



- Wprowadzenie
- Wybrane sieci miejscowe
- Bezprzewodowa sieć ZigBee/IEEE802.15.4

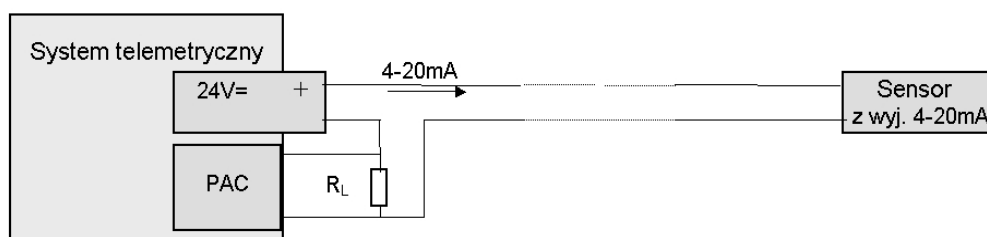
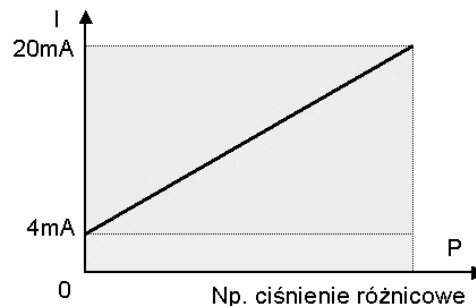
Dzisiaj właściwie nikomu nie trzeba tłumaczyć takich pojęć jak standaryzacja , normalizacja , unifikacja, dotyczących bardzo różnych obszarów działalności człowieka.

Ograniczając zakres rozważań do systemów sterowania można stwierdzić, że efektem tych prac są między innymi protokoły komunikacyjne. W ramach wykładu „ Protokoły w systemach wbudowanych” przedstawione zostaną istotne cechy dotyczące wybranych przewodowych sieci przemysłowych, tzw. sieci miejscowych oraz niedawno wprowadzanego standardu bezprzewodowego, tzn. protokołów ZigBee oraz IEEE 802.15.4.



- Standardy analogowe

Dwuprzewodowa pętla prądowa 4 – 20 mA



Zygmunt Kubiak

Protokoły w systemach wbudowanych (2)

Rozwój systemów sterowania rozpoczął się od systemów analogowych, w których dla potrzeb komunikacji na bliskie odległości wykorzystywano jako nośnik informacji prąd a na dalekie odległości najczęściej częstotliwość.

Określenie systemy sterowania, w ramach tego wykładu, należy rozumieć jako pojęcie obejmujące problematykę pomiarów i sterowania.

Aby informacja mogła być wykorzystana w urządzeniach czy systemach, sygnały wyjściowe i wejściowe różnych urządzeń i przetworników muszą spełniać odpowiednie standardy. Wśród standardów analogowych największe znaczenie mają sygnały prądowe (zasięg). Stosowane były różne standardy, np. 0 – 5 mA, 0 – 20 mA, -20 - +20 mA. W systemach telemetrycznych analogowych dla realizacji zdalnych pomiarów (przy odległościach do 3000m) stosowany jest głównie standard prądowy 4-20mA. W standardzie tym, prąd w przedziale 4-20mA zmienia się proporcjonalnie do zmiennej procesowej, tzn. wartość 4mA odpowiada kalibracji dla dolnego zakresu zmiennej (0%) a 20mA - górnemu zakresowi zmiennej (100%). Pokazano to na rysunku. Przesunięcie początkowej wartości prądu o 4mA umożliwia zasilanie oddalonego układu przetwornika i dlatego do połączenia układów wystarcza linia dwuprzewodowa. Mimo intensywnego rozwoju systemów transmisji cyfrowej, rozwiązania analogowe są ciągle z powodzeniem stosowane, co jest między innymi wynikiem różnorodności standardów cyfrowych.



