Wi-Fi w systemach embedded

Wi-Fi to technologia bezprzewodowej komunikacji, która w ostatnich latach stała się powszechną i szeroko obecną na rynku elektroniki. Dojrzałość i powszechna akceptacja rynku zachęcają wiele firm do tworzenia modułów komunikacyjnych przeznaczonych do systemów embedded wykorzystujących tę technologię, gdyż ryzyko biznesowe związane z możliwością trafienia w technologię, która nie będzie się rozwijać jest tutaj niskie. W efekcie produktów z Wi-Fi jest na rynku wiele, a klienci mają problem, na co się zdecydować i jakie kryteria brać pod uwagę.

Według danych organizacji Wi-Fi Alliance technologia ta zmieniła całkowicie sposób, w jaki komunikujemy się we współczesnej technice, gdyż tylko w użytku domowym jest 200 mln urządzeń z Wi-Fi, plus mamy około 750 tysięcy hotspotów. Z tego potencjału korzysta 700 mln ludzi na całym świecie. Tak duży potencjał rynku konsumenckiego przenosi się na inne dziedziny techniki, m.in. rynek produktów embedded. Niemniej nie jest to łatwe, ponieważ rynek pecetów jest bardzo różnorodny od strony technicznej. Produkty różnią się od strony zasobów pamięci, wydajności procesora, przez co adaptacja rozwiązań Wi-Fi w systemach embedded nie jest procesem prostym.

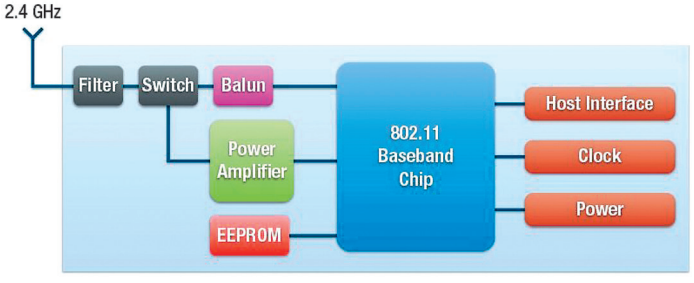
W typowych warunkach z uwagi na złożoność i trudność techniczną rozwiązań cyfrowej komunikacji radiowej, rynek produktów embedded implementuje W-Fi w postaci modułów komunikacyjnych. Wymagania w stosunku do nich są standardowe: muszą być małe, tanie, ich działanie ma być niezależne od platformy sprzętowej itd. Są to na tyle ogólne kryteria, że wybór dostawcy i produktu nie jest łatwy.

Wi-Fi w aplikacjach M2M

Komunikacja M2M (machine-to-machine) to temat, który łączy się najczęściej z sieciami telefonii komórkowej GSM. Jednak M2M to znacznie szersze pojęcie i łączy w sobie media takie jak Ethernet, Zigbee, PLC, GSM i także Wi-Fi, a więc wszystkie popularne media komunikacyjne, nie tylko bezprzewodowe. W przypadku sprzętu stacjonarnego komunikacja może być zrealizowana za pomocą kabla. Wi-Fi lub inaczej mówiąc wireless LAN to technologia, która jest bliska klasycznym sieciom lokalnym przewodowym. Przewodowy Ethernet może zostać łatwo przekonwertowany na bezprzewodowe Wi-Fi, przez co koszty rozbudowy można znacznie ograniczyć. Można też łączyć sieci ethernetowe przewodowe z Wi-Fi tak, że komunikacja bezprzewodowa staje się ich uzupełnieniem i rozszerzeniem. Taki sposób wybiera wiele firm integracyjnych ceniąc je za elastyczność i niski koszt realizacji komunikacji.

Który standard Wi-Fi?

W tabeli 1 pokazano charakterystykę podstawowych standardów Wi-Fi i główne parametry. Standardy 802.11a i 802.11b to starsze wersje i niekompatybilne ze sobą. Urządzenia 802.11a pracują wyłącznie paśmie 5 GHz a 802.11b w 2,4 GHz. 802.11n skupia najwięcej sprzętu i jest najpopularniejszą wersją, wstecznie kompatybilną z 802.11b i 802.11g. Wszystkie trzy działają w zakresie 2,4 GHz a dodatkowo „n" pracuje w paśmie 5 GHz.



