote attestation. TPM może też współpracować z Secure Boot. Opisywane rozwiązania są bazą m.in. dla szyfrowania dysków BitLocker w systemie Windows czy też rozwiązań opartych na dm-crypt i/LUKS [3].

Hardware Security Module to dedykowane urządzenie kryptograficzne przeznaczone do ochrony kluczy na skalę korporacyjną, dostępne jako karta PCIe lub autonomiczne urządzenie sieciowe. Klucz prywatny nigdy nie opuszcza modułu w postaci niezaszyfrowanej; aplikacja przesyła dane do podpisania lub zaszyfrowania, a HSM zwraca wyłącznie wynik operacji [2]. Standardem certyfikacji jest norma FIPS 140-2/140-3 wydana przez NIST, definiująca cztery poziomy bezpieczeństwa, od podstawowego stosowania zatwierdzonych algorytmów na poziomie pierwszym, aż po mechanizmy wykrywania manipulacji i reakcje ochronne (w tym zeroization, czyli aktywne kasowanie kluczy – zależnie od konstrukcji urządzenia) na poziomie trzecim. Przykładowo w wielu zastosowaniach płatniczych wymagane są HSM spełniające wysokie poziomy certyfikacji, często FIPS 140 Level 3 lub równoważne [2].

Praktyczny przykład: BitLocker z TPM i podpisywanie kodu z HSM

W typowym środowisku korporacyjnym TPM 2.0 na stacji roboczej przechowuje klucz VMK, czyli Volume Master Key, będący kluczem głównym chroniącym zaszyfrowany wolumin dysku BitLocker. Klucz ten zapisywany jest w postaci zapieczętowanej, powiązanej z rejestrami PCR opisującymi stan UEFI, menadżera rozruchu i zasad Secure Boot. Przy każdym uruchomieniu moduł weryfikuje niezmienność łańcucha rozruchu i dopiero wówczas odblokowuje klucz, umożliwiając odszyfrowanie dysku transparentnie dla użytkownika i bez możliwości wyeksportowania klucza przez oprogramowanie [3].

Równolegle, w serwerowni, HSM certyfikowany na poziomie FIPS 140-2 Level 3 przechowuje klucz prywatny certyfikatu EV Code Signing, czyli certyfikatu o rozszerzonej walidacji potwierdzającego tożsamość wydawcy oprogramowania. Potok CI/CD, będący zautomatyzowanym łańcuchem budowania i wdrażania oprogramowania, przesyła do modułu skrót artefaktu przez interfejs PKCS#11, czyli standardowe API umożliwiające aplikacjom dostęp do operacji kryptograficznych sprzętu bez znajomości jego wewnętrznej budowy, a HSM zwraca podpis bez ujawniania klucza. Każda operacja jest ponadto rejestrowana w niezmiennym logu audytowym, co jest wymagane przez wystawców certyfikatów EV i regulatorów sektora finansowego. Zestawienie obu mechanizmów ilustruje zasadę głębokiej obrony: TPM zabezpiecza węzeł końcowy przy niemal zerowym koszcie dodatkowym, a HSM chroni klucze o znaczeniu krytycznym dla całej organizacji [4].

Dobre praktyki wdrożenia

W zakresie TPM należy potwierdzić aktywację modułu w UEFI i wersję 2.0, włączyć Secure Boot oraz skonfigurować kopię klucza odzyskiwania BitLocker w usłudze Active Directory lub Microsoft Entra ID. Regularne zaświadczanie stanu platformy, realizowane przez narzędzia klasy MDM, czyli systemy centralnego zarządzania urządzeniami końcowymi w organizacji, pozwala wykrywać modyfikacje łańcucha rozruchowego przed przyznaniem dostępu do zasobów. Przed każdą aktualizacją oprogramowania układowego należy upewnić się, że kopia klucza odzyskiwania jest dostępna, ponieważ zmiana UEFI modyfikuje wartości PCR [1].

W przypadku HSM kluczowe jest dobranie poziomu certyfikacji FIPS do kontekstu: Level 2 często wystarcza dla ogólnej ochrony kluczy PKI, zaś Level 3 zwykle będzie wymagany dla infrastruktury płatniczej i krytycznej. Klucze główne powinny być generowane wyłącznie wewnątrz modułu, a operacje administracyjne muszą wymagać uwierzytelnienia dwuosobowego, określanego jako dual control. Procedura zniszczenia kluczy (nazywana zeroization) przy wycofaniu urządzenia jest typowym wymaganiem standardów i dobrych praktyk w zakresie eksploatacji tego typu urządzeń. Dla obu technologii zaleca się śledzenie harmonogramu migracji do algorytmów postkwantowych opracowywanych przez NIST, ponieważ aktualizowalne oprogramowanie układowe TPM 2.0 i nowoczesnych HSM w niektórych platformach może umożliwić częściową migrację bez wymiany sprzętu (np. wdrożenie nowych prymitywów kryptograficznych, czyli bazowych algorytmów matematycznych takich jak funkcje skrótu czy schematy podpisu) [2].

Filip Krzyżański

[1] https://tiny.pl/w2rrchy6q
[2] https://tiny.pl/fkn00kxvj
[3] https://tiny.pl/478q7_hd4
[4] https://tiny.pl/j4mh831xf

TRZECIARĘKA ZD-11P
Uchwyt montażowy typu „Trzecia ręka”, pająk – uchwyt z latarką, ZD11P

TRZECIARĘKA ZD-11P-1
Uchwyt montażowy typu „Trzecia ręka”, pająk – uchwyt z latarką i lupą, ZD11P-1

TRZECIARĘKA SN-394
Uchwyt montażowy typu „Trzecia ręka”, pająk z lupą 50 mm, przykręcany do blatu Proskit SN-394

TRZECIARĘKA ZD-11M-1
Uchwyt montażowy typu „Trzecia ręka”, pająk – z uchwytem na szpulkę cyny, ZD11M-1

TRZECIARĘKA ZD-11M-2
Uchwyt montażowy typu „Trzecia ręka”, pająk – uchwyt z lupą i podświetleniem LED ZD11M-2

TRZECIARĘKA ZD-11M-3
Uchwyt montażowy typu „Trzecia ręka”, pająk – uchwyt z lupą i podświetleniem LED ZD-11M-3

TRZECIARĘKA ZD-11M
Uchwyt montażowy typu „Trzecia ręka”, pająk – uchwyt ZD11M

TRZECIARĘKA SN-392
Uchwyt montażowy typu „Trzecia ręka” z lupą 90 mm, Proskit SN-392

TRZECIARĘKA
Uchwyt montażowy typu „Trzecia ręka” z lupą 60 mm

Programowanie w środowisku MicroPython (11)

Komunikacja przez ESP-NOW

Poprzednie odcinki znajdują się pod adresem: **https://ulubionykiosk.pl/media**

ESP-NOW to prosty interfejs komunikacyjny, z którego możemy korzystać za darmo i bez ograniczeń. Idealnie nadaje się do zbierania danych z sensorów rozmieszczonych w niewielkiej odległości od siebie, do obsługi domowej automatyki itp. Może być także świetną alternatywą dla Bluetooth.

W 2019 roku inżynierowie firmy Espressif podjęli trud pracowania nowego interfejsu komunikacji radiowej, który miał być prostszy niż Wi-Fi i Bluetooth, oferować większy zasięg i zapewniać wystarczający poziom bezpieczeństwa, aby nie dało się łatwo podsłuchać wiadomości, ani zastosować techniki ataku typu *reply attack*.

ESP-NOW wykorzystuje częstotliwość 2,4 GHz – podobnie jak Wi-Fi i Bluetooth, nie potrzeba zatem żadnych dodatkowych zasobów sprzętowych poza tymi, które moduły ESP32 (a także stare ESP8266) mają już wbudowane. Wynika z tego bardzo istotny wniosek: komunikację przez ESP-NOW można zastosować nawet w urządzeniach, które zostały wyprodukowane przed rokiem 2019. Wystarczy zaktualizować oprogramowanie i już można korzystać z możliwości ESP-NOW.

Interfejs ten umożliwia dwukierunkową komunikację pomiędzy dwoma urządzeniami, a także komunikację typu „jeden do wszystkich". Urządzenia można ze sobą sparować (ale nie zawsze jest taka potrzeba), dzięki czemu można bardzo łatwo tworzyć proste sieci. Parowanie urządzeń ma zastosowanie w celu wprowadzenia szyfrowania – połączone w ten sposób urządzenia zapisują sobie klucz szyfru AES-128.

Zasięg komunikacji jest całkiem dobry. Testy przeprowadzone przez wielu radioamatorów dowodzą, że przy pomocy ESP-NOW można przesyłać dane na odległość ok. 300 metrów, a w trybie long range nawet 500...800 metrów w otwartej przestrzeni.

ESP-NOW ma jednak pewną wadę – działa tylko i wyłącznie na modułach produkowanych przez firmę Espressif. Zatem wybierając ten interfejs skreślamy jednocześnie możliwość komunikacji z modułami firm Nordic, Microchip czy jakiejkolwiek innej. Póki co nie jest pewne, czy Espressif kiedykolwiek umożliwi wykorzystywanie swojego interfejsu na sprzęcie innych producentów.

Interfejs ESP-NOW wciąż dynamicznie się rozwija i ciągle dodawane są nowe funkcjonalności. Dlatego przed przystąpieniem do testów koniecznie zainstaluj najnowszego MicroPythona. W chwili pisania tego odcinka dostępna jest wersja 1.27.0 i to z nią zgodne są wszystkie przykłady. Wiadomo już teraz, że MicroPython 1.27.0 obsługuje ESP-NOW w wersji 1.0, ale dostępny jest także ESP-NOW 2.0, który obsługiwać można póki co tylko w ESP-IDF, a w MicroPythonie jeszcze nie. Zasadnicza różnica jest taka, że stara wersja ESP-NOW umożliwia wysyłanie wiadomości o długości maksymalnie 250 bajtów, a nowa wersja – 1470 bajtów. Być może obsługa ESP-NOW 2.0 zostanie dodana w MicroPythonie 1.28.0.

Trochę teorii

Jak już wspomniano, ESP-NOW wykorzystuje transmiter Wi-Fi, zatem oprócz zaimportowania modułu odpowiedzialnego za ESP-NOW, musimy także dodać moduł obsługujący sieć Wi-Fi.

```
import network
import espnow
```

Wszystkie moduły z rodziny ESP32 mają po dwie karty sieciowe – jedna może pracować jako klient (*station*), a druga jako *access point*. Musimy utworzyć instancję jednej z nich, a następnie ją aktywować. Jeżeli chcemy wykorzystać kartę sieciową klienta, należy użyć poniższego polecenia:

```
wlan = network.WLAN(network.STA_IF)
```

Poprzednie części kursu i dodatkowe materiały dostępne są na stronie **https://ulubionykiosk.pl/media**

Jeżeli chcemy wykorzystać *access point* do ESP-NOW, wystarczy tylko zmienić argument przekazywany do konstruktora klasy WLAN:

```
wlan = network.WLAN(network.AP_IF)
```

Obie karty sieciowe mogą być użyte na potrzeby ESP-NOW i mają takie same możliwości (ale inny adres MAC!). W praktycznych zastosowaniach może się zdarzyć, że oprócz ESP-NOW będziemy chcieli mieć dostęp do sieci Wi-Fi i Internetu. W takiej sytuacji możemy zastosować kartę sieciową *station* zupełnie normalnie na potrzeby dostępu do Internetu, a kartę *access point* – do obsługi ESP-NOW.

Niezależnie od tego, którą kartę sieciową wybierzemy, musimy ją aktywować poleceniem:

```
wlan.active(True)
```

Identyfikatorem wszystkich urządzeń w sieci ESP-NOW jest adres MAC karty sieciowej, która obsługuje transmisję bezprzewodową. Możemy ten adres pozyskać w następujący sposób:

```
mac = wlan.config('mac')
print(f"MAC Address: {mac}")
```

Tak odczytany adres MAC zapisany zostaje w zmiennej typu **bytes**, składającej się z 6 bajtów. Wyświetlając je funkcją **print** uzyskamy mniej więcej taki rezultat:

```
b'\xd8\xa0\x1di\x9fD'
```

Nie wygląda to jak adres MAC, jaki widzimy na komputerach, gdzie poszczególne bajty adresu oddzielone są znakiem dwukropka. Aby wyświetlić adres MAC w sposób tradycyjny, możemy posłużyć się funkcją hexlify z modułu binascii.

```
binascii.hexlify(mac, ":").decode().upper()
```

Funkcja **hexlify** przekształca ciąg bajtów na ich reprezentację ASCII, wykorzystując cyfry w zakresie 0–9 i litery a–f. Drugim argumentem tej funkcji jest separator, jaki ma oddzielać bajty i musi to być jeden znak. Funkcja **hexlify** zwraca obiekt typu **bytes**, czyli poprzedzony jest znakiem b'. Aby się go pozbyć, musimy bytes przekonwertować na string, korzystając z metody **decode**. Ostatnim etapem jest zamiana małych liter na wielkie przy pomocy metody **upper**. Po takim zabiegu zobaczymy w konsoli adres MAC w tradycyjnej postaci, do której wszyscy są przyzwyczajeni:

```
'DC:DA:0C:1E:4E:E0'
```

Możemy teraz przejść do obsługi klasy ESP-NOW. Najpierw musimy utworzyć i aktywować jej instancję:

```
e = espnow.ESPNow()
e.active(True)
```

Metoda **active** przyjmuje argument True lub False, aby aktywować lub dezaktywować klasę, zaś jeżeli wywołamy ją bez argumentu, wówczas metoda zwróci informację, czy klasa jest obecnie aktywna.

Aby wysłać wiadomość musimy wywołać metodę **send**, która przyjmuje trzy argumenty:

1. Pierwszy z nich to adres MAC odbiorcy. Możemy wykorzystać także adres specjalny b'\xFF\xFF\xFF\xFF\xFF\xFF', aby wysłać wiadomość do wszystkich urządzeń. Możemy także podać **None**, jeżeli chcemy wysłać wiadomość do wszystkich urządzeń, jakie zostały wcześniej sparowane.
2. Drugi argument to dane do wysłania, podane jako string, bytes lub bytearray.
3. Trzeci argument jest opcjonalny. Jeżeli podamy True, to klasa sprawdzi, czy wiadomość została odczytana przez wybranego odbiorcę lub wszystkich sparowanych odbiorców. W razie niepowodzenia, metoda zgłosi wyjątek ETIMEDOUT. Jest to domyślne zachowanie tej metody. Jeżeli podamy False, wówczas metoda nie będzie sprawdzać faktu odebrania wiadomości i zakończy działanie natychmiast po wysłaniu wiadomości.

Oto przykład wysłania krótkiej wiadomości tekstowej do wszystkich odbiorców, jacy są w zasięgu:

```
e.send(b'\xFF\xFF\xFF\xFF\xFF\xFF', "Hello world!")
```

Odebrane wiadomości są najpierw zapisywane do bufora klasy ESPNow, gdzie czekają na odczytanie przez nasz program. Odebrać je możemy na trzy sposoby. Pierwszym z nich jest wykorzystanie metody **recv**, która zwraca dane w postaci krotki **(mac, msg)**, gdzie mac to adres nadawcy podany jako bytes, a msg to dane jako bytearray. Jeżeli w buforze nie ma żadnych danych, funkcja zwraca krotkę **(None, None)**.

Metoda **recv** przyjmuje tylko jeden argument – **timeout**, czyli czas oczekiwania w milisekundach. Możliwe są następujące opcje:

- 0 – brak oczekiwania. Funkcja natychmiast kończy pracę, jeżeli w buforze nie ma żadnych danych,
- liczba dodatnia – czas w milisekundach, na który program jest zawieszany w oczekiwaniu na wiadomość,
- liczba ujemna – funkcja czeka w nieskończoność,
- None lub brak argumentu – funkcja zachowuje się zgodnie z konfiguracją domyślną lub konfiguracją użytkownika, ustaloną przy pomocy metody **config**.

Inny sposób to użycie metody **irecv**. Działa dokładnie tak samo, jak **recv**, ale zwracając dane nie alokuje nowych zmiennych w pamięci, lecz zwraca wskaźniki do wewnętrznego bufora klasy. Dlatego też używanie tej funkcji jest wskazane w przerwaniach. Metoda irecv również przyjmuje argument **timeout**, który działa tak samo, jak w **recv**.

Trzecia metoda to **recvinto**. Jej drugim argumentem jest wartość **timeout**, tak samo jak w poprzednio omawianych metodach. Pierwszym argumentem musi być lista, do której zostaną zapisane dane zwracane przez metodę. Pierwszym elementem tej listy musi być zmienna typu **bytearray** o długości 6 bajtów, służąca do zapisywania adresu MAC nadawcy. Drugim elementem listy jest również **bytearray**, w którym zostaje zapisana wiadomość o długości maksymalnie 250 bajtów.

Wspomniano, że metoda **irecv** może być z powodzeniem wykorzystywana w przerwaniach. Najpierw jednak musimy skonfigurować klasę, wywołując w tym celu metodę **irq**, która przyjmuje tylko jeden argument – nazwę funkcji, która ma zostać uruchomiona, kiedy zostanie odebrana jakaś wiadomość. Ta funkcja również musi przyjmować jeden argument – jest on instancją klasy ESPNow, która odebrała wiadomość.

Należy pamiętać, że jeżeli ESP32 odbierze jakąś wiadomość zanim skonfigurujemy obsługę przerwań, wówczas klasa nie wywoła funkcji obsługującej przerwania, a wiadomość będzie czekała w buforze tak długo, aż przyjdzie jakaś następna wiadomość. Dopiero wtedy uruchomi się obsługa przerwań. Dobrym zwyczajem jest, aby po konfiguracji przerwań ręcznie sprawdzić, czy są jakieś wiadomości oczekujące w buforze, a jeżeli tak, to samodzielnie wywołać funkcję obsługującą przerwanie.

Kolejną metodą klasy ESPNow jest **any**. Sprawdza ona, czy w buforze są jakieś wiadomości do odczytania i w takiej sytuacji zwraca True. Metoda nie przyjmuje żadnych argumentów.

Aby przesyłać wiadomość do wybranego przez nas urządzenia, najpierw musimy je sparować przy pomocy metody **add_peer**. Jako argument podajemy adres MAC urządzenia, które ma odebrać wiadomość. Adres musi być zapisany w postaci obiektu bytes o długości 6 bajtów. Urządzenie odbierające nie musi być sparowane z urządzeniem nadającym – pod warunkiem, że transmisja nie jest szyfrowana. Oto przykład takiej operacji:

```
peer_mac = b'\xd8\xa0\x1di\x9fD'
e.add_peer(peer_mac)
```

Pamiętaj, że jeżeli chcesz wysyłać wiadomości do wszystkich urządzeń przy pomocy adresu b'\xFF\xFF\xFF\xFF\xFF\xFF', to również musisz go wcześniej dodać do listy sparowanych adresów.