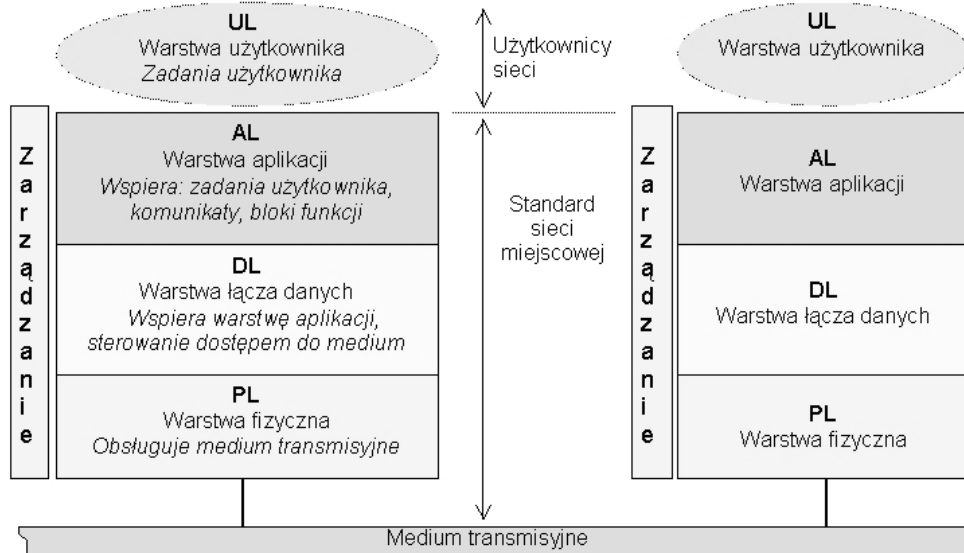
- Systemy cyfrowe – przewodowe
  - Sieci przemysłowe
    - Sieci firmowe
      - np. Mitsubishi - MiniNet
    - Sieci miejscowe (Fieldbus)
      - HART (ang. Highway Addressable Remote Transducer)
      - ASi (ang. Actuator Sensor Interface)
      - CAN (ang. Controller Area Network)
      - Modbus
      - Profibus DP
      - I inne

Cechą nowych rozwiązań systemów cyfrowych jest rozproszona struktura urządzeń i układów wejścia/wyjścia. Poszczególne urządzenia systemu, na najniższym poziomie systemu sterowania, tworzą sieć przemysłową. W ramach rozwiązań przewodowych można wyróżnić urządzenia z rozwiązaniami komunikacyjnymi specyficznymi tylko dla danego producenta, tzn. sieci firmowe oraz rozwiązania zdecydowanie bardziej uniwersalne, znormalizowane tzw. **sieci miejscowe** (ang. fieldbus) łączące inteligentne węzły. Z założenia sieci miejscowe są sieciami czasu rzeczywistego, a ponieważ przeznaczone są do pracy w warunkach przemysłowych muszą charakteryzować się zwiększoną odpornością na zakłócenia. Jedną z głównych przyczyn gwałtownego wzrostu popularności sieci miejscowych jest rozwój technologii półprzewodnikowej, który powoduje tak radykalny spadek kosztów elementów, że opłacalne staje się wyposażanie nawet poszczególnych układów wejściowych i wyjściowych systemu jak sensory, przetworniki pomiarowe, układy wykonawcze – w sterowniki mikroprocesorowe. Coraz częściej pojawiają się monolityczne układy scalone zawierające kompletne kontrolery poszczególnych sieci.

Ze względu na ograniczenia czasowe wykładu, przedstawione zostaną tylko najbardziej charakterystyczne cechy wybranych sieci miejscowych.



Model sieci miejscowej



Zygmunt Kubiak

Protokoły w systemach wbudowanych (4)

Rysunek przedstawia model sieci miejscowej, definiujący główne jej zadania. Model ten zasadniczo obejmuje tylko trzy warstwy (1, 2 i 7) znanego modelu odniesienia OSI, opracowanego dla sieci rozległych. Dla pełnego obrazu trzeba jednak dodać, że istnieją sieci miejscowe dla których zdefiniowano więcej warstw.