Rys. 1. Wykorzystanie Wi-Fi SoC wymaga implementacji driverów komunikacyjnych w aplikacji

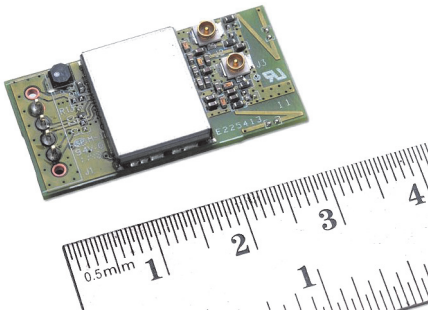
Standard 802.11n wykorzystuje technologię MIMO zwielokratniającą liczbę aktywnych torów radiowych i anten ponad jeden, przez co możliwe jest osiągnięcie większych szybkości transmisji. Niemniej podczas współpracy z urządzeniami dostępowymi starszych generacji z tej możliwości nie daje się skorzystać, gdyż nie jest ona obsługiwana przez punkt dostępowy.

Powyższe suche fakty na temat technologii są wstępną osią selekcji produktów. Poza nimi jest cały szereg bardziej specyficznych funkcji, które trzeba rozważyć. Ponadto zagadnienia związane z szybkością transmisji danych w wielu systemach embedded nie mają wielkiego znaczenia, bo sprzęt ten nie wymienia takiej ilości danych. Jednak czy to znaczy, że konstruktorzy powinni wybierać starsze rozwiązania, bo one spełniają ich aktualne potrzeby?

Niekoniecznie, gdyż szybko zmieniający się rynek elektroniki konsumenckiej powoduje, że nowe technologie są dostępne i tanie, starsze zaś szybko wypadają z rynku, a ceny produktów dalekie są od optymalnych. Wypadanie z rynku starszych technologii nie wynika z tego ze mają one słabe parametry, tylko z tego, że nie ma na nie wystarczająco dużego zapotrzebowania. Rynek M2M jest nieporównywalnie mniejszy od konsumenckiego i trzeba się przez to podporządkować i iść za rozwojem technologii, albo nastawić się na kłopoty z kupnem komponentów. Z drugiej strony najnowsze układy procesorów komunikacyjnych są znacząco droższe od tych starszych, które są na rynku od pewnego czasu.

Z tego też powodu w aplikacjach M2M implementowanie własnych rozwiązań Wi-Fi za pomocą układów scalonych i poprzez samodzielną budowę toru radiowego nie ma sensu, gdyż szybko zmieniająca się technologia przy tej skali zastosowań nie pozwoli na zamortyzowanie stałych kosztów inżynierskich projektu.

Widać to w cenach procesorów komunikacyjnych. Najkorzystniejsze pod względem cen są starsze procesory komunikacyjne, które są popularne i ciągle produkowane przez wielu wytwórców półprzewodników. Przykładem może być chip 88W8686 b/g firmy Marvell dostępny jako układ SoC i aplikowany przez wielu producentów modułów komunikacyjnych. Popularność jego wynika z kompatybilności zapewnianej w rach rodziny 802.11 n, b i g, przez co wydaje się być optymalnym rozwiązaniem dla tych, którzy nie potrzebują dużych szybkości transmisji, ale chcą mieć rozwiązanie zdolne do funkcjonowania na rynku przez długi czas.



Rys. 2. Dla systemów embedded bazujących na Linuksie moduł komunikacyjny z układem SoC i certyfikowanym torem radiowym wydaje się być korzystną propozycją

SoC kontra moduł

Kolejną ważną decyzją jest to, czy decydować się na rozwiązanie w postaci układy scalonego typu SoC, czy na moduł (rys. 1). Generalnie moduł komunikacyjny daje mniejsze ryzyko tego, że procesor sygnałowy stanie się niedostępny i projekt interfejsu komunikacyjnego trzeba będzie zmienić. Producent modułów zapewniając kompatybilność pinową i funkcjonalną zapewnia konstruktorowi komfort migracji w takiej sytuacji.