Jeżeli chcemy wprowadzić szyfrowanie wiadomości, najpierw na wszystkich urządzeniach musimy określić 16-bajtowy klucz PMK (*Primary Master Key*) przy pomocy metody **set_pmk**. Na każdym urządzeniu w naszej sieci klucz PMK musi być identyczny:

```
pmk = b'\x00\x11\x22\x33\x44\x55\x66\x77\x88\x99\xAA\xBB\
xCC\xDD\xEE\xFF'
e.set_pmk(pmk)
```

Kolejnym krokiem jest sparowanie nadajnika i odbiornika, przy czym w tym przypadku to odbiorca musi sparować się z nadawcą. Potrzebujemy do tego klucz LMK (*Local Master Key*), który również ma długość 16 bajtów. Następnie wywołujemy metodę **add_peer** z dodatkowymi argumentami, jak na przykładzie poniżej:

```
peer_mac = b'\xd8\xa0\x1di\x9fD'
lmk = b'\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0A\x0B\x0C\
x0D\x0E\x0F'
e.add_peer(peer_mac, lmk, encrypt=True)
```

Aby usunąć powiązane urządzenie, należy posłużyć się funkcją **del_peer(mac)**, a żeby dostać różne informacje na jego temat, należy wywołać metodę **get_peer(mac)**. Możemy także wyświetlić wszystkie dodane urządzenia przy pomocy **get_peers()**.

Ćwiczenia praktyczne

Aby zrealizować ćwiczenia, zaprezentowane w tym odcinku kursu, potrzebować będziemy co najmniej dwie płytki z modułami ESP32 lub ESP32-S3. Jedna będzie pełniła rolę nadajnika, a druga będzie odbiornikiem, który wyświetli w konsoli odebrane wiadomości.

Na **listingu 1** przedstawiono kod najprostszego możliwego odbiornika ESP-NOW – składa się on zaledwie z kilkunastu linijek. Linia 1 służy do tego, aby adres MAC odbiornika wyświetlić w konsoli. Należy go skopiować i wkleić do kodów nadajnika w odpowiednim miejscu.

Po zainicjalizowaniu sieci WLAN oraz klasy ESPNow, program ogranicza się do jednej pętli nieskończonej while True (linia 2).

W linii 3 widzimy wywołanie metody **recv** z argumentem -1, co oznacza, że program zatrzymuje się w tym miejscu i czeka w nieskończoność, aż zostanie odebrana jakaś wiadomość. Kiedy to nastąpi, adres MAC nadawcy oraz dane wiadomości zostają zapisane do zmiennych **sender** oraz **data**.

Obie zmienne są typu **bytes**. Moglibyśmy je wyświetlić już teraz, jednak w konsoli dostalibyśmy napis poprzedzony znakiem b', a wszystkie polskie znaki diakrytyczne byłyby wyświetlone jako kody znaków UTF-8. Aby przekształcić obiekt **bytes** na ładnie wyglądający string, musimy wywołać metodę **decode** (linia 4). Pozostaje już tylko wyświetlić nadawcę oraz wiadomość, co robimy w linii 5.

```
# Plik receiver.py
import espnow
import network

sta = network.WLAN(network.STA_IF)
sta.active(True)

mac = sta.config('mac')
print(f"MAC Address: {mac}")                                    # 1

e = espnow.ESPNow()
e.active(True)

while True:                                                     # 2
    sender, data = e.recv(-1)                                   # 3
    data = data.decode()                                        # 4
    print(f"{sender} -> {data}")                                # 5
```

Listing 1. Kod pliku receiver.py

```
# Plik sender.py
import espnow
import network

sta = network.WLAN(network.STA_IF)
sta.active(True)

mac = sta.config('mac')
print(f"MAC Address: {mac}")

e = espnow.ESPNow()
e.active(True)

peer_mac = b'\xd8\xa0\x1di\x9fD'                                # 1
everyone = b'\xFF\xFF\xFF\xFF\xFF\xFF'                          # 2
e.add_peer(peer_mac)                                            # 3
e.add_peer(everyone)

e.send(everyone, "Wiadomość do wszystkich")                     # 4
e.send(peer_mac, "Wiadomość do wybranego odbiorcy")             # 5
e.send(peer_mac, "Wiadomość do wybranego odbiorcy               # 6
                  bez potwierdzenia odbioru", False)
```

Listing 2. Kod pliku sender.py

Uruchamiamy kod w edytorze Thonny. Na konsoli wyświetli się adres MAC. Należy go skopiować i przejść do **listingu 2**, gdzie znajduje się kod najprostszego możliwego nadajnika. W linii 1 znajduje się zmienna **peer_mac**, gdzie musimy wkleić adres MAC odbiornika. W linii 2 tworzymy także zmienną **everyone**, do której zapisujemy uniwersalny adres MAC. Spowoduje to wysłanie wiadomości do wszystkich odbiorników, jakie są w zasięgu nadajnika.

Zanim zaczniemy wysłać wiadomości, musimy te adresy MAC dodać przy pomocy metody **add_peer**, co jest realizowane w linii 3 i kolejnej.

W linii 4 wysyłamy wiadomość do wszystkich. W kolejnej linii 5 znajduje się polecenie wysłania wiadomości tylko do jednego odbiorcy. Jeżeli odbiorca nie odbierze tej wiadomości, to dostaniemy wyjątek ETIMEDOUT. Jeżeli nie interesuje nas sprawdzanie, czy wiadomość została doręczona, możemy dodać argument False (linia 6).

Przejdźmy teraz do **listingu 3**, gdzie znajduje się kod odbiornika korzystającego z przerwań. Pojawiła się w nim

```
# Plik receiver_irq.py
import espnow
import network

sta = network.WLAN(network.STA_IF)
sta.active(True)

mac = sta.config('mac')
print(f"MAC Address: {mac}")

e = espnow.ESPNow()
e.active(True)

def receive_cb(e):                                              # 1
    while e.any():                                              # 2
        sender, data = e.irecv()                                # 3
        data = data.decode()
        print(f"{sender} -> {data}")

e.irq(receive_cb)                                               # 4

if e.any():                                                     # 5
    receive_cb(e)
```

Listing 3. Kod pliku receiver_irq.py

```
# Plik receiver_encrypted.py
import espnow
import network

sta = network.WLAN(network.STA_IF)
sta.active(True)

mac = sta.config('mac')
print(f"MAC Address: {mac}")

e = espnow.ESPNow()
e.active(True)
e.set_pmk(b'\x00\x11\x22\x33\x44\x55\x66\x77                    # 1
           \x88\x99\xAA\xBB\xCC\xDD\xEE\xFF')

sender_mac = b'\xdc\xda\x0c\x1eN\xe0'
e.add_peer(sender_mac, b'\x00\x01\x02\x03\x04\x05\x06\x07\x08 # 2
           \x09\x0A\x0B\x0C\x0D\x0E\x0F', encrypt=True)

while True:
    sender, data = e.recv(-1)
    data = data.decode()
    print(f"{sender} -> {data}")
```

Listing 4. Kod pliku receiver_encrypted.py

funkcja **receive_cb** (linia 1), która jest wywoływana po odebraniu wiadomości. Ponieważ mogłoby się zdarzyć, że zostanie odebranych kilka wiadomości zanim funkcja zostanie wywołana, to przy uruchomieniu jej musimy przeprowadzić obsługę wszystkich wiadomości znajdujących się już w buforze odbiorczym. W tym celu w programie pojawiła się pętla while, która wykonuje się tak długo, aż metoda **any** zwróci False (linia 2), czyli do momentu całkowitego opróżnienia bufora odbiorczego. Obsługa wiadomości wygląda bardzo podobnie do tej, którą przedstawiono na listingu 1, a jedyna różnica jest taka, że zamiast metody recv wykorzystujemy **irecv** (linia 3).

Aby obsługa przerwań działała, musimy ją skonfigurować i w linii 4 wskazujemy, jaka funkcja ma się wywoływać po odebraniu wiadomości. Istnieje prawdopodobieństwo, że zostanie odebrana jakaś wiadomość, zanim jeszcze skonfigurujemy przerwania. W takiej sytuacji przerwanie nie zostanie zgłoszone, a wiadomość będzie czekać w buforze, aż zostanie odebrana jakaś kolejna wiadomość i dopiero wtedy zostanie wywołana funkcja przerwania. Aby uniknąć takiej sytuacji, musimy sprawdzić przy pomocy metody **any**, czy w buforze odbiorczym coś się znajduje i jeżeli tak, to ręcznie wywołać funkcję **receive_cb** (linia 5).

Listing 4 demonstruje, w jaki sposób można wprowadzić szyfrowanie do odbiornika wiadomości. W linii 1 definiujemy klucz PMK. Pamiętajmy, że transmisja szyfrowana wymaga, aby odbiornik był sparowany z nadajnikiem. Zatem w linii 2 dodajemy go metodą add_peer, gdzie podajemy jego adres MAC, a także klucz LMK.

Analogicznie postępujemy tworząc kod nadajnika, który jest przedstawiony na **listingu 5**. W liniach 1 podajemy taki sam klucz PMK, a w linii 2 dodajemy odbiornik z identycznym kluczem LMK.

Kolejny przykład pokazuje, w jaki sposób można uzyskać większy zasięg połączenia, ale kosztem 4-krotnego zmniejszenia prędkości transmisji. Zobaczmy kod z **listingu 6**. W linii 1 zmieniamy

```
# Plik sender_encrypted.py
import espnow
import network

sta = network.WLAN(network.STA_IF)
sta.active(True)

mac = sta.config('mac')
print(f"MAC Address: {mac}")

e = espnow.ESPNow()
e.active(True)
e.set_pmk(b'\x00\x11\x22\x33\x44\x55\x66\x77                    # 1
           \x88\x99\xAA\xBB\xCC\xDD\xEE\xFF')

receiver_mac = b'\xd8\xa0\x1di\x9fD'
e.add_peer(receiver_mac, b'\x00\x01\x02\x03\x04\x05\x06\x07\x08     # 2
           \x09\x0A\x0B\x0C\x0D\x0E\x0F', encrypt=True)

e.send(receiver_mac, "Szyfrowana wiadomość")
```

Listing 5. Kod pliku sender_encrypted.py

```
# Plik receiver_long_rangr.py
import espnow
import network

sta = network.WLAN(network.STA_IF)
sta.active(True)
sta.config(channel=6, protocol=network.WLAN.PROTOCOL_LR)        # 1

mac = sta.config('mac')
print(f"MAC Address: {mac}")

e = espnow.ESPNow()
e.active(True)
e.config(rate=espnow.RATE_LORA_250K)                            # 2

while True:
    sender, data = e.recv(-1)
    data = data.decode()
    print(f"{sender} -> {data}")
```

Listing 6. Kod pliku receiver_long_range.py

```
# Plik sender_long_range.py
import espnow
import network

sta = network.WLAN(network.STA_IF)
sta.active(True)
sta.config(channel=6, protocol=network.WLAN.PROTOCOL_LR)        # 1

mac = sta.config('mac')
print(f"MAC Address: {mac}")

e = espnow.ESPNow()
e.active(True)
e.config(rate=espnow.RATE_LORA_250K)                            # 2

everyone = b'\xFF\xFF\xFF\xFF\xFF\xFF'
e.add_peer(everyone)

e.send(everyone, "Test długiego zasięgu")
```

Listing 7. Kod pliku sender_long_range.py

konfigurację sieci WLAN. Przestawiamy jej protokół z normalnego Wi-Fi na **PROTOCOL_LR**, który jest autorskim rozwiązaniem inżynierów firmy Espressif. Tak skonfigurowany nadajnik może komunikować się tylko z odbiornikami, które zostały skonfigurowane w ten sam sposób. Ponadto musimy określić, który kanał pasma chcemy wykorzystywać. W kodach demonstracyjnych autorzy podają kanał 6, choć nie tłumaczą dlaczego – nie wchodząc w szczegóły również zastosujemy ten sam kanał.

Kolejnym krokiem jest zmodyfikowanie konfiguracji klasy ESPNow, co robimy w linii 2. Tak skonfigurowana klasa będzie pracować w trybie długiego zasięgu z prędkością transmisji 250 kbit/s. Kod nadajnika znajdziemy na **listingu 7**. Należy go skonfigurować tak samo i w taki sam sposób jak odbiornik.

To wszystko na temat komunikacji przez ESP-NOW. W następnym odcinku, który będzie już ostatnią częścią kursu MicroPythona, zobaczymy w jaki sposób możemy połączyć moduł ESP32 z telefonem poprzez Bluetooth.

Dominik Bieczyński
leonow32@gmail.com

Zobacz więcej:
- Repozytorium kursu na GitHubie
  https://github.com/leonow32/micropython
- Dokumentacja klasy ESP-NOW
  https://docs.micropython.org/en/latest/library/espnow.html

Pomiary charakterystyk częstotliwościowych (8)

Obwody w.cz.

Poprzednie odcinki znajdują się pod adresem: **https://ulubionykiosk.pl/media**

W ostatniej części cyklu o pomiarach charakterystyk częstotliwościowych skoncentrowano się głównie na testach komercyjnych urządzeń, podzespołów i przyrządów w.cz., w większości dostępnych „z wirtualnej półki sklepowej", czyli w sprzedaży internetowej. Przebadane zostały różnorodne anteny, filtry, wzmacniacze, tłumiki i sztuczne obciążenia w.cz. W testach wykorzystano przede wszystkim dwa zautomatyzowane i dość zaawansowane przyrządy pomiarowe z rodziny nanoVNA, dzięki możliwościom których autor materiału mógł skupić się przede wszystkim na metodyce i parametrach samych pomiarów. Przedstawiony dalej materiał może okazać się inspiracją i źródłem praktycznej wiedzy dla Czytelników o ambicjach konstruktorskich w dziedzinie radioelektroniki. Stanowi też preludium do cyklu publikacji poświęconego szeroko pojętej technice radiokomunikacyjnej.

Środowisko, metodyka i ramy pomiarów

Wykorzystane w testach sprzętowe środowisko pomiarowe zostało oparte na dwóch półprofesjonalnych wektorowych analizatorach obwodów (ang. *Vector Network Analyser*) w.cz. i b.w.cz. z rodziny **nanoVNA** [1]. Każdorazowo były one dostosowywane do partykularnych urządzeń testowanych, a także przyjętego zakresu testów. W przypadku testów urządzeń aktywnych dodatkowo używano: regulowanego zasilacza stabilizowanego na napięcia 3 V, 5 V, 9 V i 12 V oraz automatycznego multimetru cyfrowego do kontroli napięć zasilania. Przy pomiarach wzmacniaczy należało zmierzyć się z zagadnieniami przesterowań na wejściu i wyjściu badanego urządzenia i dlatego też stosowano obserwację jakości sygnałów za pomocą prostego oscyloskopu cyfrowego oraz półprofesjonalnego analizatora widma z rodziny **tinySA** (ang. *Spectrum Analyser*) [2]. Wszystkie wymienione analizatory zostały przed rozpoczęciem właściwych pomiarów skalibrowane zgodnie z instrukcjami dostępnymi na stronach twórców tych urządzeń.

Analizator wektorowy nanoVNA był wykorzystywany w dwóch wersjach: podstawowej (**fotografia 19**), pracującej w zakresie częstotliwości od 50 kHz do 900 MHz (z podziałem na dwa podpasma) oraz w wersji znacznie bardziej zaawansowanej H4 Plus (**fotografia 20**), pracującej w zakresie częstotliwości od 50 kHz do 2,7 GHz (z wewnętrznym podziałem na trzy podpasma). Liczne i wyczerpujące opisy sposobu eksploatacji obu wymienionych przyrządów pomiarowych można bez problemu znaleźć w Internecie (m.in. pod adresem [1] i dalszymi odnośnikami). W tym miejscu warto wspomnieć, że pierwszy z nich, zarówno z uwagi na ograniczony zakres pomiarowy, jak i funkcjonalny, a także niewielki rozmiar wyświetlacza (2,8"), można traktować bardziej jako podręczne, kieszonkowe urządzenie do pomiarów polowych (w terenie) – przydatne głównie przy strojeniu anten na pasma HF, VHF oraz na niższe podpasma UHF. Natomiast drugi z zastosowanych przyrządów (z wyświetlaczem o przekątnej 4" oraz znacznie poszerzonym zakresem mierzonego pasma częstotliwości i rozbudowanymi funkcjami pomiarowymi) świetnie sprawdził się jako całkiem przyzwoity,

Fotografia 19. Zestaw analizatora wektorowego w wersji NanoVNA-H [1]

Fotografia 20. Analizator wektorowy w wersji NanoVNA-H4 Plus

Poprzednie części kursu i dodatkowe materiały dostępne są na stronie **https://ulubionykiosk.pl/media**

Fotografia 21. Zestaw analizatora widma TinySA [2]

półprofesjonalny przyrząd laboratoryjny, dostępny za dość przystępną cenę. Natomiast wspomniany analizator tinySA w wersji podstawowej (**fotografia 21**) nie nadaje się raczej do zastosowań istotnie ambitniejszych niż zgrubna obserwacja widma badanego sygnału. W szczególności sprawdził się przy wykrywaniu obecności wyraźnych zniekształceń nieliniowych sygnału podstawowego, objawiających się poprzez występowanie znacznych wartości jego wyższych harmonicznych.