HART (ang. Highway Addressable Remote Transducer)



Format ramki

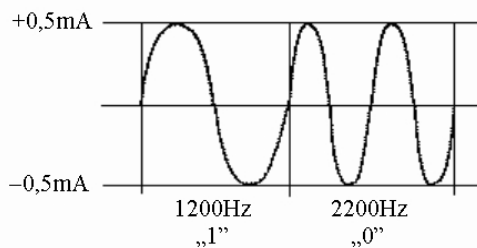
	Model OSI	Sieć miejscowa HART
7	Warstwa aplikacji	Instrukcje
6	Warstwa prezentacji	
5	Warstwa sesji	
4	Warstwa transportowa	
3	Warstwa sieciowa	
2	Warstwa łącza danych	Reguły protokołu HART
1	Warstwa fizyczna	Bell 202

Protokół komunikacyjny HART® (Highway Addressable Remote Transducer) opracowano w firmie Rosemount w roku 1986. Stanowi on zgodnie z zamysłem twórców naturalne rozszerzenie przemysłowego standardu analogowego 4-20mA o cyfrową komunikację z „inteligentnymi” (mikroprocesorowymi) układami wejścia/wyjścia. Wspomniany standard ma już długą historię oraz bardzo dużo aplikacji w przemyśle, głównie chemicznym i pomimo rozwoju technik cyfrowych pojawia się również w nowych instalacjach.

Architekturę różnych sieci najczęściej porównuje się z modelem odniesienia OSI. Model ten nie uwzględnia specyfiki sieci miejscowych, które z założenia są sieciami czasu rzeczywistego, a ponieważ przeznaczone są do pracy w warunkach przemysłowych muszą charakteryzować się zwiększoną odpornością na zakłócenia. Różnice dotyczą też fizycznych środków łączności i topologii sieci. Przy uwzględnieniu tych różnic model OSI stanowi użyteczną bazę odniesienia. Sieć HART stosuje tylko trzy warstwy, 1, 2 i 7.

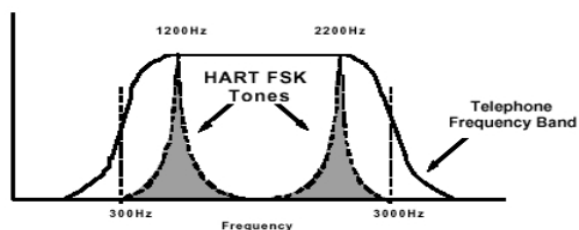


## HART (ang. Highway Addressable Remote Transducer)



Sygnał analogowy

Modulacja w sieci HART



Widmo sygnału HART

Pasma telefoniczne

Zygmunt Kubiak

Protokoły w systemach wbudowanych (6)

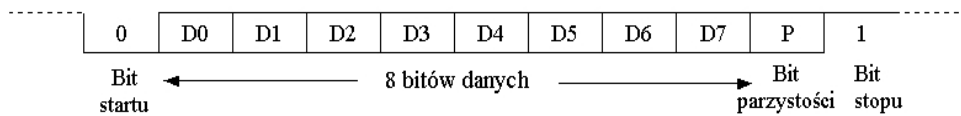
Warstwa fizyczna dotyczy technicznych aspektów przesyłania danych w postaci strumienia bitów. HART wykorzystuje modulację FSK (ang. Frequency Shift Keying). Przyjęto standard Bell 202. Jest to metoda kluczenia częstotliwości z fazą ciągłą: jeden cykl 1200Hz reprezentuje binarne 1, natomiast dwa cykle 2200Hz - binarne 0. Taki dobór częstotliwości pozwala na uniknięcie, tzw. zniekształceń włączeniowych.

Standard Bell 202 opracowano w USA dla potrzeb transmisji cyfrowej w sieci telefonicznej. Powstało szereg modemów scalonych dla tego standardu. Najbardziej popularne to SYM20C15 z firmy Symbios Logic, HT20C12 z SMAR Research Corp. oraz FX614 z CML Semiconductor Products. Przyjęcie takiego rozwiązania pozwala na bezproblemowe przekazywanie ramek HART poprzez sieć telefoniczną.