Rozwiązanie oparte o SoC wymaga instalacji driverów, które zwykle dostarcza producent, ale tylko dla Linuksa i Windows, bo technologia Wi-Fi wywodzi się z pecetów. Jeśli urządzenie embedded bazuje na Linuksie, nie będzie to przeszkodą, o ile firma jest jeszcze w stanie przebrnąć przez certyfikację toru radiowego.

Gdy certyfikacja dla firmy nie jest problemem, ale drivery już tak, bo Wi-Fi będzie implementowane nie do platformy pecetowej, można skorzystać z kontrolera Wi-Fi/IP łączącego procesor lub mikrokontroler z układem SoC Wi-Fi. Natomiast, aby obejść wysoki koszt certyfikacji, można wykorzystać rozwiązanie, w którym układ SoC jest dostępny w postaci małego modułu (rys. 2).

Kompletny moduł komunikacyjny Wi-Fi (rys. 3) to z kolei propozycja dla tych, którzy chcą kupić rozwiązanie certyfikowane, wolne od problemów z driverami i niezależne od wykorzystywanego mikrokontrolera i systemu operacyjnego.

Im produkt bardziej uniwersalny i zintegrowany, tym cena jest wyższa, dlatego decyzja o inwestycji w konkretne rozwiązanie powinna uwzględniać koszt pracy inżynierskiej rozkładający się na skalę produkcji. Układy SoC kosztują od 5 do 15 dolarów w zależności od wielkości zamówienia, certyfikowane moduły zawierające procesor baseband w SoC i tor radiowy od 10 do 25 dolarów, a kompletne moduły Wi-Fi od 20 do 40 dolarów. Kontrolery Wi-Fi/IP kosztują od 5 do 10 dolarów. Koszt certyfikacji zależy od konkretnych uwarunkowań firmy, ale gdy jest zlecany na zewnątrz przedsiębiorstwa może sięgnąć nawet 20 tys. dolarów dla najbardziej złożonych rozwiązań i szerokiego zakresu testów wymaganego, gdy urządzenie będzie sprzedawane na całym świecie.

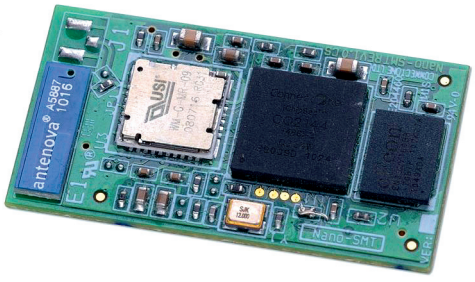
Wielu producentów gotowych modułów komunikacyjnych wykorzystuje ten sam rozkład wyprowadzeń i wymiary dla wersji „b/g" i „n", przez co mogą one być używane zamiennie. Co więcej wiele modułów Wi-Fi daje się bez zmian zainstalować w miejscu, gdzie wcześniej był zainstalowany interfejs do przewodowego Ethernetu.

Wewnętrzna czy zewnętrzna antena?

Projektowanie anten wymaga przeprowadzenia głębokich analiz na temat tego, jak będzie wyglądał finalny wyrób i jak będzie używany. Plastikowe obudowy zwykle mogą opierać się na antenach wewnętrznych, bo sygnał w.cz. jest w stanie propagować przez nie bez przeszkód, ale w przypadku obudów metalowych już tak się nie da. Stąd wiele modułów ma wbudowaną antenę wewnętrzną i pozwala na podłączenie anteny zewnętrznej, zamontowanej na zewnątrz obudowy.