Jeśli chodzi o generalną metodykę samych pomiarów, to należy w tym miejscu wyjaśnić, że wykorzystywane w testach analizatory wektorowe umożliwiały pomiar przede wszystkim dwóch kluczowych elementów doskonale znanej w technice mikrofalowej tzw. **macierzy rozproszenia S** [3]. Są nimi zespolone parametry: **S11** oraz **S21**. Nie wdając się tutaj w zbyt daleko idące dywagacje teoretyczne, oba wymienione parametry są badane w warunkach dopasowania do impedancji wyjściowej (port oznaczony jako „S11") oraz wejściowej VNA (port oznaczony jako „S21"), wynoszącej dokładnie 50 Ω. Pomiar parametru S11 odbywa się na podstawie analizy zespolonego sygnału odbitego od wrót wejściowych badanego urządzenia, czyli tzw. straty zwrotnej (ang. *Return Loss*). Natomiast pomiar parametru S21 jest oparty wyłącznie o analizę zespolonego sygnału odebranego na wrotach wyjściowych testowanego ustroju w warunkach odpowiedniego pobudzenia na jego wrotach wejściowych. Analiza parametru S11 może zostać wykorzystana do wyznaczenia m.in. takich szczegółowych parametrów elektrycznych, jak moduł impedancji |Z|, rezystancja R, reaktancja X, czy współczynnik fali stojącej WFS (ang. SWR, *Standing Wave Ratio*) – kluczowych przede wszystkim przy ocenie dopasowania, sprawności i ogólnej jakości pracy torów nadawczych. Z kolei analiza parametru S21 jest najbardziej przydatna do oceny wzmocnienia napięciowego i mocy dla danego zakresu częstotliwości dwuwrotników, jakimi są m.in. filtry i wzmacniacze pasmowe. Warto w tym miejscu wyraźnie podkreślić dwa zasadnicze aspekty praktyczne:

- pomiary szeroko pojętych charakterystyk częstotliwościowych nie muszą dotyczyć wyłącznie transmitancyjnej analizy elementu S21 macierzy rozproszenia, dostępnego wyłącznie w przypadku dwuwrotników (czwórników z wrotami wejściowymi i wyjściowymi – jak np. filtry, tłumiki czy wzmacniacze),
- w szczególności, pomiary szeroko pojętych charakterystyk częstotliwościowych w zakresie analizy elementu S11 macierzy rozproszenia są kluczowe dla przypadków jednowrotników, czyli dwójników z wyłącznie pojedynczymi wrotami (jak np. anteny czy sztuczne obciążenia).

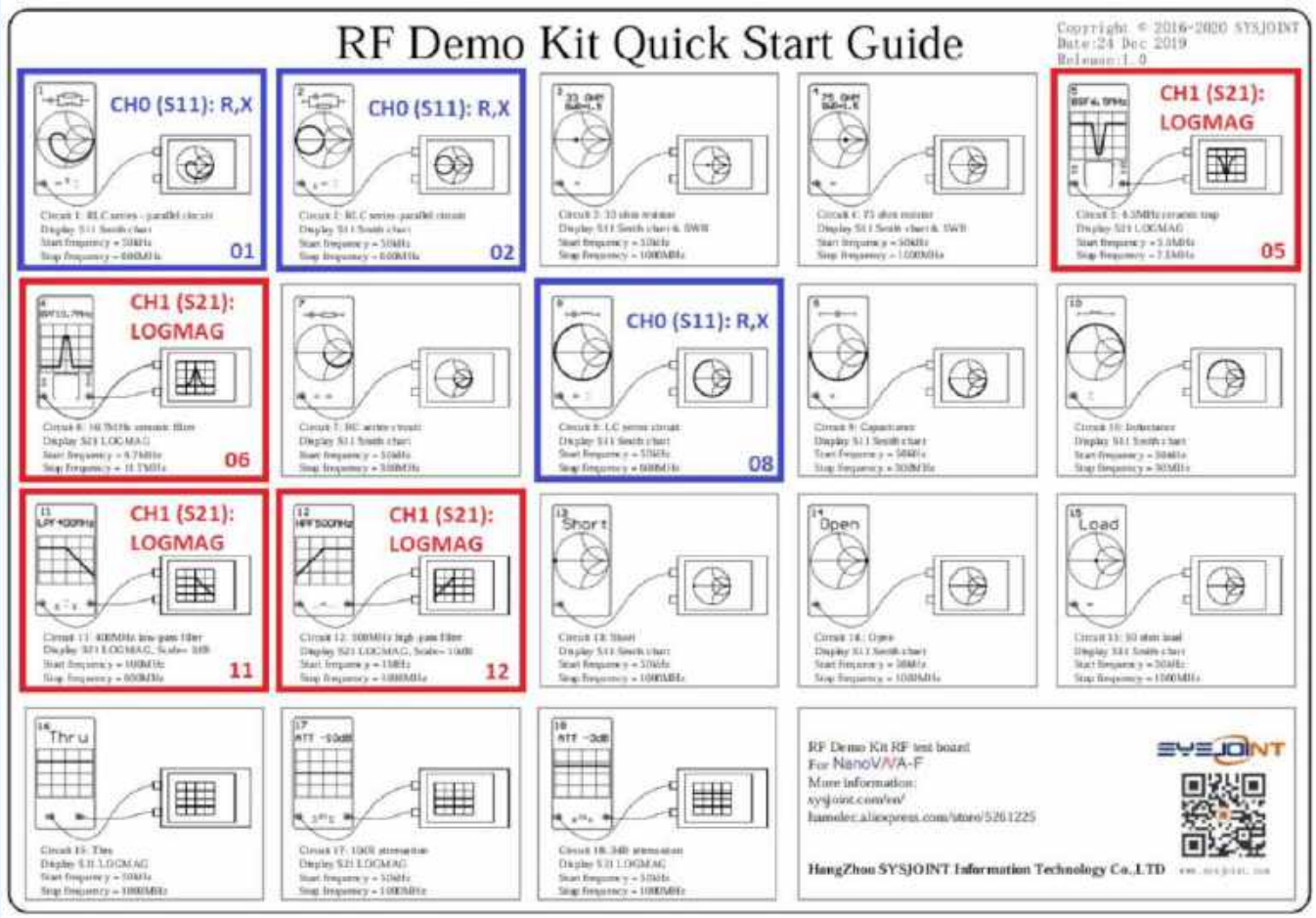
Wyznaczone na potrzeby tej publikacji ramy pomiarów zostały podzielone na trzy główne grupy. Pierwsza z nich to swego rodzaju „wprawka" oparta na dedykowanej właśnie do tego celu (**fotografia 22**) płytce testowej (ang. EvB, *Evaluation Board*) [4], nazwanej przez producenta RF Demo-Kit i wyposażonej w 18 przykładowych obwodów jedno- i dwuwrotników pasywnych. Ta część prezentowanych eksperymentów pomiarowych miała na celu przede wszystkim oswojenie Czytelnika z podstawowym środowiskiem pomiarowym i jego możliwościami, jednak sam RF Demo-Kit będzie szerzej wykorzystywany w trakcie zapowiadanego wcześniej cyklu edukacyjnego o szeroko pojętych technikach radiowych – także do przybliżenia Czytelnikom sposobu korzystania z tzw. wykresu kołowego Smitha, zwizualizowanego na spodniej stronie płytki testowej. W drugiej grupie ujęto pomiary dwójników (jednowrotników): wybranych odbiorczo-nadawczych radiokomunikacyjnych anten HF/VHF/UHF, sztucznych obciążeń rezystancyjnych oraz rezonatorów kwarcowych, które zostały wykorzystane do konstrukcji przebadanych i opisanych dalej filtrów pasmowo-przepustowych SSB. Trzecia grupa pomiarów obejmowała czwórniki (dwuwrotniki), takie jak: tłumiki rezystancyjne, filtry pasmowoprzepustowe i pasmowozaporowe oraz szerokopasmowe wzmacniacze na pasma HF/VHF/UHF. Specyfiki konkretnych pomiarów w każdej z wymienionych grup (w szczególności: sposób pomiaru, zakres częstotliwości, jak również mierzone parametry) różniły się na tyle pomiędzy poszczególnymi przypadkami, że zostały wyczerpująco opisane dopiero przy partykularnych przypadkach testowych.

Pierwsze kroki, czyli pomiary obwodów na płycie nanoVNA EvB

Jako pierwsze badane urządzenie wybrano płytkę demonstracyjną RF Demo-Kit (fotografia 22), przeznaczoną do testów i nauki obsługi urządzeń z rodziny nanoVNA a – w szczególności – do zdobywania praktycznych umiejętności związanych z pracą z tzw. wykresem kołowym Smitha [3, 4]. Jakkolwiek, ostatnie z wymienionych zadań nie będzie poruszane w tym opracowaniu, a zostanie szczegółowo podjęte we wspomnianym wcześniej cyklu publikacji o technikach RF. Na PCB RF Demo-Kit umieszczono

Fotografia 22. Płytka testowa do analizatora nanoVNA RF Demo-Kit [4]

Fotografia 23. Pomiar filtru ceramicznego na płytce RF Demo-Kit wykonany analizatorem nanoVNA

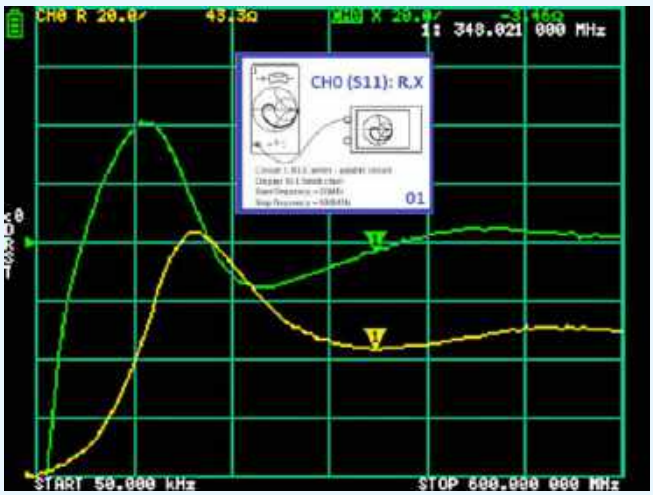


Rysunek 99. Wykaz testów do płytki RF Demo-Kit [4]

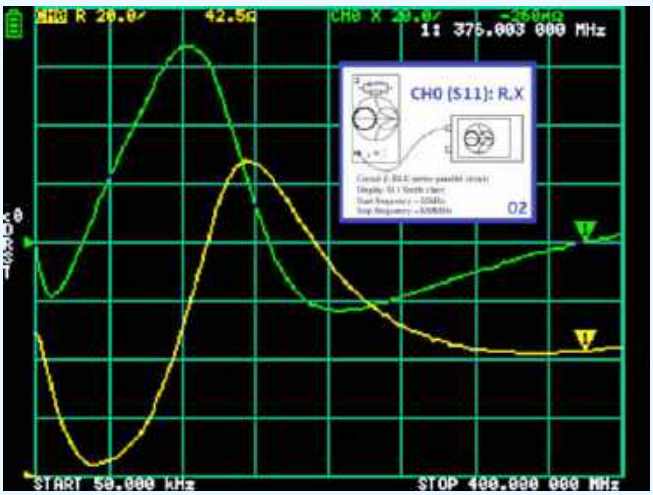
aż 18 obwodów jedno- i dwuwrotników pasywnych, podłączanych do analizatora VNA za pomocą załączonych w zestawie z płytką, przejściowych przewodów połączeniowych SMA-IPEX (**fotografia 23**). Na **rysunku 99** zaprezentowano opublikowany na stronie producenta płytki [4], graficzny wykaz dedykowanych testów z wyróżnionymi kolorowymi ramkami konfiguracjami testowymi (niebieskie – dwójniki, czerwone – czwórniki), które autor uznał za warte pomierzenia i prezentacji w ramach tego artykułu. **Rysunki 100** do **106** przybliżają charakterystyki pomiarowe wybranych obwodów: impedancję Z=R+jX dla dwójników oraz moduł transmitancji napięciowej |A(jΩ)| w skali logarytmicznej dla czwórników. Dla ułatwienia identyfikacji konkretnego obwodu, na każdym rysunku wklejono wyciętą z rysunku 99, odpowiednią etykietkę mierzonego obwodu. Przedstawione w tym rozdziale przykładowe proste pomiary, wykonane z wykorzystaniem podstawowej wersji przyrządu nanoVNA, mają za zadanie przede wszystkim pomóc Czytelnikowi w zdobyciu wprawy w prawidłowej konfiguracji mierzonych charakterystyk (dobór parametrów, skal i zakresów ich prezentacji oraz pracy z markerami) i dlatego nie będą tu głębiej analizowane.

Pomiary dwójników. Anteny, sztuczne obciążenia i rezonatory kwarcowe

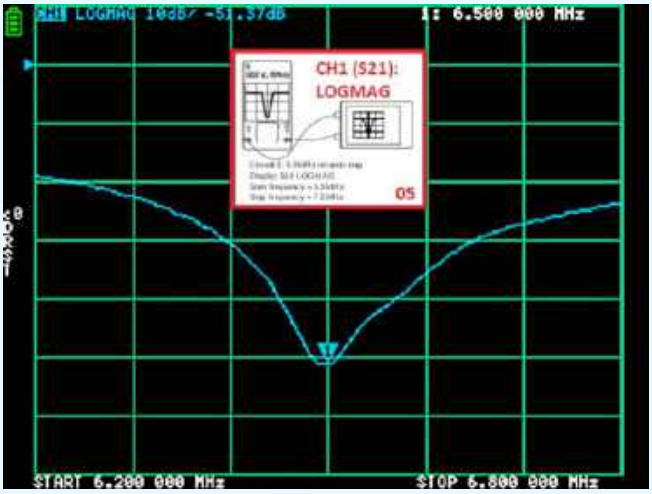
W ramach pomiarów dwójników w pierwszej kolejności pod lupę wzięto fabryczne anteny na pasma HF, VHF oraz UHF. Na **fotografii 24**



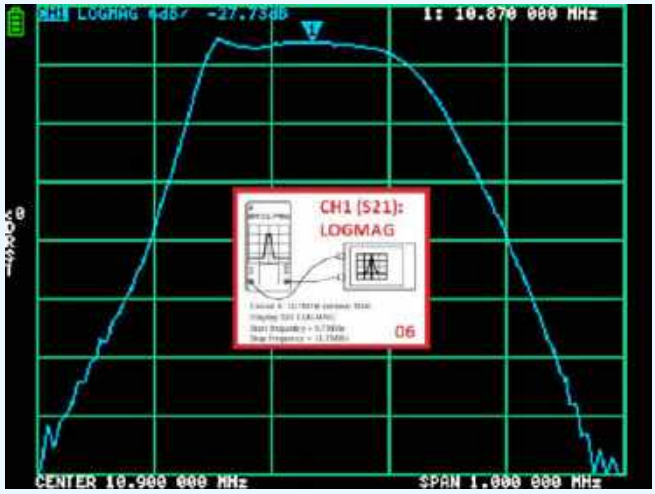
Rysunek 100. Rezultaty pomiarów obwodu nr 1 na płytce RF Demo-Kit



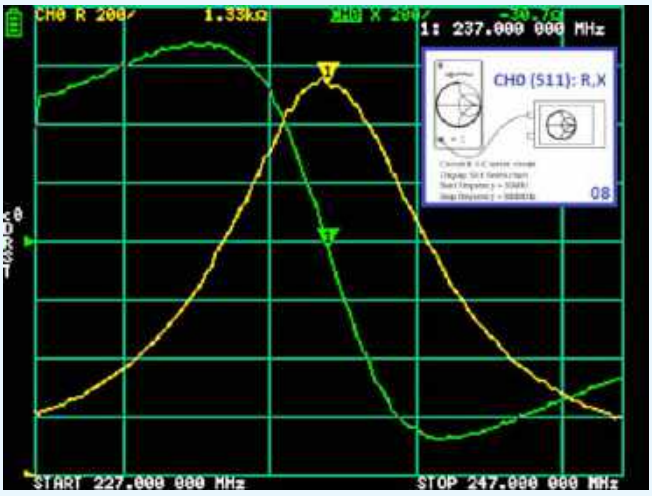
Rysunek 101. Rezultaty pomiarów obwodu nr 2 na płytce RF Demo-Kit



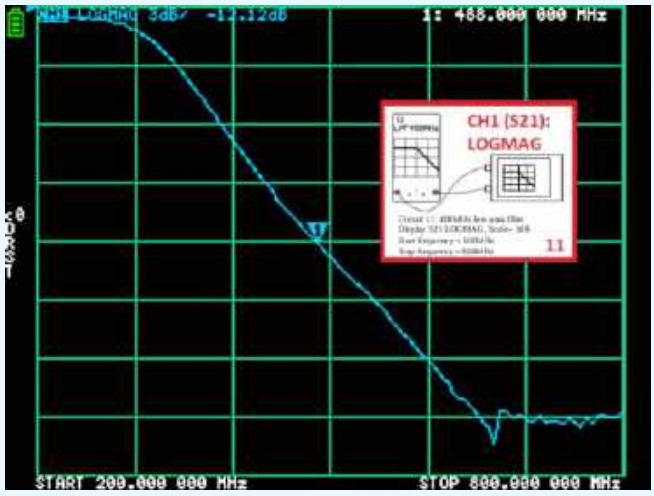
Rysunek 102. Rezultaty pomiarów obwodu nr 5 na płytce RF Demo-Kit



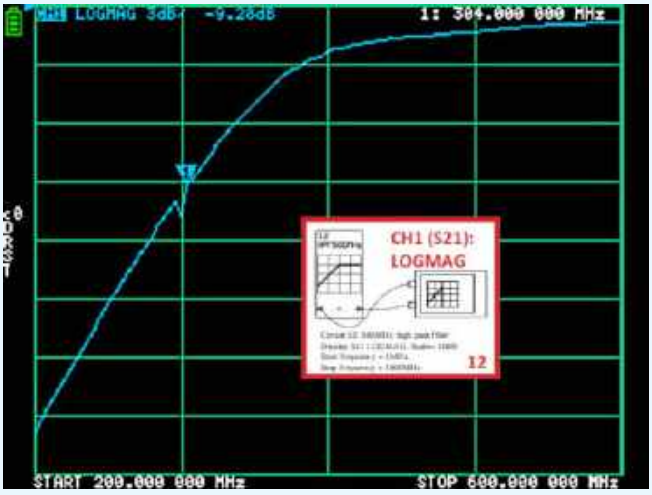
Rysunek 103. Rezultaty pomiarów obwodu nr 6 na płytce RF Demo-Kit