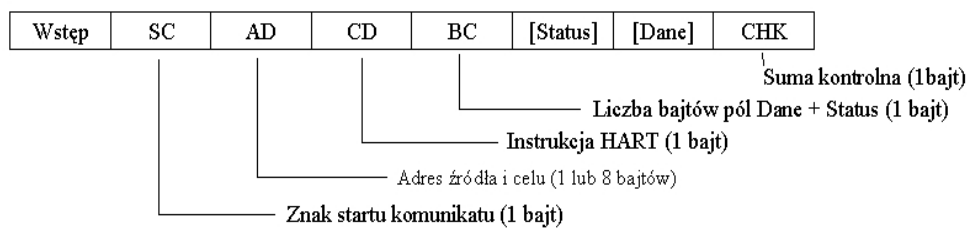
Sieć HART może pracować w konfiguracji „punkt-punkt” (pojedynczy układ slave o adresie 0) albo „wielopunkt” zrealizowany na magistrali dwu- lub trzyprzewodowej. Pierwszy sposób stosowany jest wspólnie z transmisją analogową 4-20mA. Pasma sygnału analogowego ograniczone jest do 25Hz. W drugim przypadku, w którym dopuszczona jest tylko transmisja cyfrowa, do sieci może być dołączonych maksymalnie 15 modułów. Każdy z nich musi mieć inny adres; dla pierwotnego master'a zarezerwowany jest adres 1, a dla wtórnego - 0. Moduły slave przełączone zostają do trybu stałego obciążenia prądem 4mA (instrukcja #6).



## HART (ang. Highway Addressable Remote Transducer)



Format znaku



Struktura komunikatu HART

Zygmunt Kubiak

Protokoły w systemach wbudowanych (7)

Strumień bitów komunikatu HART dzielony jest na bajty (8 bitowe znaki), z których każdy jest kodowany zgodnie z regułami stosowanymi w układach UART: 1 bit startu, 8 bitów danych, 1 bit parzystości i 1 bit stopu.

Komunikat rozpoczyna się wstępem, którego długość wynosi 5 lub 20 bajtów (przy braku synchronizacji); same znaki FFH. Specyfikacja HART przewiduje dwa rodzaje formatu ramki: krótki i długi. Formaty różnią się polem adresu. Znak startu (pole SC) służy do rozróżnienia kierunku transmisji (M → S lub S → M), zaznaczenia czy ramka została wygenerowana w trybie cyklicznego generowania odpowiedzi przez moduł slave (ang. burst) oraz określenia formatu ramki. Adres dla formatu krótkiego ma długość 1 bajtu. Najstarszy bit jest adresem master'a („1” - pierwotny, „0” - wtórny). Kolejny bit BM służy do przełączania slave z/do trybu „burst”. Następne dwa bity są zerami, a cztery ostatnie to pole adresu slave. Adres ramki długiej definiuje dwa pierwsze bity jak wyżej. Pozostałe sześć bitów oznacza producenta. Drugi bajt określa typ urządzenia. Dalsze sześć bajtów to unikatowy numer modułu slave. Pole statusu (2 bajty) występuje opcjonalnie w odpowiedzi modułu slave i dotyczy jego stanu. Pole danych może zawierać 0 - 25 bajtów, a treść jest zdefiniowana w polu instrukcji.

Protokół HART może być użyty różnych trybach komunikacyjnych. Przewidziano możliwość stosowania dwóch modułów master (pierwotny i wtórny). Wtórny master w postaci podręcznego komunikatora może być użyty bez zakłócania komunikacji z masterem pierwotnym, służy do monitorowania i konfigurowania pracy systemu. Oba moduły master mają różne adresy, co pozwala na identyfikację odpowiedzi modułu (modułów) slave na rozkazy każdego z nich. Najczęściej stosowanym trybem jest komunikacja cyfrowa master-slave, realizowana jednocześnie z transmisją analogową 4-20mA. Odpowiada to konfiguracji sieciowej „punkt-punkt”. W tym przypadku można wyróżnić dwa węzły analogowe i dwa węzły cyfrowe. Protokół HART może być też użyty w konfiguracji „wielopunkt” zrealizowany na magistrali, ale wtedy mogą występować wyłącznie węzły cyfrowe. Opcjonalnym trybem komunikacyjnym jest „burst”, w którym pojedynczy moduł slave cyklicznie wysyła standardowe komunikaty. Szczelina czasowa między komunikatami umożliwia modułowi master zmianę rozkazu lub trybu.