Tabela 1. Standardy Wi-Fi i ich parametry

Wersja standardu 802.11	Pasmo (GHz)	Maksymalna prędkość (Mbps)	Typowa prędkość (Mbps)	Zasięg w pomieszczeniach (m)	Zasięg na zewnątrz (m)
A	5	54	25	40	100
B	2,4	11	6	70	150
G	2,4	54	26	80	200
N	2,4 lub 5	600 (4x4)	75 (1x1 @20)	100	250



Rys. 3. W urządzeniach bazujących na RTOS warto rozważyć użycie kompletnego modułu komunikacyjnego

Praktycznie bez względu na zysku energetycznego wykorzystywanej anteny, te umieszczone wewnątrz obudowy zapewniają mniejszy o 20–50% zasięg niż wersje zewnętrzne. Wyjęcie anteny z obudowy pozwala na osiągnięcie zasięgu od 100 do 200 metrów, o ile na drodze nie pojawią się przeszkody w postaci np. ścian.

Kontroler Wi-Fi/IP

Komunikacja za pośrednictwem Wi-Fi to nie tylko interfejs radiowy i procesor komunikacyjny baseband. Ważne są też szczegóły związane z bezpieczeństwem transmisji. Specjalizowany kontroler Wi-Fi/IP rozwiązuje ten problem w sposób szybki i efektywny kosztowo. Po pierwsze pełni on rolę sterownika sprzętowego do procesora baseband zawartego w układzie SoC, zawiera niezbędne drivery, stos i warstwę oprogramowania aplikacyjnego niezbędnego do zapewniania pracy w określonym standardzie. Dzięki niemu mikrokontroler aplikacji jest zwalniany z realizacji wielu złożonych zadań programowych.

Kontroler Wi-Fi/IP pełni także rolę sprzętowego firewalla, chroniąc aplikację przed możliwymi atakami, gdy połączenie jest wykorzystywane do komunikacji z Internetem. Jest to możliwe, ponieważ zawiera on stos TCP/IP oraz obsługuje protokoły takie jak HTTP, FTP i SMTP, DHCP. Obsługiwane jest ponadto szyfrowanie danych SSL3. Dzięki temu procesor aplikacji jest w stanie obsłużyć komunikację za pomocą prostych komend. Zarządzanie pracą kontrolera realizowane jest poprzez wbudowany web serwer, do którego można się dostać zdalnie poprzez przeglądarkę internetową. Jest to wygodnie rozwiązanie, które coraz częściej jest traktowane jako standard przemysłowy.

Szczegóły także mają znaczenie

Projektanci systemów embedded często podnoszą kwestie bezpieczeństwa danych transmitowanych w sieciach Wi-Fi. Trzeba mieć świadomość, że protokoły szyfrowania danych takie jak WEP, WPA, WPA2 dotyczą tylko warstwy radiowej, pomiędzy urządzeniem a punktem dostępowym, do którego jest ono podłączone. Dane płynące od punktu dostępowego do Internetu nie są chronione, o ile nie zostanie wykorzystany protokół SSL3, za pomocą którego szyfrowana jest cała droga komunikacyjna. Skuteczne szyfrowanie danych i obsługa SS3 jest wymagająca od strony obliczeniowej, dlatego przerzucenie tej pracy na moduł Wi-Fi/IP jest nierzadko korzystne.

Warto jeszcze zwrócić uwagę, że na rynku pojawiają się moduły komunikacyjne umożliwiające routing pomiędzy sieciami GSM a Wi-Fi. Są one najczęściej używane do zapewnienie dostępu do Internetu w obszarach gdzie nie ma infrastruktury przewodowej, np. w pojazdach. Taką funkcję także obsługuje kontroler Wi-Fi/IP, który można dołączyć z jednej strony do procesora sygnałowego SoC Wi-Fi, a z drugiej do modemu komórkowego. W ten sposób można też dodać do własnej aplikacji dostęp do internetu, niezależny od łącza Wi-Fi lub też uzupełniający główne połączenie na wypadek problemów komunikacyjnych lub awarii głównego połączenia. Jest to cenna właściwość w automatach sprzedających lub systemach security.

Amir Friedman, Connect One

Dane kontaktowe

SE Spezial-Electronic Polska
tel. 22 840 91 10, info@spezial.pl
www.spezial.pl