Rysunek 104. Rezultaty pomiarów obwodu nr 8 na płytce RF Demo-Kit

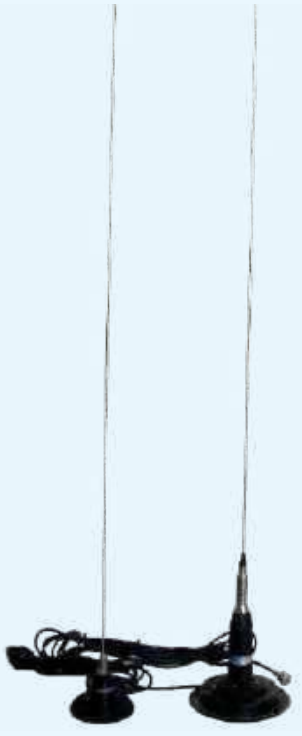


Rysunek 105. Rezultaty pomiarów obwodu nr 11 na płytce RF Demo-Kit

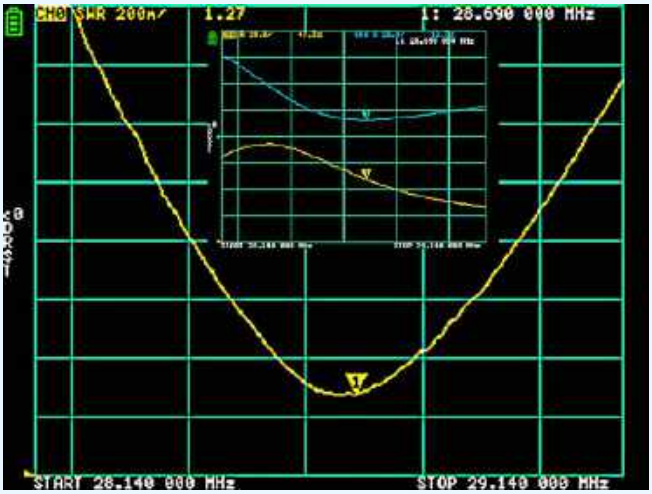


Rysunek 106. Rezultaty pomiarów obwodu nr 12 na płytce RF Demo-Kit

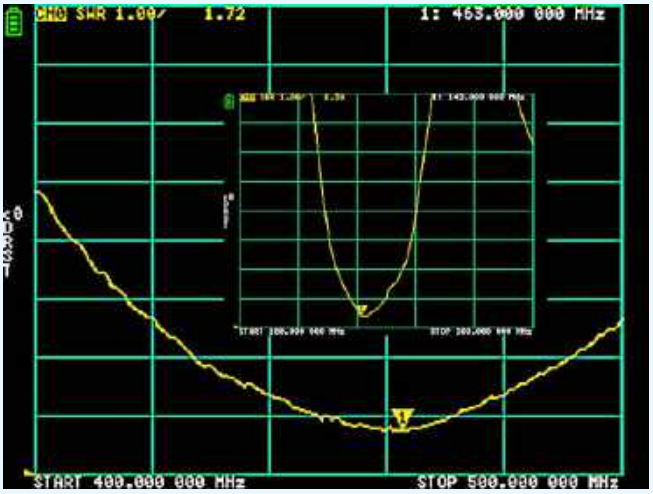
zaprezentowano dwie samochodowe (z podstawami magnetycznymi), pionowe anteny na podpasmo CB pasma KF – często określane jako 27 MHz lub pasmo 11 metrów. CB Radio (ang. *Citizens Band*) jest formą amatorskiej radiokomunikacji analogowej, wykorzystującej tzw. pasmo obywatelskie, które w Polsce i w większości Europy obejmuje zakres od 26,960 MHz do 27,400 MHz. Do pracy z emisjami AM lub FM z maksymalną mocą nadawaną do 4 W i przy użyciu fabrycznie homologowanych transceiverów nie jest wymagane posiadanie licencji radiooperatora. Kluczowe parametry krótszej i prostszej konstrukcyjnie (po lewej stronie na fotografii 24) anteny markowanej HUSTLER pokazano na skonsolidowanym **rysunku 107** (obie składowe impedancji zespolonej Z=R+jX oraz współczynnik fali stojącej SWR). Jak wynika z obu wykresów, omawiana antena ma rezonans (R≈50 Ω, X≈0j Ω, SWR≈1) w okolicach częstotliwości Frez=28,6 MHz, czyli całkiem daleko poza polskim pasmem częstotliwości CB Radia i teoretycznie wymaga ona podstrojenia na drodze regulacji długości wysuniętego promiennika. Jakkolwiek należy w tym miejscu wyjaśnić, że przedmiotowa antena (podobnie jak i inne dyskutowane dalej



Fotografia 24. Testowane anteny CB: HUSTLER i SIRIO ML-145



Rysunek 107. Wykresy parametrów SWR, R i X anteny CB HUSTLER



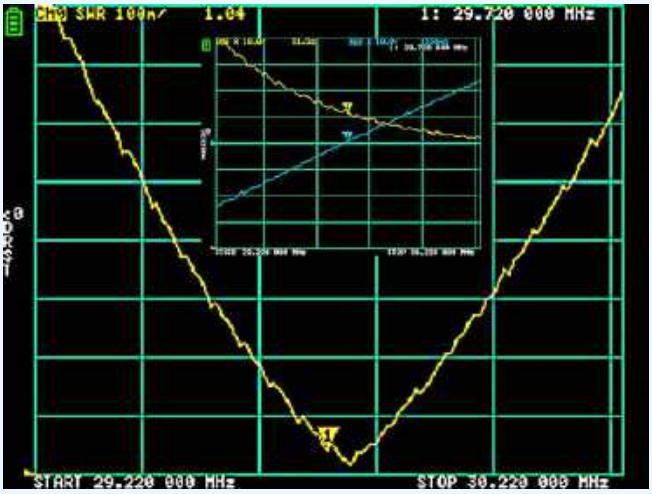
Rysunek 109. Wykresy parametrów SWR dla pasm VHF/UHF standardowej anteny do radiotelefonu ręcznego

„samochodówki") była mierzona po postawieniu na podstawie wykonanej z dwustronnie pokrytego miedzią laminatu szklano-epoksydowego o wymiarach około 50×50 cm, który nie był odpowiednio uziemiony w warunkach domowych. Tymczasem taka antena samochodowa powinna zostać zestrojona i pomierzona w rzeczywistych warunkach eksploatacji, tzn. na dachu auta, z którym będzie użytkowana, a nawet w konkretnym jego miejscu. Zatem zebrane tutaj wnioski o nieprawidłowym zestrojeniu omawianej anteny w praktyce eksploatacyjnej mogą okazać się w co najmniej znacznym stopniu nietrafione. Z kolei po prawej stronie na fotografii 24 ukazano markową antenę typu SIRIO ML-145, która jest dłuższa i bardziej zaawansowana konstrukcyjnie (m.in. dzięki wbudowanej w połowie długości promiennika, dodatkowej cewce wydłużającej go elektrycznie) od omówionej powyżej anteny HUSTLER. Skonsolidowany **rysunek 108** także prezentuje parametry Z=R+jX oraz SWR. Rezonans tej anteny wypada w pobliżu częstotliwości Frez=29,7 MHz, czyli jeszcze dalej od dozwolonego pasma częstotliwości CB niż w przypadku poprzedniczki. Jednak także w tym przypadku ponownie mają zastosowanie uwagi odnośnie do prawidłowych, realnych warunków dostrajania i pomiarów anten samochodowych.

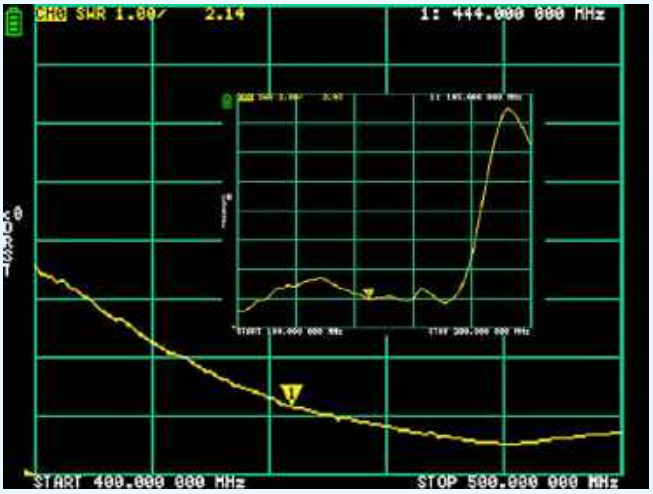
W dalszych krokach pomierzono dwie anteny mobilne na pasma VHF (144 MHz/2 m) oraz UHF (433 MHz/70 cm), dedykowane do pracy z dwupasmowym, ręcznym radiotelefonem typu BAOFENG UV-5R. Zostały one pokazane na **fotografii 25** – od lewej: wydłużona antena dodatkowa typu „DIAMOND RH901S" oraz krótka antena będąca standardowym wyposażeniem wzmiankowanego ręcznego duobandera. Zaaranżowane warunki pomiarowe były dobrze zbliżone do rzeczywistych warunków eksploatacji tych anten. Na skonsolidowanym **rysunku 109** zilustrowano przebiegi współczynnika SWR krótkiej anteny standardowej (osobno w pasmach VHF oraz UHF), które w obu przypadkach, w użytecznych zakresach pasma, plasuje się pomiędzy wartościami 1,5 a 2,0. Należy uznać je za całkiem satysfakcjonujące wobec bardzo niewielkich gabarytów badanej, wysoce „kompromisowej" anteny. Z kolei na skonsolidowanym **rysunku 110** zobrazowano wartości parametru SWR dla elastycznej anteny DIAMOND RH901S (alternatywa dla ww. antenki standardowej) w obu rozpatrywanych pasmach częstotliwości. Paradoksalnie są one istotnie gorsze od osiągów króciutkiej antenki standardowej, bo oscylują w przedziale pomiędzy 2,0 a 3,0. Jakkolwiek finalną atrakcyjność użytkową drugiej z tych anten powinien poprawiać jej istotnie lepszy zysk kierunkowy promieniowania względem anteny standardowej.

W następnej kolejności dokonano pomiarów pokazanej na **fotografii 26** pary samochodowych anten VHF/UHF (od lewej: NAGOYA NL-770R, obok DIAMOND SMA-F UT106UV). Skonsolidowany **rysunek 111** ukazuje przebiegi współczynnika SWR

Fotografia 25. Testowane anteny VHF/UHF do radiotelefonu ręcznego



Rysunek 108. Wykresy parametrów SWR, R i X anteny CB SIRIO ML-145



Rysunek 110. Wykresy parametrów SWR dla pasm VHF/UHF anteny DIAMOND RH901S

Poprzednie części kursu i dodatkowe materiały dostępne są na stronie
https://ulubionykiosk.pl/media

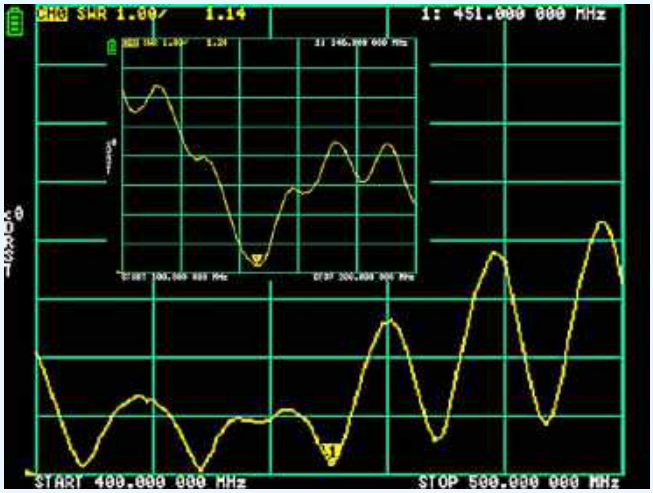
pierwszej z nich w pasmach VHF i UHF. W przypadku obu użytecznych zakresów tych pasm SWR leży znacznie poniżej wartości 1,5, co należy uznać za bardzo dobry rezultat. Z kolei na skonsolidowanym **rysunku 112** przedstawiono przebiegi współczynnika SWR dla drugiej anteny. Są one wyraźnie gorsze od osiągów wcześniej omówionego produktu (wartości poniżej 2,0) – wyjaśnia to uproszczona, wręcz miniaturowa i bardzo „ekonomiczna" konstrukcja tej anteny.

Fotografia 26. Testowane samochodowe anteny VHF/UHF

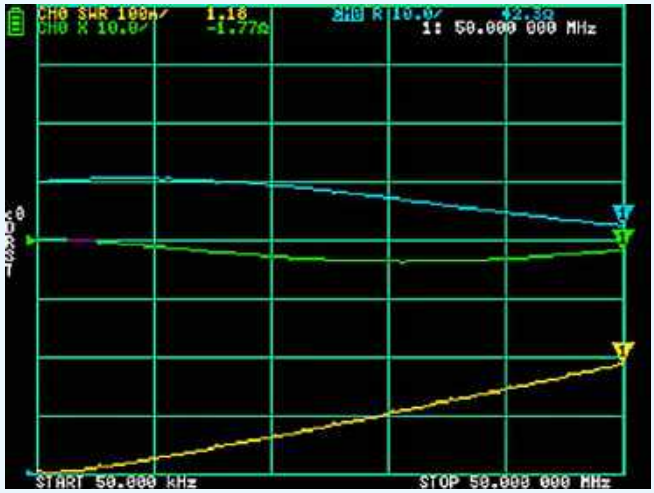
Na **fotografii 27** pokazano dwa wykonania sztucznych obciążeń rezystancyjnych 50 Ω, przeznaczonych do pracy w pasmie HF (KF – praktycznie do około 30 MHz). Były one prezentowane przed kilku laty na łamach „Elektroniki Praktycznej" jako projekty AVT3210/1 oraz AVT3210/2. Bazują one na połączeniach znacznej liczby połączonych równolegle, zwykłych rezystorów o dopuszczalnych mocach strat 0,25 W i nadają się do pracy

Fotografia 27. Sztuczne obciążenia AVT3210/1 i AVT3210/2

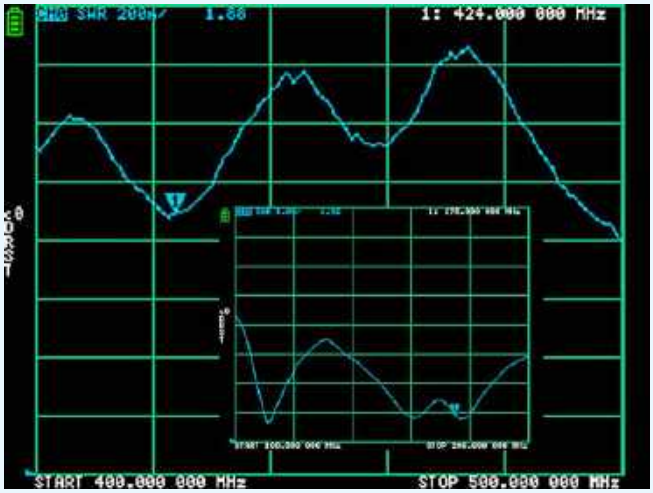
z ciągłymi i szczytowymi mocami strat odpowiednio 5 W i 10 W oraz 10 W i 20 W, czyli praktycznie wyłącznie do testowania urządzeń nadawczych QRP (bardzo małej i małej mocy). Pierwsze z obciążeń ma wbudowany prosty, diodowy detektor szczytowy napięcia na obciążeniu, natomiast drugi wyposażono w progowy detektor chwilowej mocy szczytowej ze wskaźnikiem w postaci ciągu diod LED. Ograniczenie stosowalności obu tych przyrządów do pasma KF wynika z niedostatecznie zwartej konstrukcji, w której dodatkowo nie zastosowano rezystorów bezindukcyjnych. Potwierdzają to pomiary parametrów Z=R+jX oraz SWR pokazane na **rysunkach 113** i **114**. W szczególności, wyraźnie lepsze własności wykazuje



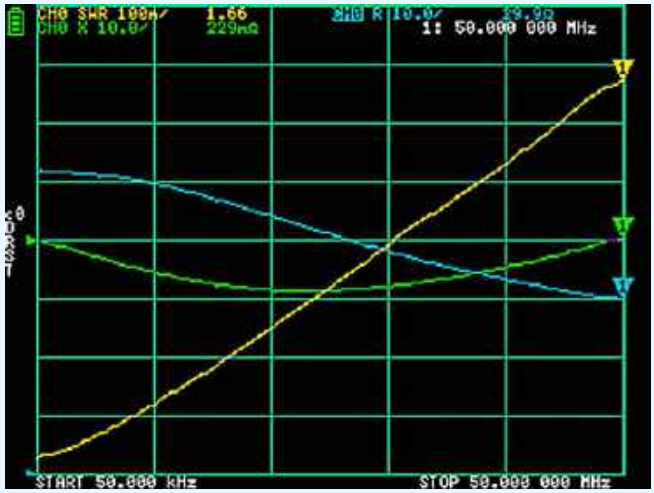
Rysunek 111. Wykresy parametrów SWR dla pasm VHF/UHF anteny NAGOYA NL-770R



Rysunek 113. Wykresy parametrów SWR, R i X sztucznego obciążenia AVT3210/1

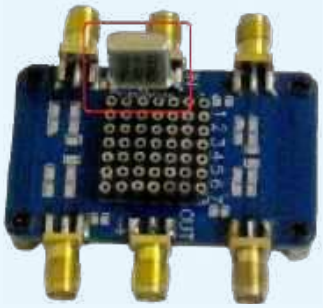


Rysunek 112. Wykresy parametrów SWR dla pasm VHF/UHF anteny DIAMOND SMA-F UT106UV



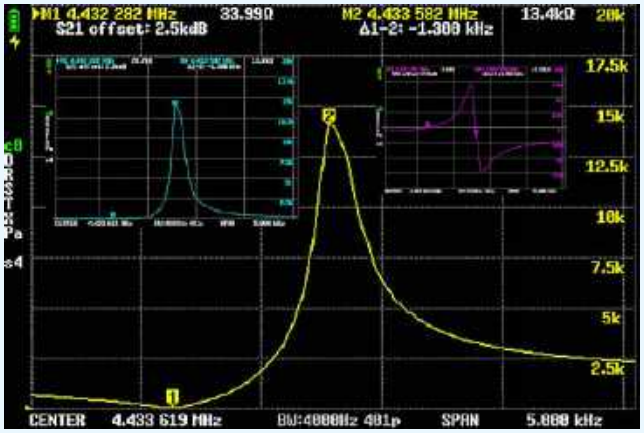
Rysunek 114. Wykresy parametrów SWR, R i X sztucznego obciążenia AVT3210/2

mniejszy i bardziej zwarty układ AVT3210/1, w którym zastosowano istotnie prostszą sieć połączeń równoległych rezystorów, a także nie występuje w nim dość znaczne obciążenie układu właściwego nieliniowym blokiem pomiarowym o niezerowych parametrach reaktancyjnych.