## Model sieci ASi

## Model OSI

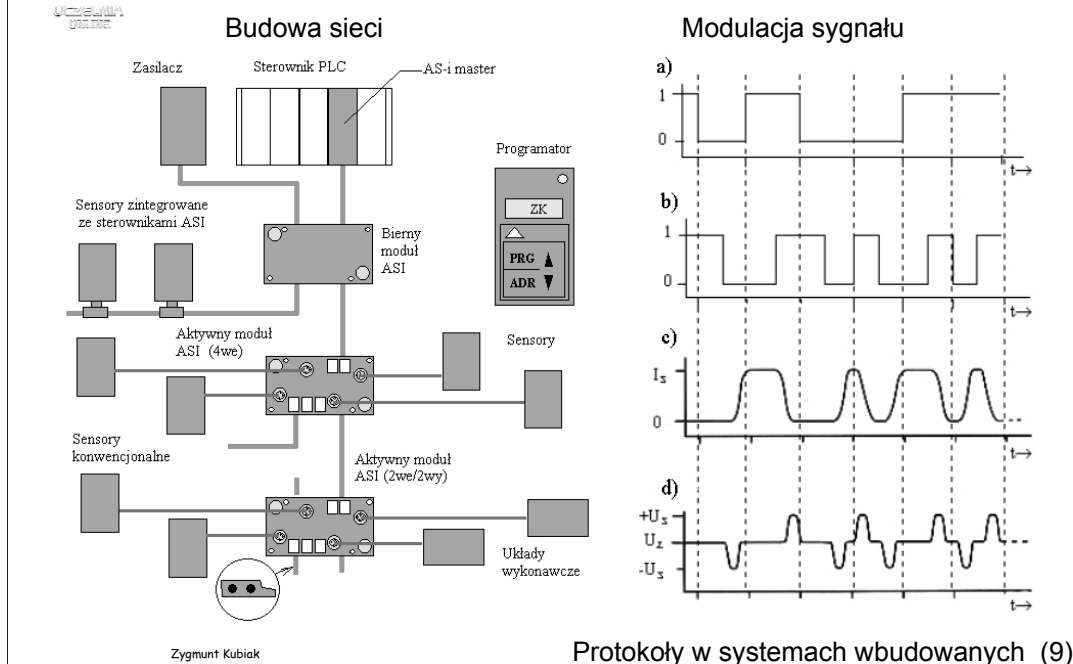
7	Warstwa aplikacji
6	Warstwa prezentacji
5	Warstwa sesji
4	Warstwa transportowa
3	Warstwa sieciowa
2	Warstwa łącza danych
1	Warstwa fizyczna

## Sieć miejscowa AS-i

Instrukcje
Reguły protokołu AS-i
Modulacja PE, APM

Sieć ASi należy do najprostszych sieci miejscowych – łączy punkty binarne. Metodą dostępu stacji do sieci AS-i jest odpytywanie (ang. polling). Jedną ze stacji jest wyróżniona i pełni rolę zarządcy (ang. master), może to być dodatkowy moduł sterownika PLC. Pozostałe węzły są podległe (ang. slaves). Master posiada pełną listę adresów stacji dołączonych do sieci i odpytuje kolejne slave, przekazując w ten sposób zgodę na transmisję w sieci. Jeden master może obsługiwać do 31 punktów podległych, tzw. modułów, które mogą zawierać układy wyjściowe albo wejściowe. Węzeł może obsługiwać 4 punkty binarne, tzn. 2 wejścia i 2 wyjścia, 4 wejścia lub 4 wyjścia. Każdy moduł musi mieć swój adres (1-31) zapisany np. w pamięci EEPROM. Moduły mogą tworzyć sieć o konfiguracji liniowej, gwiazdowej lub drzewiastej. Jako łącze stosowany jest specjalny dwużyłowy ( $2 \times 1,5 \text{ mm}^2$ ), nieekranowany, profilowany kabel o długości do 100m (300m z regeneratorem). Zalety takiego rozwiązania są następujące: prosty montaż i serwis okablowania, szybki i prawidłowy montaż modułów węzłowych sieci, prosta diagnostyka sieci, łatwa rekonfiguracja oraz duża odporność na uszkodzenia mechaniczne. Wadą przyjętego kabla jest mniejsza, w porównaniu ze skrętką, odporność na zakłócenia elektromagnetyczne. Zostało to zrekompensowane przez zwiększenie napięcia zasilania (30V DC) oraz zastosowanie dużych prądowych (60mA) sygnałów sterujących.