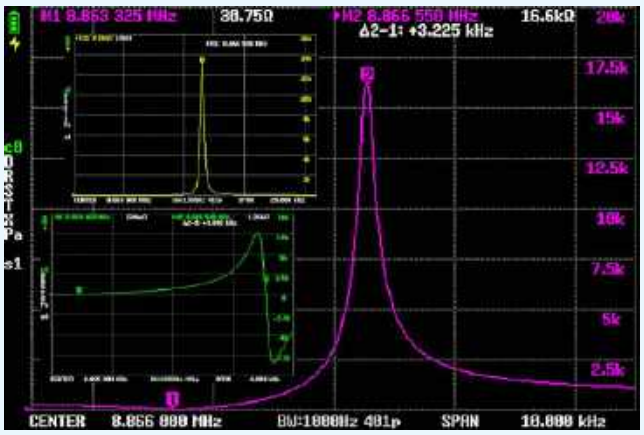


Fotografia 28. Rezonator kwarcowy w dedykowanej podstawce pomiarowej

Grupę pomiarów częstotliwościowych charakterystyk dwójników liniowych zamyka przegląd własności dwóch grup rezonatorów kwarcowych (po 10 sztuk w każdej grupie) o częstotliwościach charakterystycznych (oznaczonych na obudowach elementów) równych 4,433619 MHz oraz 8,867238 MHz. **Fotografia 28** przedstawia jeden z wymienionych kwarców osadzony na specjalnej podstawce, przeznaczonej właśnie do pomiarów tego typu elementów. Niewidoczny na zdjęciu układ połączeń pomiędzy poszczególnymi polami połączeniowymi (stykowymi) płytki umożliwia zestawianie na niej nieco bardziej złożonych konfiguracji połączeń, np. polegających na dodaniu innych elementów dołączonych do głównego komponentu szeregowo bądź równolegle (do masy). Skonsolidowane **rysunki 115** i **116** prezentują pełne charakterystyki Z=R+jX (|Z|, R, X) pomierzonych reprezentantów obu grup kwarców, umieszczone na pojedynczych rycinach. Na obu wykresach |Z| markerami wyróżniono lokacje rezonansów: szeregowego i równoległego. Dla obu grup rezonatorów powtarzalność parametrów w ramach danej grupy okazała się zaskakująco dobra (rozbieżności na poziomie tylko ±10 Hz), a różnice pomiędzy częstotliwościami obu rezonansów Fpar-Fser na poziomie pojedynczych kHz nieźle rokowały na zastosowanie przedmiotowych rezonatorów w pasmowych filtrach kwarcowych p.cz. [5], stosowanych do formułowania lub wyodrębnienia zmodulowanego sygnału jednowstęgowego SSB (ang. *Single Side Band*).



Rysunek 115. Wykresy parametrów SWR, R i X rezonatora kwarcowego 4,433 MHz

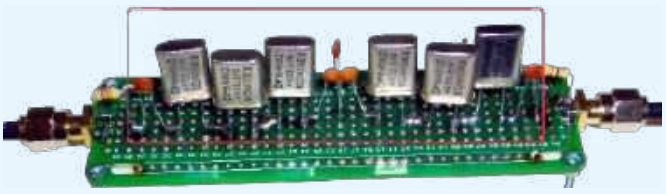


Rysunek 116. Wykresy parametrów SWR, R i X rezonatora kwarcowego 8,867 MHz

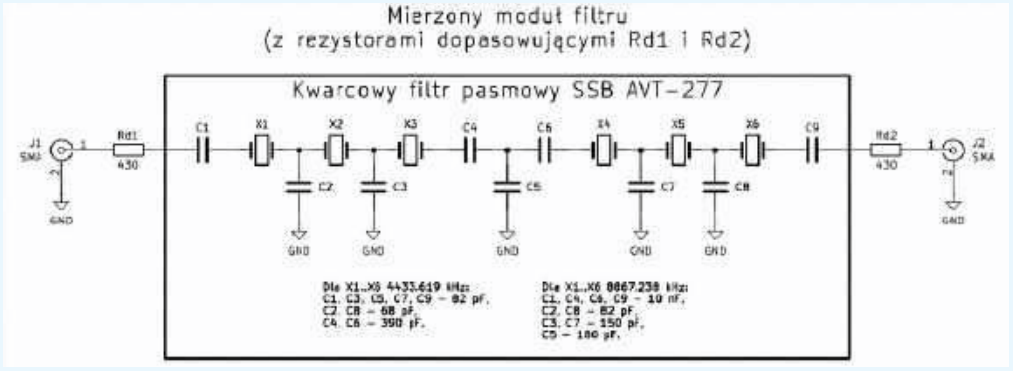
Pomiary czwórników Filtry, wzmacniacze i tłumiki

Dla zwiększenia przejrzystości przekazu (bez utraty jego ciągłości narracji) przejdziemy teraz płynnie do omówienia charakterystyk filtrów kwarcowych SSB, zbudowanych w oparciu o rezonatory kwarcowe – przebadane, a następnie omówione na końcu poprzedniego rozdziału. Na **rysunku 117** pokazano schemat układów badanych filtrów SSB oraz podano rekomendowane wartości elementów, zaś na **fotografii 29** zilustrowano jeden z wykonanych dwóch prototypów. Filtry zostały wykonane wg projektu opisanego w [6]. Z założenia projekt ten miał umożliwić skuteczną i stosunkowo łatwą implementację filtrów kwarcowych, pozbawioną uciążliwego i kosztownego: mierzenia, wyznaczania szczegółowych parametrów, a – ostatecznie – dobierania konkretnych rezonatorów z całkiem dużej grupy (do kilkudziesięciu sztuk) elementów o zbliżonych parametrach. Ponieważ deklarowane impedancje: wejściowa i wyjściowa badanych filtrów powinny być zbliżone do 500 Ω, na modelowym schemacie filtru uwzględniono dopasowujące rezystancje szeregowe Rd1=Rd2=430 Ω. Uzupełniają one oporności 50 Ω zarówno źródła sygnału pomiarowego, jak i wejścia pomiarowego przyrządu, obciążającego wyjście filtru. Oczywiście w konsekwencji zmierzony sygnał wyjściowy był mniejszy od oczekiwanego o wartość tłumienia (wniesionego przez dzielniki oporowe, powstałe na wejściach i wyjściach badanych filtrów) na poziomie około:

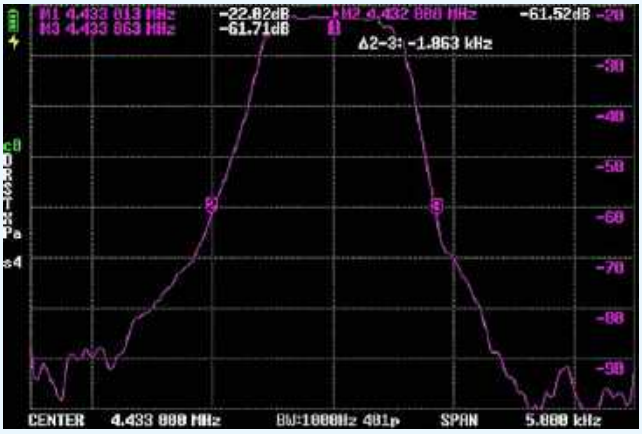
$$[500\ \Omega/(50\ \Omega+430\ \Omega+500\ \Omega)]\cdot[500\ \Omega/(500\ \Omega+430\ \Omega+50\ \Omega)]\approx 0{,}5102\cdot 0{,}05102\approx 0{,}026$$



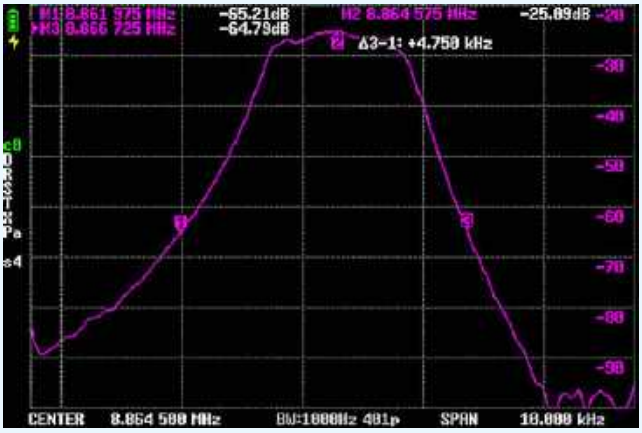
Fotografia 29. Prototyp jednego z badanych filtrów SSB



Rysunek 117. Schemat układów badanych filtrów kwarcowych SSB



Rysunek 118. Charakterystyki częstotliwościowe tłumienności filtru SSB na częstotliwość 4,433 MHz



Rysunek 119. Charakterystyki częstotliwościowe tłumienności filtru SSB na częstotliwość 8,866 MHz

Po uwzględnieniu wewnętrznej korekty przyrządu pomiarowego na pomiar w warunkach dopasowania 50 Ω:

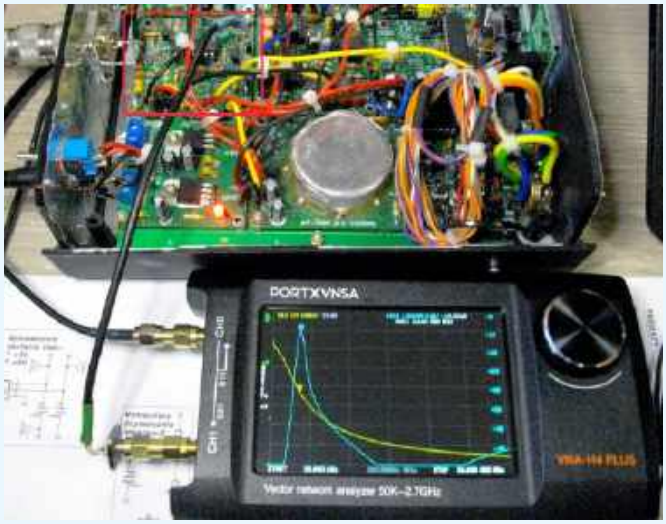
(x·2·2=x·4)

otrzymujemy wyniki pomiaru pomniejszone o około 20·log10(0,026·4) czyli 19,65 dB.

Taką właśnie poprawkę należy uwzględnić, analizując charakterystyki częstotliwościowe tłumienności pokazane na **rysunkach 118** i **119**. Rysunek 118 prezentuje uzyskaną charakterystykę filtru SSB opartego na sześciu niemal identycznych rezonatorach o częstotliwościach charakterystycznych równych 4,433619 MHz. Jak widać, tłumienie –40 dB względem środka pasma przepustowego tego filtru wyznacza jego zakres przenoszenia na jedynie około 1,9 kHz (czyli dość mało). Z kolei w przypadku wykonania filtru opartego na rezonatorach na częstotliwości 8,867238 MHz, analogiczne pasmo wynosi aż około 4,8 kHz (to znów nieco za dużo).

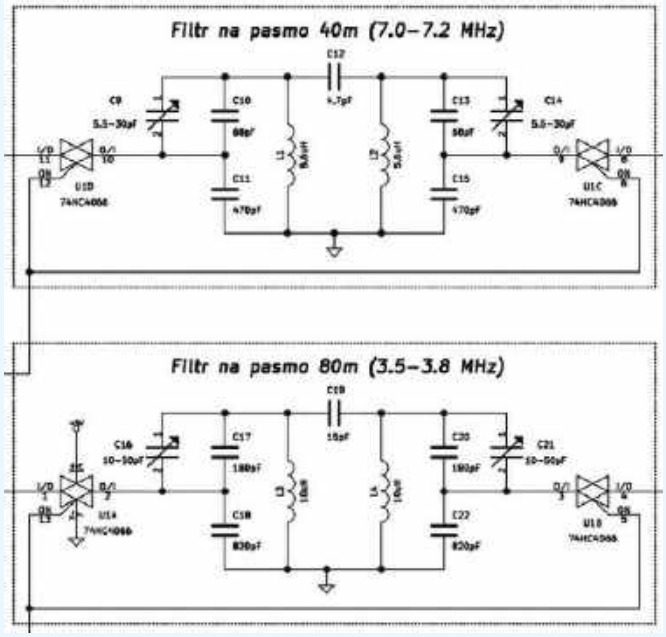
Doświadczenie praktyczne autora podpowiada tu, że pierwszy z filtrów może być ciekawą propozycją dla prostej konstrukcji jednopasmowego transceivera na pasmo 80 m – pracującego wyłącznie z pojedynczą, dolną wstęgą LSB (ang. *Lower Side Band*). Natomiast drugi filtr, z racji lokacji pasma przepustowego w bliskiej okolicy częstotliwości 9 MHz (bardzo chętnie wybieranej na p.cz. w prostych wielopasmowych transceiverach SSB z pojedynczą przemianą) oraz potencjalnej możliwości dalszego zawężania pasma audio sygnału SSB już w torze m.cz., wydaje się mieć nieco większy potencjał na potrzeby trochę ambitniejszych i bardziej rozbudowanych konstrukcji urządzeń radiokomunikacyjnych na pasma KF.

Niejako kontynuując tematykę konstrukcji radioamatorskich na pasma KF, autor pokusił się o pomiar „in vitro" filtrów pasmowych w.cz. na pasma 80 m oraz 40 m (**fotografia 30**)

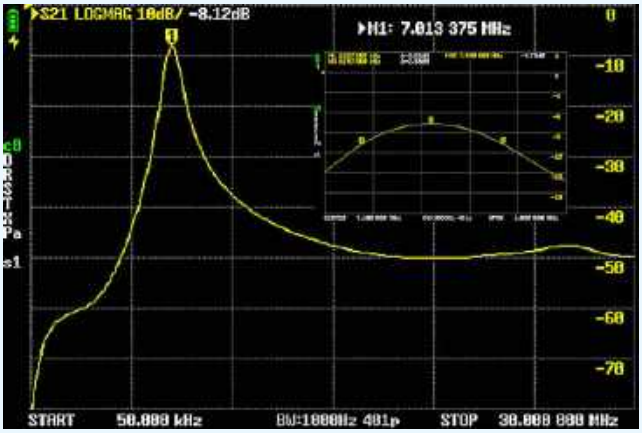


Fotografia 30. Moduł filtrów pasmowych LC w „RX Dosia" podczas pomiarów

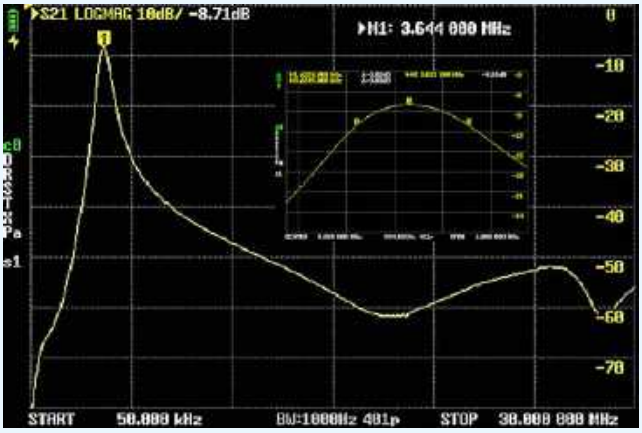
wg własnego projektu z odbiornika nasłuchowego KF „Dosia" [7]. Szczególnie intrygujące było to, czy filtry zaimplementowane i zestrojone przed niemal dziesięcioma laty nadal utrzymują wymagane parametry. Na **rysunku 120** przedstawiono fragment schematu modułu AVT3190, kluczowy z punktu widzenia kształtowania pasma przedmiotowego odbiornika, czyli strojone obwody selektywne LC. W praktyce ich pomiar objął pełny odcinek od wejścia antenowego odbiornika aż do (czasowo odłączonego od reszty urządzenia) wyjścia modułu filtrów. Oczywiście, pozostawiono aktywne i załączone, pełne zasilanie badanego modułu (+5 VDC/+9 VDC) oraz sterowanie cyfrowo-analogowym selektorem pasma 40 m/80 m. Skonsolidowane **rysunki 121** i **122** ilustrują charakterystyki przenoszenia przedmiotowych filtrów LC. Z rysunku 121 wynika, że filtr na pasmo 40 m co prawda obejmuje wymagany zakres 7,0...7,2 MHz i to całkiem skutecznie, bo na poziomie lepszym niż –40 dB, eliminuje wszelkie sygnały z pasma KF, jednak z dość znacznym zapasem (faktyczna szerokość zmierzonego pasma przepustowego to niemal 600 kHz przy spadku transmitancji o około –3 dB). Z kolei rysunek 122 pokazuje, że filtr na pasmo 80 m obejmuje wymagane pasmo 3,5...3,8 MHz i zapewnia tłumienie pozapasmowe dla fal krótkich znacznie lepsze niż –40 dB ze względnie



Rysunek 120. Fragment schematu filtrów pasmowych LC z „RX Dosia"



Rysunek 121. Charakterystyki przenoszenia filtru LC z „RX Dosia" na pasmo 40 m



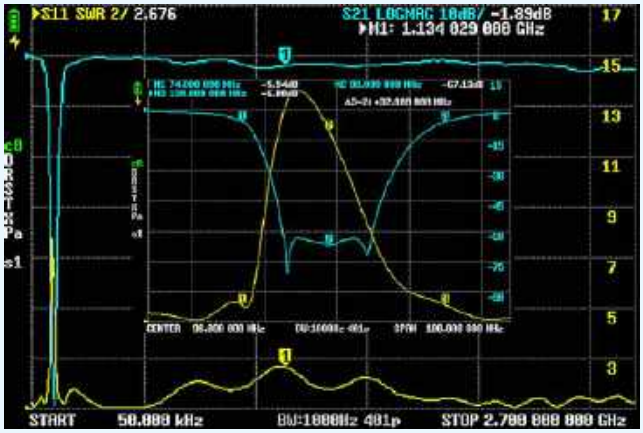
Rysunek 122. Charakterystyki przenoszenia filtru LC z „RX Dosia" na pasmo 80 m

niewielkim zapasem 3-decybelowego pasma przenoszenia, którego szerokość wyniosła około 450 kHz. Wnioski są takie, że oba przebadane filtry pasmowe LC niezmiennie zachowują przyzwoite walory użytkowe – zwłaszcza jak na potrzeby prostego odbiornika nasłuchowego – i nie jest niezbędna ich optymalizacja, która zapewne musiałaby prowadzić do poważniejszych zmian układowych.

Zestawienie pomiarów biernych filtrów pasmowych w.cz. zamykają dwa pokazane na **fotografiach 31** i **32** filtry przeciwzakłóceniowe. Pierwszy z nich to pasmowo-zaporowy filtr dedykowany do blokowania zakłóceń od silnych, rozsiewczych stacji radiowych UKF/FM na wejściu wysokoczułych, szerokopasmowych odbiorników SDR. Deklarowane parametry filtru to:

Fotografia 31. Filtr pasmowozaporowy na pasmo radiowe FM

Fotografia 32. Filtr pasmowoprzepustowy na pasmo 433 MHz

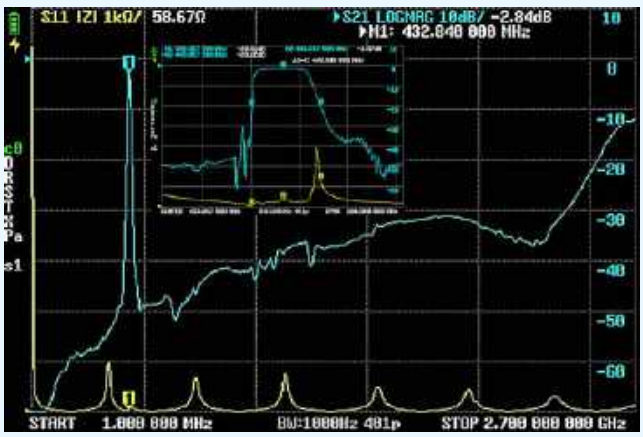


Rysunek 123. Charakterystyki przenoszenia filtru pasmowozaporowego na pasmo radiowe FM

- zakres częstotliwości roboczej: 88...108 MHz,
- impedancja charakterystyczna: 50 Ω,
- tłumienność w pasmie przenoszenia: <1 dB,
- tłumienność w pasmie blokowania (76...120 MHz): ≥50 dB,
- maksymalna moc wejściowa: +30 dBm (1 W).

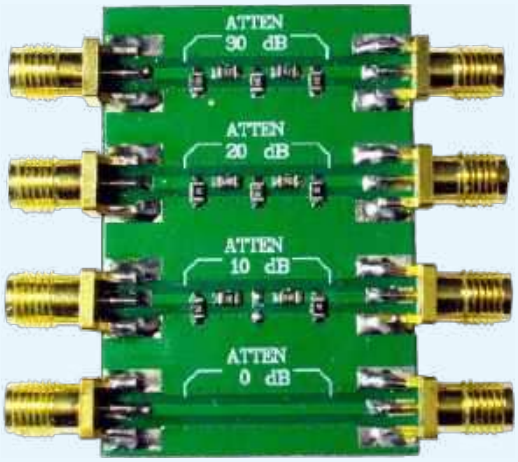
Na skonsolidowanym **rysunku 123** pokazano, że przebadany filtr zaporowy FM spełnia postawione przed nim wymagania w zakresie tłumienności, całkiem przyzwoicie zachowuje się też współczynnik SWR, który jest stabilnie mniejszy od 2,0 w zakresie przenoszenia, co najmniej aż do około 700 MHz. Z kolei drugi z badanych tu przyrządów to pasmowoprzepustowy filtr blokujący sygnały spoza pasma 70 m o częstotliwości roboczej 433 MHz ±20 MHz, impedancji wejściowej i wyjściowej 50 Ω, tłumienności w pasmie przepustowym <1,5 dB, tłumienności w pasmie blokowania ≥45 dB (w odległości ≥50 MHz od środka pasma przepustowego) i maksymalnej mocy wejściowej +13 dBm (20 mW). Skonsolidowany **rysunek 124** wskazuje na to, że zbadany filtr wypełnia deklarowane parametry w zakresie tłumienności poza pasmem przepustowym, które jednak nie przekracza ±15 MHz, a impedancja wejściowa w tym pasmie jest dość nierównomierna i miejscami wyraźnie przekracza deklarowane 50 Ω. Podane informacje definiują zatem ten filtr bardziej jako układ odbiorczy o nieco ograniczonych zastosowaniach.

Osobną rodziną czwórników są tłumiki, dzięki którym można osłabić zbyt silny sygnał sterujący, by nie przesterować wejścia kolejnego bloku w torze przetwarzania sygnału – np. wzmacniacza, mieszacza lub ustroju pomiarowego. W ramach przeprowadzonych testów przebadano dwa tego typu podzespoły: poczwórny tłumik stały (**fotografia 33**) o dostępnych wartościach tłumienia: 0/10/20/30 dB (z możliwością dowolnego łączenia w szereg) oraz tłumik regulowany cyfrowo (**fotografia 34**) o 64 stopniach regulacji

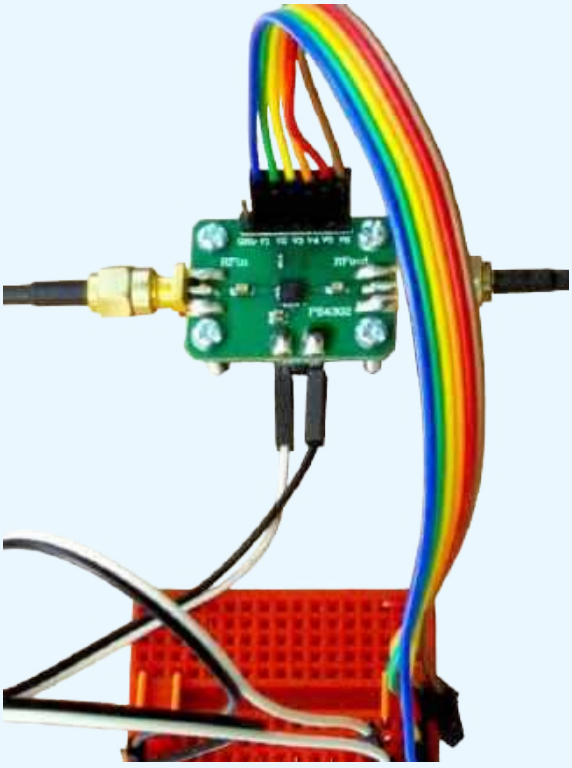


Rysunek 124. Charakterystyki przenoszenia filtru pasmowoprzepustowego na pasmo 433 MHz

Poprzednie części kursu i dodatkowe materiały dostępne są na stronie **https://ulubionykiosk.pl/media**



Fotografia 33. Tłumik stały 0/10/20/30 dB

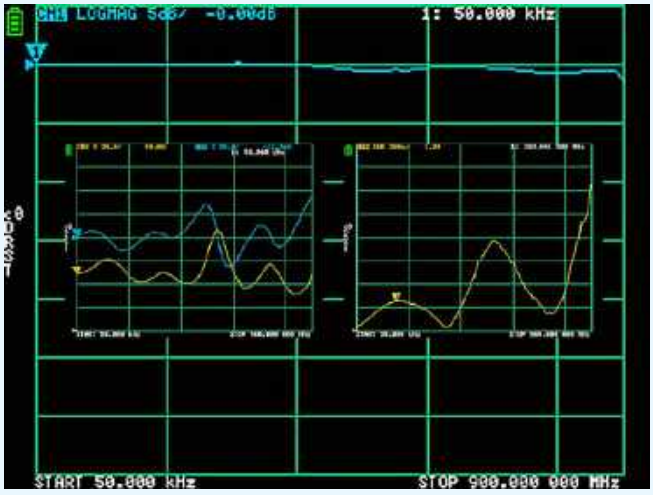


Fotografia 34. Tłumik regulowany z układem scalonym PE4302

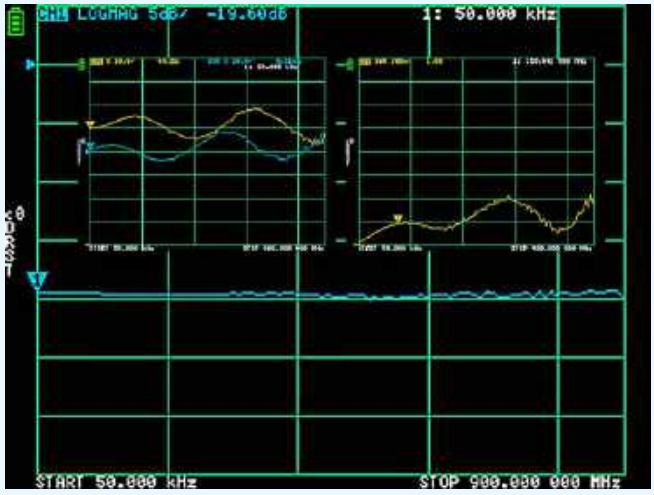
z krokiem 0,5 dB w zakresie dynamiki od 0 do 31,5 dB. Deklarowane parametry tłumika stałego, to:

- pasmo robocze: 0...4,0 GHz,
- maksymalna moc odbierana: 23 dBm (200 mW),
- WFS: ≤1,20 w całym dozwolonym pasmie pracy,
- dostępne wartości tłumienia: 0 dB (odniesienie), 10±0,8 dB, 20±1,1 dB, 30±1,0 dB.

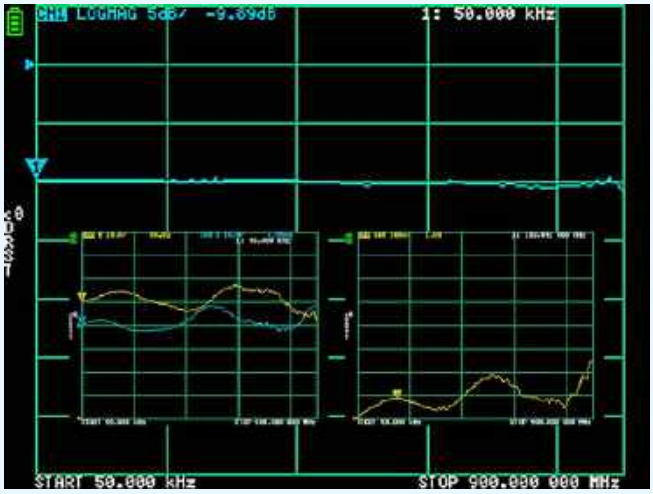
Na skonsolidowanych **rysunkach 125...128** pokazano przebiegi tłumienia w funkcji częstotliwości (w zakresie



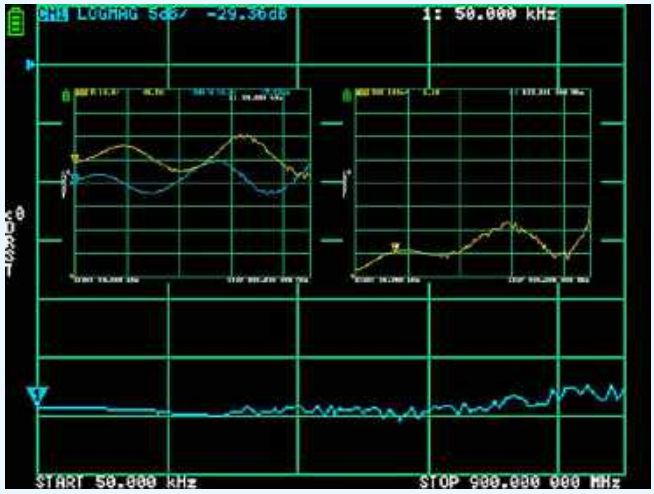
Rysunek 125. Charakterystyki częstotliwościowe: tłumienności, SWR oraz R i X tłumika stałego przy A=0 dB



Rysunek 127. Charakterystyki częstotliwościowe: tłumienności, SWR oraz R i X tłumika stałego przy A=20 dB

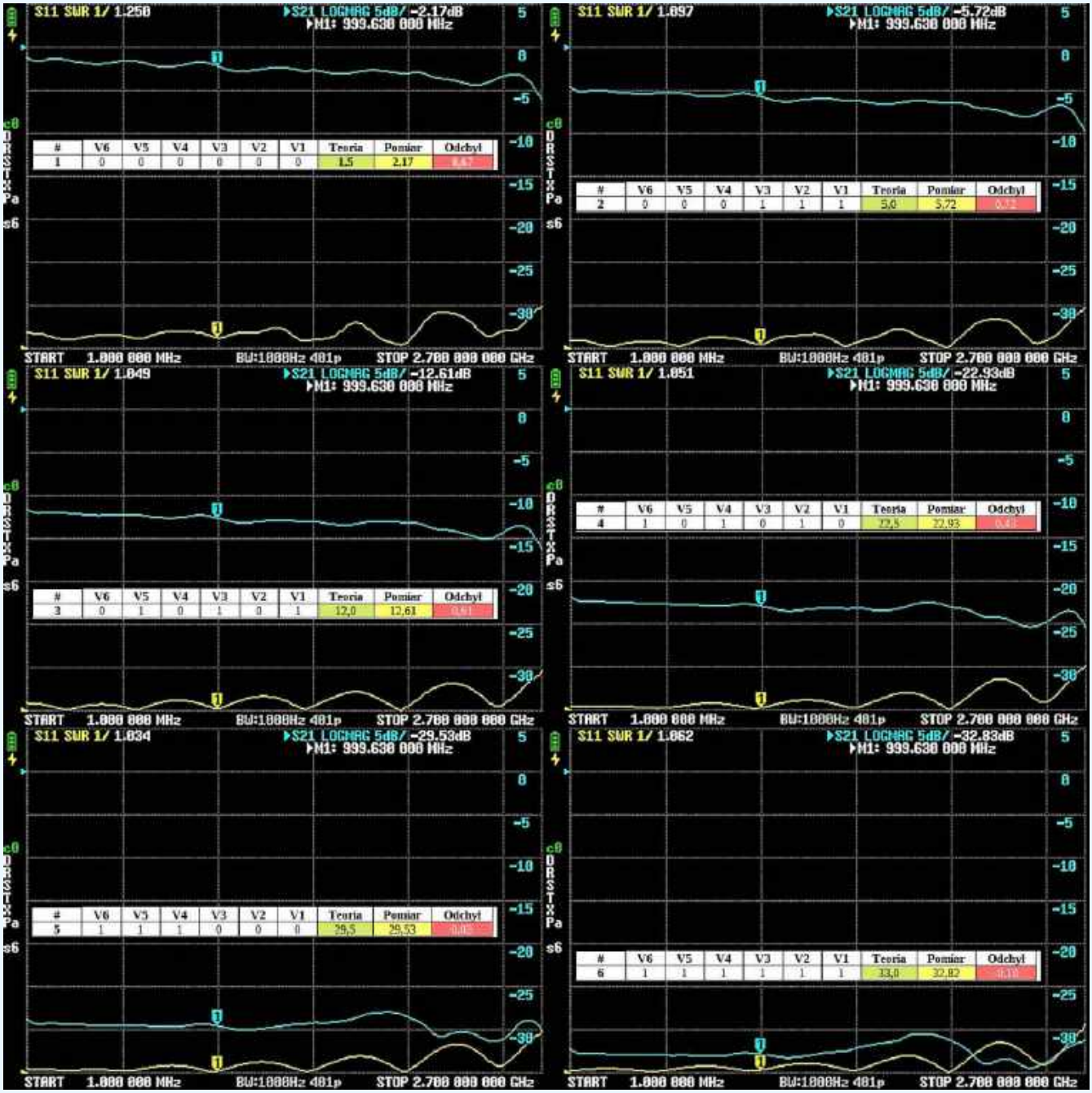


Rysunek 126. Charakterystyki częstotliwościowe: tłumienności, SWR oraz R i X tłumika stałego przy A=10 dB



Rysunek 128. Charakterystyki częstotliwościowe: tłumienności, SWR oraz R i X tłumika stałego przy A=30 dB

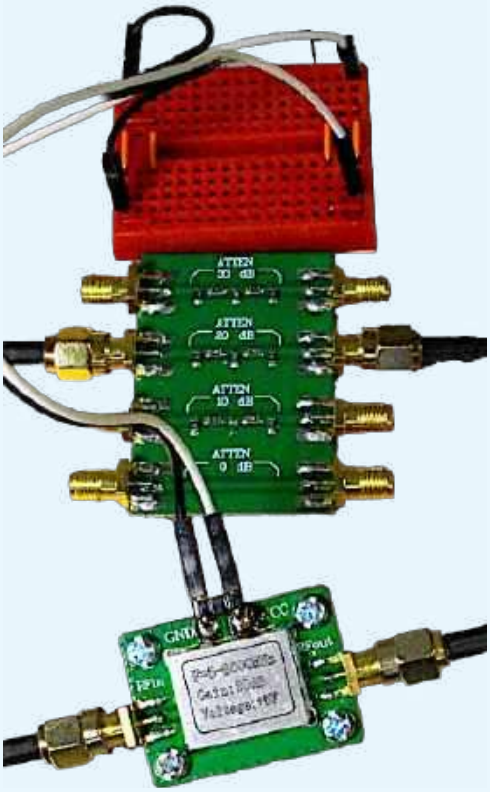
Poprzednie części kursu i dodatkowe materiały dostępne są na stronie **https://ulubionykiosk.pl/media**



Rysunek 129. Charakterystyki częstotliwościowe tłumienności i SWR tłumika regulowanego z chipem PE4302

od 50 kHz do 900 MHz, dostępnym w podstawowej wersji analizatora nanoVNA), uzupełnione o pomniejszone wykresy współczynnika SWR oraz składowych R i X wejściowej impedancji zespolonej Z badanego tłumika. Wykresy sporządzono dla wszystkich czterech możliwych, elementarnych wartości tłumień. Nie wdając się nazbyt w szczegółowe dywagacje nad licznymi anomaliami zaprezentowanych charakterystyk, śmiało można stwierdzić, że przebadany zestaw tłumików stałych nie może pretendować do rangi tłumików wzorcowych: uzyskane parametry dość znacząco odbiegają od wartości deklarowanych i – co gorsza – trend ten nasila się wraz ze wzrostem częstotliwości pomiaru. Jakkolwiek, przyrząd ten można śmiało wykorzystywać jako skuteczne zabezpieczenie przed przesterowaniem wejść urządzeń zbyt czułych na dysponowany sygnał sterujący. Również z nienajlepszej strony zaprezentował się moduł tłumika regulowanego krokowo, oparty na układzie scalonym PE4302 produkcji Peregrine Semiconductor. Co prawda producent w nocie katalogowej układu (dostępnej w materiałach dodatkowych do tego kursu) wyczerpująco opisuje wszelkie niedoskonałości układu, jednak wydaje się, że uzyskane pomiarowo wartości odbiegają jeszcze nieco od wyznaczonych ram tolerancji. Na skonsolidowanym **rysunku 129** ujęto wykresy jego parametrów: tłumienia A [dB] oraz współczynnika SWR [1] na jego wejściu. Pomierzono je przyrządem nanoVNA-H4+ w maksymalnym dostępnym zakresie częstotliwości, tzn. od 50 kHz do 2,7 GHz. Układ zasilono stabilizowanym napięciem 3,0 V, a żądane tłumienie wypadkowe uzyskiwano poprzez ustawienie każdego ze sterujących pinów wejściowych oznaczonych V1...V6 w stanie logicznym niskim „0” (0 V) lub wysokim „1” (3,0 V). Załączenie danego pinu sterującego Vx w stan wysoki powinno wprowadzić do sumarycznego tłumienia wypadkowego A tłumienie cząstkowe A(Vx) wg schematu:

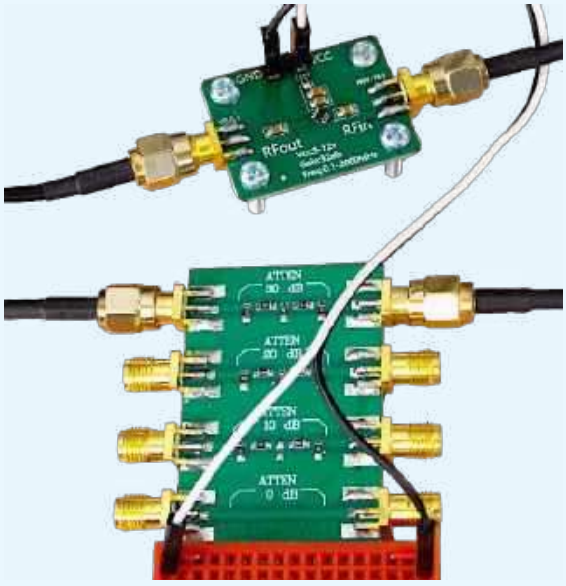
- A(V6)=16 dB,
- A(V5)=8 dB,
- A(V4)=4 dB,
- A(V3)=2 dB,
- A(V2)=1 dB,
- A(V1)=0,5 dB.