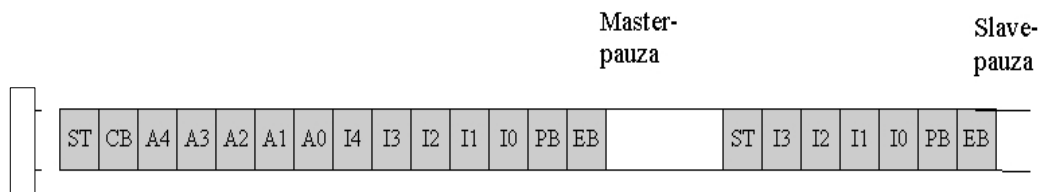




W sieci AS-i realizowana jest transmisja w paśmie podstawowym. Właściwości transmisyjne naturalnego kodu binarnego nie są najlepsze: ma on składową stałą, liczba kolejnych elementów '0' i '1' nie jest ograniczona i dlatego nie gwarantuje prawidłowej synchronizacji odbiornika. Z drugiej strony, torem transmisyjnym dla AS-i jest para przewodów, którą przesyłane są zarówno dane jak i zasilanie. Powyższe przyczyny powodują konieczność stosowania kodu transmisyjnego. Przyjęto kod PE (ang. Phase Encodage) zwany też kodem Manchester. Reguła kodowania jest następująca: '1' kodowana jest jako przejście w środku bitu, od poziomu niższego do wyższego, '0' - odwrotnie. Zaletą takiego kodowania jest co najmniej jedno przejście dla każdego bitu. Przebiegi w nadajniku kontrolera magistrali AS-i pokazano na rysunku. Słowo nadawane, w naturalnym kodzie binarnym (rys.a), kodowane jest według reguł kodu PE (rys.b) a następnie podawane na filtr dolnoprzepustowy. Przebieg ten o ograniczonym paśmie wchodzi na konwerter U/I, na którego wyjściu otrzymujemy prąd  $I$  z przedziału (0...60) mA. Takie zmiany prądu są forsowane na magistrali (rys.c). Oddziaływanie między wyjściem nadajnika a specjalnym zasilaczem z odpowiednio dobraną wartością indukcyjności wyjściowej prowadzi do uzyskania naprzemiennej modulacji impulsowej (APM - ang. Alternate Puls Modulation) napięcia zasilającego (rys.d). Modulacja APM odpowiada różniczkowaniu przebiegu z rys.c. Amplituda impulsów napięciowych w torze transmisyjnym wynosi około 2V.



## Format ramki



- ST - bit startu, zawsze ST=0,  
 CB - bit sterujący, 0 - transmisja dane/parametry, 1 - instrukcja sterująca,  
 A0...A4 - adres modułu slave, 01H...1FH - AS-i-slave 1 ... AS-i-slave 31,  
 I0..I4 - bity informacyjne zależne od typu wywołania,  
 PB - bit parzystości, testowane są bity bez ST i EB, 0 - parzysta liczba '1',  
 EB - bit stopu, zawsze EB=1.

Master wysyła telegram zaopatrzonego w adres modułu slave. Odpowiada wyłącznie wskazany moduł. Ta prosta metoda ściśle determinuje czas dostępu każdego punktu do magistrali. Dla sieci AS-i przyjęto częstotliwość zegara równą 167kHz co daje czas trwania jednego bitu 6μs. Master-pauza wynosi co najmniej 3 i maksymalnie 10 odcinków jednostkowych. Jeśli slave jest zsynchronizowany, wtedy już po trzech odcinkach bitowych przełącza się na nadawanie odpowiedzi. Przy braku synchronizacji wymagane są dwa dodatkowe bity. Jeśli master nie otrzyma bitu startowego odpowiedzi w ciągu 10 bitów pauzy, przechodzi do następnego wywołania. Slave-pauza trwa tylko jeden odcinek czasowy. Czas cyklu dostępu w sieci AS-i zależy od liczby modułów podrzędnych; przy pełnej obsadzie 31 modułów czas cyklu wynosi około 5ms.