Fotografia 35. Wzmacniacz LNA 50...4000 MHz/20 dB

Do uzyskanej tą drogą wartości należało dodać stałą stratę wtrącenia, która wg deklaracji producenta nie powinna przekraczać 1,75 dB (typowo: 1,5 dB) w pasmie od 0 Hz do 2,2 GHz. Ponieważ trudno byłoby przetestować i zaprezentować przebiegi pomiarowe dla wszystkich możliwych 2^6=64 możliwych nastaw i w całym deklarowanym użytecznym pasmie częstotliwości roboczych, autor wybrał arbitralnie do analizy i prezentacji sześć nastaw, które w jego odczuciu znacząco różniły się zarówno uzyskiwanymi wartościami pożądanego tłumienia wypadkowego, jak i wzajemnymi konfiguracjami sąsiednich, pojedynczych bitów lub ich grup V6... V1. Zgrubne wnioski, wyciągnięte choćby już z tych wybiórczych pomiarów, są następujące: odchyłki uzyskanych nastaw od wartości teoretycznych (oczekiwanych) większe od minimalnego kroku regulacji raczej przekreślają badany moduł w zastosowaniach profesjonalnych, jakkolwiek użycie go w mniej wymagających aplikacjach półprofesjonalnych czy amatorskich (np. do analogowo-cyfrowej, automatycznej regulacji wzmocnienia w torze w.cz. – wstępnej, p.cz. – właściwej czy nawet m.cz. – uzupełniającej odbiornika radiokomunikacyjnego) wydaje się całkiem sensowne.

Rysunek 130. Charakterystyki częstotliwościowe tłumienia i SWR wzmacniacza LNA 50...4000 MHz/20 dB

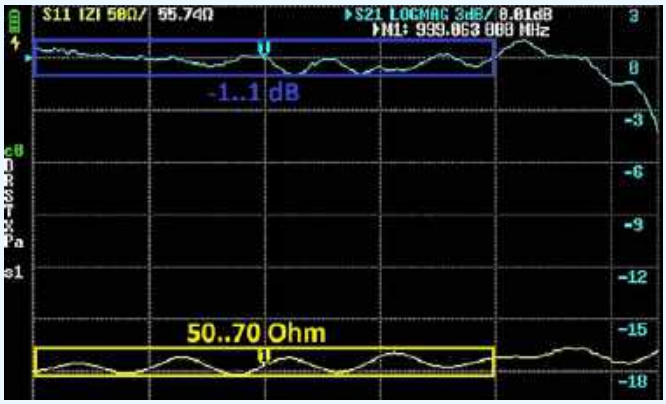


Fotografia 36. Wzmacniacz LNA 0,1...2000 MHz/30 dB

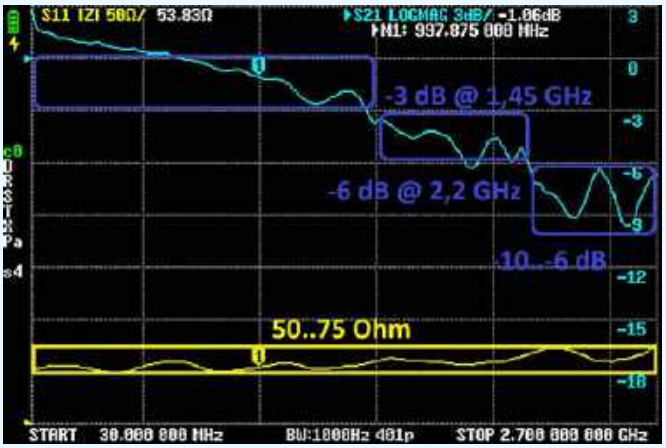
Ostatnią grupą testowanych czwórników były trzy miniaturowe wzmacniacze modułowe na pasma HF/VHF/UHF. Pierwszy z nich (**fotografia 35**) to niskoszumny wzmacniacz LNA (ang. *Low Noise Amplifier*) o bardzo dużej czułości, przeznaczony do pracy w zakresie częstotliwości 50...4000 MHz, np. w torach odbiorczych stacji bazowych telefonii komórkowej jako tzw. MHA (ang. *Mast-Head Amplifier*), czyli umieszczany bezpośrednio przy antenie, zaraz za filtrem dupleksowym (deklarowany współczynnik szumów jest tu na niezwykle niskim poziomie NF=0,6 dB). Z uwagi na niskie napięcie zasilania wzmacniacza równe 5 VDC, aby uniknąć przesterowania jego wejścia sygnałem z analizatora nanoVNA-H4+, zastosowano wstępny tłumik 20 dB, który w praktyce całkowicie skompensował jego wzmocnienie deklarowane na tym samym poziomie. I tak, zilustrowane na **rysunku 130**, skorygowane o –20 dB, wzmocnienie badanego urządzenia oscylowało w granicach od około +0,5…+1 dB w zakresie częstotliwości do około 500 MHz, spadając do około –3 dB na krańcu zakresu pomiarowego (2,7 GHz). Warto podkreślić, że moduł impedancji wejściowej |Z|, praktycznie w całym mierzonym pasmie częstotliwości, tylko dość nieznacznie odbiegał od oczekiwanych 50 Ω, co powinno mieć bardzo korzystny wpływ na energetyczną efektywność współpracy z anteną odbiorczą. Deklarowane parametry kolejnego przebadanego wzmacniacza (**fotografia 36**) to:

- zasilanie Vdd: 5...12 VDC,
- wzmocnienie: 30 dB przy Vdd=9 VDC,
- pasmo przenoszenia: 0,1...2000 MHz,
- LNA – niskim poziom szumów (niestety, nie podano jaki).

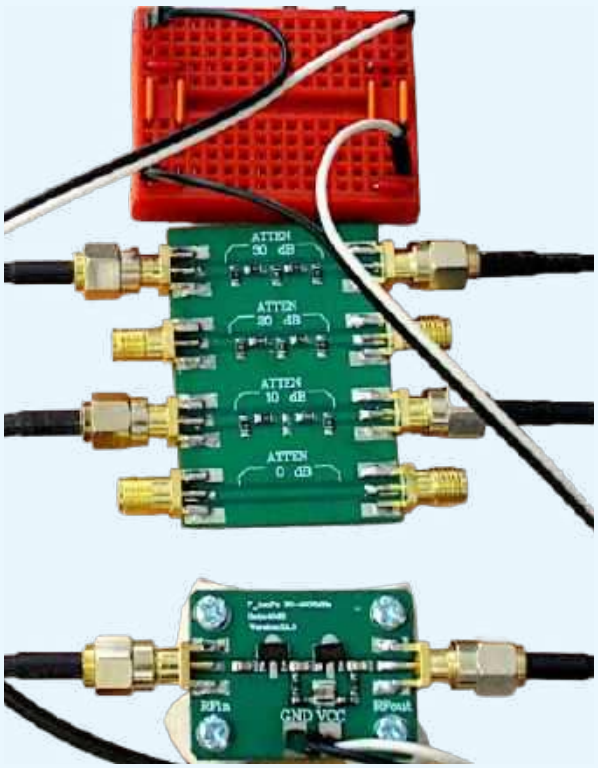
Na stronie oferenta produktu można znaleźć też ciekawe informacje o tym, że wzmocnienie może osiągnąć nawet 32,5 dB przy Vdd=12 V, a regulując Vdd w zakresie od 5 do 8 VDC można uzyskać efekt regulacji wzmocnienia w użytecznym zakresie. Niestety, nie podano tego zakresu – jest to warte zbadania, koniecznie wraz z wpływem takiej regulacji na liniowość przetwarzania wzmacniacza. **Rysunek 131** odzwierciedla rezultaty testów pomiarowych, które zostały przeprowadzone przy nominalnym Vdd=9 VDC. Dobrze prezentuje się charakterystyka przenoszenia wzmacniacza w całym deklarowanym pasmie (a nawet istotnie powyżej niego), która w szczególności w zakresie do 1 GHz jest bardzo dobrze wyrównana. Całkiem korzystnie wypadł też pomiar |Z|, który w całym mierzonym zakresie częstotliwości oscylował pomiędzy 50 a 70 Ω. Ostatni z pomierzonych wzmacniaczy szerokopasmowych (**fotografia 37**) był przeznaczony do pracy w pasmie 30...4000 MHz jako LNA (jakkolwiek, brak danych



Rysunek 131. Charakterystyki częstotliwościowe tłumienia i SWR wzmacniacza LNA 0,1...2000 MHz/30 dB



Rysunek 132. Charakterystyki częstotliwościowe tłumienia i SWR wzmacniacza LNA 30...4000 MHz/40 dB



Fotografia 37. Wzmacniacz LNA 30...4000 MHz/40 dB

szczegółowych odnośnie do parametru NF), oferując wzmocnienie 40 dB przy impedancjach wejściowej i wyjściowej 50 Ω oraz zasilaniu Vdd=5 VDC. Urządzenie testowano sygnałem sterującym profilaktycznie stłumionym wstępnie o 40 dB.

Rysunek 132 pokazuje, że co prawda parametr |Z| w całym deklarowanym pasmie pracy tylko dość nieznacznie przekracza pożądaną wartość 50 Ω, to jednak sama częstotliwościowa charakterystyka przenoszenia jest wyraźnie poszarpana i spada aż do około –6 dB na górnym krańcu deklarowanego roboczego pasma częstotliwości. Wydaje się, że ten wzmacniacz mógłby nieźle sprawdzić się jako przedwzmacniacz RF (a może nawet jako drugi stopień przedwzmacniacza w warunkach odbioru bardzo słabych sygnałów), jednak tylko do częstotliwości około 1 GHz i przy przetwarzaniu sygnałów radiowych (wąskopasmowych), z uwagi na nierozpoznane własności szumowe oraz bardzo nierównomierną charakterystykę przenoszenia.

Podsumowanie

W ostatniej już części cyklu publikacji o pomiarach charakterystyk częstotliwościowych skupiono się na układach w.cz. w większości dostępnych w handlu detalicznym. Wnioski z pomiarów nie tylko dają wiedzę praktyczną na temat różnorakich charakterystyk i właściwości badanych urządzeń w.cz., ale także podkreślają rolę i znaczenie dobrze przeprowadzonych pomiarów weryfikacyjnych w warsztacie pracy rozważnego konstruktora urządzeń i systemów radiokomunikacyjnych. W tym miejscu autor chciałby gorąco zachęcić Czytelników EP do lektury przyszłego cyklu publikacyjnego, który z założenia ma stać się swego rodzaju studium nad obszerną dziedziną radiokomunikacji, tzn. od podstawowych zagadnień emisji i propagacji fal radiowych, poprzez ich przenoszenie i przetwarzanie w torach elektrycznych, aż do licznych technik efektywnej i bezpiecznej obróbki analogowych i cyfrowych informacji we współcześnie stosowanych kanałach radiokomunikacyjnych – ciągłych i ziarnistych.

Adam Sobczyk, EP

Literatura i inne źródła:
[1] https://nanovna.com/
[2] https://tinysa.org/
[3] J. Szóstka, Mikrofale, WKiŁ, 2008
[4] http://sysjoint.com/, (dot. produktu RF Demo-Kit)
[5] A. Janeczek SP5AHT, *Konstrukcje krótkofalarskie dla początkujących*, WKiŁ, 1994
[6] A. Janeczek SP5AHT, *Filtr kwarcowy SSB* (kit AVT277), „Elektronika Praktyczna" 2/96
[7] A. Sobczyk SQ5RWQ, *Modułowy odbiornik nasłuchowy na pasma 80 m i 40 m „Dosia"* (2), „Elektronika Praktyczna¨ 10/2017

FN-SWM10
Zgrzewarka do ogniw – spawarka punktowa z kolorowym wyświetlaczem i funkcją powerbank FNIRSI SWM10

FN-DPOS-350P
Dwukanałowy oscyloskop 350 MHz, FNIRSI DPOS350P

FN-2C53T
Dwukanałowy oscyloskop z multimetrem i generatorem 50 MHz FNIRSI 2C53T

BESTSELLERY sklepu AVT – sklep.avt.pl

Mierniki Testery FNIRSI

Rabat dla Czytelników EP
przy zakupie podaj kod **EP2505FN**

-3%

Rabat dla Prenumeratorów EP
przy zakupie podaj numer prenumeraty

-6%

FN-LCR-ST1
Miernik pęsetowy, tester elementów FNIRSI LCR-ST1

FN-LCR-P1
Tester elementów FNIRSI LCR-P1

FN-HRM10
Tester rezystancji wewnętrznej akumulatorów FNIRSI HRM-10

FN-G1200
Mikroskop cyfrowy G1200 z wyświetlaczem 7 cali, powiększenie ×1200, tryb foto/video

FN-DWS200-F245
Stacja lutownica 200 W z kolbą F245, FNIRSI DWS200

FN-1014D
Oscyloskop dwukanałowy 100 MHz; Generator sygnału DDS, FNIRSI 1014D

koktajl niusów

Moduł graficzny MX5000B-XA firmy Aetina

Aetina wprowadza do oferty moduł graficzny MX5000B-XA, oparty na układzie NVIDIA RTX PRO 5000 z architekturą Blackwell. Rozwiązanie to jest przeznaczone do zastosowań związanych z obliczeniami AI oraz zaawansowaną grafiką 3D, w tym do symulacji, grafiki generatywnej i analizy multimodalnej.

Zastosowany procesor graficzny udostępnia 10 496 rdzeni CUDA do obliczeń ogólnego przeznaczenia, 80 rdzeni RT do obsługi ray tracingu oraz 320 rdzeni Tensor wykorzystywanych w zadaniach AI. Moduł wyposażono ponadto w 24 GB pamięci GDDR7 o przepustowości do 896 GB/s. Wydajność w operacjach FP32 wynosi 40,62 TFLOPS.

Standardowy zakres temperatury pracy MX5000B-XA mieści się w przedziale od 0 do 55°C. Producent oferuje również wersje przystosowane do pracy w rozszerzonym zakresie temperatur, od –40 do 70°C. Moduł może być dodatkowo zabezpieczony powłoką konformalną, która zwiększa odporność na wilgoć, pył i inne czynniki środowiskowe.

Pod względem obsługi programowej MX5000B-XA wspiera standardy DirectX 12 Ultimate, Vulkan 1.2 oraz OpenGL 4.6. Umożliwia to wykorzystanie go zarówno w aplikacjach graficznych, jak i obliczeniowych działających pod kontrolą systemów Windows 10, Windows 11 oraz 64-bitowych wersji Linuxa.

Konstrukcja została wyposażona w cztery wyjścia DisplayPort 2.1a, co pozwala na obsługę systemów wyświetlania o rozdzielczości do 8K. Wśród przewidywanych obszarów zastosowań modułu znajdują się profesjonalne systemy wizualizacji, aplikacje kontroli jakości oraz interaktywne kokpity operatorskie stosowane w zaawansowanych instalacjach przemysłowych.

https://csi.pl/mx5000b-xa-z-architektura-nvidia-blackwell/

Miernik temperatury grotów lutowniczych TM-100

TM-100 to miernik przeznaczony do pomiaru temperatury grotów lutowniczych. Urządzenie pracuje w zakresie od 0 do 550°C, a jego dokładność pomiarowa wynosi ±0,5% dla całego zakresu skali. Czas pojedynczego pomiaru wynosi od 2 do 3 sekund.

Konstrukcja przyrządu została opracowana z myślą o uzyskiwaniu stabilnych odczytów dla szerokiej gamy grotów lutowniczych. W urządzeniu zastosowano oryginalny czujnik temperatury, który jest łatwy w konserwacji i może być wymieniony w razie potrzeby. Trwałość miernika określono na co najmniej 200 użyć. TM-100 jest przeznaczony do pracy z szeroką gamą grotów lutowniczych.

Urządzenie wyposażono we wbudowany wyświetlacz LED, który umożliwia odczyt mierzonych wartości również w warunkach ograniczonego oświetlenia. Miernik jest zasilany czterema bateriami AA o napięciu 6 V, a czas pracy przekracza 100 godzin. Zamiast baterii można stosować także akumulatorki. Przyrząd ma również wskaźnik rozładowania baterii.

Wśród dostępnych funkcji znajduje się zatrzymywanie wartości szczytowej oraz zapamiętywanie wskazań maksymalnej temperatury. Urządzenie wyłącza się automatycznie, jeżeli po jego uruchomieniu nie nastąpi zmiana mierzonej temperatury o co najmniej 100°C.

TM-100 wykorzystuje termoparę typu K (CA), a rozdzielczość pomiarowa wynosi 1°C. Wymiary urządzenia to 8,3×14×3,8 cm, a masa 150 g (bez baterii). Dopuszczalne warunki pracy obejmują temperaturę otoczenia od 0 do 50°C oraz wilgotność względną w zakresie od 20 do 85% RH, bez kondensacji.

https://www.robtools.pl/,199,Miernik-temperatury-grotow.html

Rozdzielacz/konwerter RSC-04

RSC-04 to rozdzielacz/konwerter przeznaczony do budowy rozległych sieci wyświetlaczy tekstowych i cyfrowych. Urządzenie umożliwia rozgałęzienie linii RS-485 do czterech wyświetlaczy, zapewniając jednocześnie izolację galwaniczną dla linii głównych. Odpowiada także za transmisję danych do wyświetlaczy oraz dystrybucję bezpiecznego napięcia zasilania pochodzącego z zewnętrznego źródła mocy.

W urządzeniu zastosowano standardowy odbiornik RS-485, galwanicznie izolowany od pozostałych wejść i wyjść. Wejście odbiornika zabezpieczono przed przepięciami oraz spolaryzowano rezystorami, aby utrzymać prawidłowy stan spoczynkowy w przypadku rozwarcia linii.

Dane są przekazywane do czterech nadajników RS-422/485, połączonych z czterema wyjściami RJ-12. Na każdym z wyjść dostępne są dwie linie danych, a także podwojone linie masy i zasilania. Wyjścia transmisyjne zabezpieczono przed przepięciami oraz zwarciami.

RSC-04 zapewnia również pełne sterowanie pojedynczym wyświetlaczem LDN/LDA wyposażonym w złącze RJ-12. Obecność zasilania sygnalizuje dioda LED umieszczona obok złącza zasilania zewnętrznego.

https://sem.pl

Nowe złącza ATTEND Technology do kart SD oraz SIM dostępne w ofercie TME

Oferta dystrybutora TME została rozszerzona o złącza ATTEND Technology z rodziny 115U. Są to elementy o kompaktowych wymiarach, przeznaczone do osadzania kart wykorzystywanych do przechowywania danych lub komunikacji. Seria została opracowana z myślą o nowoczesnych aplikacjach elektronicznych i różnych wymaganiach projektowych, ze szczególnym uwzględnieniem miniaturyzacji współczesnych urządzeń.

Złącza 115U są przeznaczone do zastosowań przemysłowych, systemów IoT, urządzeń motoryzacyjnych oraz maszyn konsumenckich. Prezentowana oferta obejmuje trzy modele. We wszystkich zastosowano mechanizm Push-Pull, który ułatwia montaż oraz wyjmowanie kart SD lub SIM.

Elementy z tej serii charakteryzują się odpornością środowiskową, a dzięki technologii montażu powierzchniowego SMT mogą być łatwo implementowane w urządzeniach docelowych. Złącza 115U są dostępne w wersjach hybrydowych i przystosowane do obsługi kart w trzech formatach: microSD, Micro SIM oraz Nano SIM. Oznacza to możliwość wykorzystania ich zarówno do komunikacji z użyciem technologii komórkowych, jak i do akwizycji danych na nośnikach pamięci.

https://www.tme.eu/pl/news/about-product/page/74214/nowe-zlacza-marki-attend-do-kart-sim-oraz-sd/

Grupa urządzeń SCANBR obsługujących magistrale CAN

Grupa urządzeń SCANBR obejmuje rozwiązania przeznaczone do zarządzania przepływem danych w magistrali CAN pojazdów, takich jak autobusy i tramwaje. Wszystkie urządzenia z tej grupy wyposażono w zabezpieczenia łączy transmisyjnych przed podaniem zbyt wysokiego napięcia (od 50 V wzwyż), a także przed zwarciami, w tym do masy.

Do grupy SCANBR należą trzy urządzenia: CANBridge, CAN Torque Switch oraz CAN FMSGateway. CANBridge pobiera wybrane ramki CAN z kanału CAN0, a następnie konwertuje je i przesyła do kanału CAN1 lub transmituje w kanale CAN0, zależnie od ustawienia przełącznika DIP-SWITCH1. W tym rozwiązaniu nie występuje przesyłanie ramek z kanału CAN1 do kanału CAN0.

CAN Torque Switch umożliwia przesyłanie wybranych ramek CAN bez modyfikacji z kanału CAN0 do CAN1. W kierunku z kanału CAN1 do CAN0 część wybranych ramek jest przesyłana bez zmian, natomiast pozostałe są transmitowane z modyfikacjami. Sposób pracy urządzenia zależy od ustawień przełączników DIP-SWITCH.

CAN FMSGateway służy do przesyłania ramek CAN z kanału CAN0 do kanału CAN1 bez modyfikacji lub z modyfikacjami, w zależności od ustawienia przełącznika DIP-SWITCH1. W tym przypadku ramki CAN nie są przesyłane z kanału CAN1 do kanału CAN0.

https://www.sims.pl/konwertery-can

Domofon GDS3710

GDS3710 to urządzenie łączące funkcje domofonu, kamery i interkomu. Model ten jest przeznaczony do kontroli dostępu do budynków oraz monitorowania zabezpieczeń. Urządzenie wyposażono w kamerę o kącie widzenia 180°, a także wbudowany czytnik kart RFID, służący do kontroli wejścia. W konstrukcji zastosowano również mikrofon i głośnik, które umożliwiają dwukierunkową komunikację audio i wideo.

Za przetwarzanie obrazu w rozdzielczości 1080p FHD odpowiada procesor ISP. Urządzenie jest przystosowane do pracy w różnych warunkach oświetlenia.

Domofon obsługuje technologię SIP/VoIP i umożliwia dwukierunkową transmisję strumieni audio oraz wideo do użytkowników korzystających m.in. ze smartfonów, punktów końcowych SIP i dedykowanego oprogramowania. Model wyposażono także w funkcje wejść i wyjść alarmowych oraz przystosowano do współpracy z narzędziem GDS Manager, opracowanym przez producenta urządzenia, firmę Grandstream Networks.

GDS3710 ma zintegrowane PoE, diody LED, czujnik ruchu oraz przełącznik oświetlenia. W połączeniu z telefonami IP z serii GXP21xx, wideotelefonami GXV, aplikacją mobilną GS-Wave oraz nagrywarką NVR GVR350x może być wykorzystywany w systemach kontroli dostępu, komunikacji wewnętrznej i rejestracji w celach bezpieczeństwa.

https://grandstream.pl/produkty/domofony/gds3710-2-2

Sygnalizator dźwiękowy SB140

SB140 firmy Fluke to sygnalizator dźwiękowy przeznaczony do kontroli szczelności zbiorników bezciśnieniowych. Urządzenie umieszcza się wewnątrz zbiornika, a wykrywanie odchyleń od norm oraz potencjalnych wycieków odbywa się z wykorzystaniem ultradźwięków emitowanych w celu lokalizacji nieszczelności.

Model ten jest przystosowany do współpracy z urządzeniami służącymi do wykrywania ultradźwięków. Częstotliwość emitowanego sygnału została dobrana tak, aby możliwe było jego wychwycenie podczas wydostawania się przez nieszczelności, także o niewielkich rozmiarach. Umożliwia to wskazywanie miejsc potencjalnych wycieków oraz prowadzenie testów szczelności w różnych zastosowaniach przemysłowych.

SB140 może być wykorzystywany m.in. w kontroli jakości w branży lotniczej, motoryzacyjnej czy kolejowej, a także podczas kontroli pomieszczeń sterylnych oraz w innych zastosowaniach przemysłowych. Urządzenie jest stosowane tam, gdzie wymagane jest testowanie szczelności i spełnienie określonych norm branżowych oraz wymagań regulacyjnych.

Sygnalizator pracuje z częstotliwością ultradźwięków 40±1,5 kHz. Dopuszczalna temperatura pracy wynosi od –20 do 54°C, a dopuszczalna wilgotność względna otoczenia mieści się w zakresie od 10 do 95% RH. Obudowa o stopniu ochrony IP40 została wykonana z wytłaczanego aluminium. Urządzenie ma wymiary 3,2×3,2×10,5 cm i jest wyposażone w przełącznik włączania i wyłączania.

SB140 jest zasilany baterią alkaliczną 9 V, dołączaną do zestawu. Deklarowany czas pracy na baterii wynosi minimum 300 godzin. Producent udziela na urządzenie 2-letniej gwarancji.

https://www.fluke.com/pl-pl/produkt/obrazowanie-przemyslowe/fluke-sb140

Szerokokątny obiektyw fotograficzny CN5x11 IAS T R1/P1

CN5x11 IAS T R1/P1 to szerokokątny obiektyw fotograficzny o ogniskowej 11 mm i kącie widzenia 100°. Parametry te pozwalają na rejestrowanie obiektu wraz z otoczeniem zarówno w ograniczonej przestrzeni studyjnej, jak i podczas dynamicznych realizacji na żywo.

Model jest dostępny w wersjach z mocowaniem RF lub PL. Konstrukcję obiektywu wyposażono w napęd e-Xs V Digital Drive Unit, odpowiadający za precyzyjne sterowanie i obsługę dodatkowych funkcji. Masa obiektywu wynosi 3 kg, co czyni go najlżejszym modelem z serii Cine-Servo.

CN5x11 IAS T R1/P1 może być stosowany m.in. z gimbalami, żurawiami kamerowymi, systemami zrobotyzowanymi oraz kamerami linowymi. Obiektyw ma także zdejmowaną jednostkę serwo, przeznaczoną do konfiguracji w zastosowaniach takich jak transmisje sportowe, wydarzenia na żywo i produkcja filmowa. Jednostka ta zapewnia również szybsze działanie przysłony oraz udostępnia port USB-C.

Wersja z mocowaniem PL obsługuje technologie Cooke /i Technology oraz ZEISS eXtended Data, umożliwiające transfer wybranych metadanych w czasie rzeczywistym. Z kolei wariant z mocowaniem RF wspiera m.in. Dual Pixel CMOS AF, przeznaczony do szybkiego i płynnego autofokusa, a także rozszerzone dane wykorzystywane do korekcji obrazu z obiektywu.

https://www.canon.pl/press-centre/press-releases/2025/09/capture-the-bigger-picture-with-the-widest-canon-cine-servo-lens-yet

Elektroniczny zamek ECHO 3450 z obsługą NFC

ECHO 3450 to elektroniczny zamek z obsługą NFC, niewymagający baterii, przewodów ani zewnętrznego zasilania. Urządzenie wykorzystuje technologię NFC do pobierania niewielkiej ilości energii potrzebnej do zablokowania i odblokowania zamka. Taka konstrukcja eliminuje kwestie związane z konserwacją, magazynowaniem i utylizacją baterii, a zarazem ogranicza wpływ eksploatacji urządzenia na środowisko.

Model ECHO 3450 oferuje trzy tryby pracy i współpracuje z aplikacją producenta dostępną na systemy iOS oraz Android. Za pomocą aplikacji można ustawiać i zmieniać tryby działania zamka. Obejmują one dwa tryby publiczne oraz jeden tryb prywatny.

W trybach publicznych dostęp do szafek wyposażonych w zamek ECHO 3450 wymaga wcześniejszego pobrania aplikacji. W trybie prywatnym użytkownicy końcowi otrzymują od właściciela przechowalni wyłączny dostęp do szafek.

W większych organizacjach oraz w podmiotach wymagających pełnej kontroli zamek ECHO 3450 może być zarządzany za pośrednictwem portalu internetowego. Wersja standardowa portalu umożliwia wgląd we wszystkie egzemplarze zamków, ich dostępność i użytkowników, a także zbiorczą wysyłkę wiadomości e-mail. Wersja profesjonalna obejmuje dodatkowe funkcje, w tym raportowanie wykorzystania poszczególnych zamków oraz możliwość ograniczania liczby zamków przypisanych do jednego użytkownika.

Zamek ECHO 3450 może być stosowany m.in. do składowania przedmiotów, gospodarowania zasobami, a także w obiektach związanych z turystyką, węzłach transportowych i klubach sportowych.

https://www.euro-locks.com/pl/produkt/zamek-echo

Separatory EasyCut 300 i EasyCut 300M

EasyCut 300 i EasyCut 300M to urządzenia przeznaczone do separacji płytek PCB. Model EasyCut 300 jest oferowany w wersji manualnej, natomiast EasyCut 300M wyposażono m.in. w dwustopniowy napęd dolnego ostrza.

W przypadku EasyCut 300 operator umieszcza narylcowany panel w prowadnicy, a następnie przeciąga płytkę na całej długości pomiędzy dwoma ostrzami. W modelu EasyCut 300M dolne ostrza wciągają panel, po czym następuje separacja.

Oba urządzenia obsługują płytki PCB o grubości od 1 do 3,2 mm oraz panele o maksymalnej długości 32 cm. W obu przypadkach wymagane podfrezowanie mieści się w zakresie od 0,3 do 0,8 mm, a kąt podfrezowania wynosi od 25 do 30°.

Wymiary modelu EasyCut 300 wynoszą 19×67×35,5 cm, a jego masa to 18,5 kg. Model EasyCut 300M ma takie same wymiary, natomiast jego masa wynosi 23,7 kg.

https://paktel.pl/produkt/easycut300-300m/

Jakub Tyburski
jakub.tyburski@elportal.pl

Hity następnego numeru • „Elektronika Praktyczna” 5/2026

Temat numeru: Badania inżynierskie – sprzęt i usługi

Badania inżynierskie stanowią nieodłączny etap rozwoju każdego urządzenia elektronicznego – pozwalają bowiem zweryfikować założenia projektowe i ograniczenia technologiczne oraz wyeliminować potencjalne źródła błędów. W praktyce oznacza to konieczność sięgnięcia po zaawansowaną aparaturę pomiarową, specjalistyczne stanowiska testowe oraz – coraz częściej – wsparcie zewnętrznych laboratoriów.

W artykule omawiamy dostępne narzędzia i usługi wspierające proces badań: od klasycznych pomiarów elektrycznych i analiz EMC, przez testy środowiskowe i niezawodnościowe, po badania kompatybilności regulacyjnej wymaganej m.in. w procedurach CE czy RED. Zwracamy uwagę na praktyczne aspekty współpracy z laboratoriami – przygotowanie próbek, interpretację wyników oraz optymalizację kosztów badań.

Pokazujemy, jak świadomie zaplanować proces testowania, aby skrócić czas wdrożenia, ograniczyć ryzyko poprawek projektowych i uzyskać wiarygodne wyniki, które realnie przekładają się na jakość finalnego urządzenia.

Elektronika w Praktyce: Optoelektronika

Optoelektronika to obszar, w którym światło przestaje być jedynie nośnikiem informacji, a staje się pełnoprawnym „sygnałem roboczym” w torach pomiarowych, transmisyjnych i sterujących. Współczesne układy coraz częściej integrują domenę optyczną i elektroniczną. Galwaniczne bariery optyczne o wytrzymałości rzędu dziesiątek kilowoltów, ultraprecyzyjne dalmierze oparte na pomiarze czasu przelotu (ToF), zaawansowane systemy obrazowania w paśmie podczerwieni czy wreszcie miniaturowe spektrometry mieszczące się na dłoni – to zaledwie skromny ułamek współczesnych osiągnięć optoelektroniki.

W artykule przyglądamy się praktycznym aspektom projektowania układów optoelektronicznych: doborowi źródeł światła (diody LED, lasery), detektorów (fotodiody PIN i APD, matryce CMOS, detektory InGaAs), torów analogowych o bardzo niskim poziomie szumów, a także metod przetwarzania sygnałów szerokopasmowych. Omawiamy również problemy, które często ujawniają się dopiero na etapie uruchamiania – w tym wpływ rozproszenia i odbić, stabilność temperaturową, nieliniowości oraz zagadnienia EMC w układach zawierających komponenty optyczne.

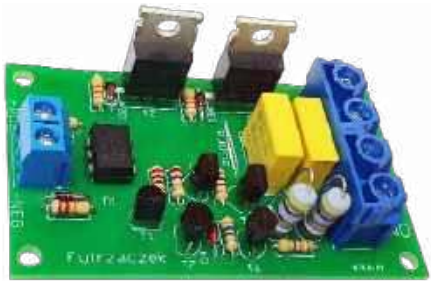
Pokazujemy, jak świadomie projektować systemy, w których światło stanowi integralny element funkcjonalny – począwszy od koncepcji, poprzez dobór komponentów, aż do walidacji gotowego rozwiązania.

Półprzewodnikowy przekaźnik NO-NC

Typowe przekaźniki półprzewodnikowe mają wyjścia w postaci „styków” NO – bez obecności napięcia sterującego pozostają rozwarte. Tymczasem w niektórych zastosowaniach przydałby się również zacisk NC, czyli zwarty przy braku sygnału sterującego. Prezentowany układ to propozycja rozwiązania tej niedogodności.

Najważniejsze parametry:

- przełączanie dodatniej linii zasilającej między dwoma wyjściami: NO i NC,
- sygnał sterujący w postaci napięcia stałego o wartości 3…15 V,
- izolacja galwaniczna między sygnałem sterującym a obwodem przełączanym,
- napięcie przełączane: 24…55 V,
- maksymalny prąd przełączany: 7 A bez chłodzenia tranzystorów, do 20 A po zastosowaniu radiatora,
- pobór prądu z obwodu wykonawczego: ok. 6 mA.



Wykaz firm ogłaszających się w tym numerze „Elektroniki Praktycznej”

Miesięcznik **„Elektronika Praktyczna”** (10 numerów w roku) jest wydawany przez AVT Korporacja Sp. z o.o. we współpracy z wieloma redakcjami zagranicznymi.

Wydawnictwo:
AVT Korporacja Sp. z o.o.
03-197 Warszawa, ul. Leszczynowa 11
tel. 22 257 84 99, e-mail: avt@avt.pl

Wydawca:
Wiesław Marciniak

Adres redakcji:
03-197 Warszawa, ul. Leszczynowa 11
e-mail: redakcja@ep.com.pl, www.ep.com.pl

Redaktor Naczelny:
Przemysław Musz

Redaktor Programowy, Przewodniczący Rady Programowej:
Piotr Zbysiński

Menedżer Magazynu:
Katarzyna Gugała, tel. 22 257 84 64

Szef Pracowni Konstrukcyjnej:
Jakub Sobański

Zespół marketingu i reklamy:
Katarzyna Gugała, Bożena Krzykawska, Grzegorz Krzykawski

Stali współpracownicy:
Lucjan Bryndza, Filip Krzyżański, Jarosław Doliński, Andrzej Gawryluk, Krzysztof Górski, Tomasz Jabłoński, Paweł Kowalczyk, Henryk Kowalski, Rafał Kozik, Michał Kurzela, Jakub Nowicki, Szymon Panecki, Adam Sobczyk, Damian Sosnowski, Ryszard Szymaniak, Adam Tatuś, Jakub Tyburski

Uwaga!
Kontakt z wymienionymi osobami jest możliwy via e-mail, według schematu: imię.nazwisko@ep.com.pl

DTP, redakcja strony internetowej www.ep.com.pl:
MAD Sp. z o.o.

Prenumerata w Wydawnictwie AVT
www.ulubionykiosk.pl lub tel. 22 257 84 22 (godz. 10.00–14.00)
e-mail: prenumerata@avt.pl