W systemach sterowania istotnym problemem jest zapewnienie wysokiej wiarygodności przekazywanych danych. Zabezpieczenie transmitowanych w sieci AS-i ramek może wydawać się słabe. W rzeczywistości wprowadzenie kodowania transmisyjnego PE i końcowego APM powoduje, że istnieje więcej stref kontroli wynikowego ciągu. W łatwy sposób można wykryć brak transmisji - brak składowej zmiennej. Przyjmuje się następujące kryteria testowania ramek transmitowanych w kodzie APM:

- pierwszy impuls telegramu musi być impulsem ujemnym,
- kolejne pary impulsów muszą mieć przeciwną polaryzację,
- odstęp między sąsiednimi impulsami nie może przekraczać 0,5 okresu zegara,
- w drugiej połowie bitu (w odniesieniu do nadawanego słowa) zawsze musi wystąpić impuls,
- liczba dodatnich impulsów, bez bitów ST i EB musi być parzysta,
- ostatni impuls słowa kodowego musi być dodatni,
- po bicie stopu (EB) nie może być impulsów (dotyczy pauzy).

Następnie po przekodowaniu ciągu z kodu APM na kod PE i dalej na kod binarny, realizowana jest kontrola parzystości odebranej ramki.



## Zestawienie standardów opartych na specyfikacji CAN

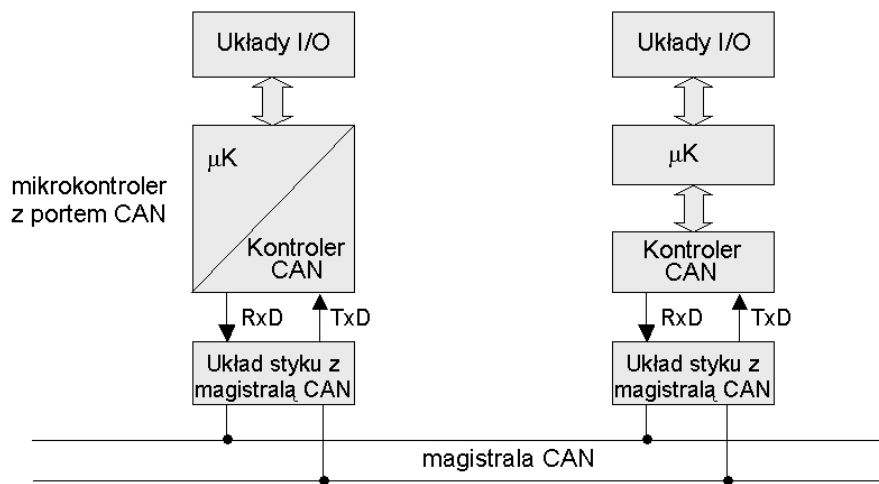
Nazwa sieci	Prędkość b/s	Medium transmisyjne	Nad./odb. układ transm.	Obszar zastosowań
SAE J1939-11	250k	2ps, ek	250	Pojazdy ciężarowe i specjalne, autobusy
SAE J1939-12	250k	2ps, ek, zs 12V	250	Rolnictwo - maszyny
SAE J2284	500k	2ps, nek	250	Automatyzacja - duże prędkości,
SAE J2411	25k, 40k	1p	SWC	Automatyzacja - małe prędkości
NMEA2000	62,5k, 125k, 250k, 500k, 1M	2ps, ek, zs	250	Przemysł morski, statki, okręty
Device Net	125k, 250k, 500k	2ps, sk, zs 24V	250	Automatyzacja przemysłu
CANopen	10k, 20k, 50k, 125k, 250k, 500k, 800k, 1M	2ps, ek - opcja, zs - opcja	250	Automatyzacja przemysłu
SDS	125k, 250k, 500k, 1M	2ps, ek, zs - opcja	250	Automatyzacja przemysłu
Fault Tolerant	<125k	2ps, nek	252	Komunikacja ****

Objaśnienia: 2ps - dwuprzewodowa skrętka, 1p - jeden przewód, ek - ekran, nek - bez ekranu, zs - przewody zasilania

Sieć CAN (ang. Controller Area Network) specjalnie została opracowana dla potrzeb pojazdów, w firmie Robert Bosch GmbH.). Po raz pierwszy na dużą skalę została zastosowana w roku 1990 w samochodach Mercedes S. W roku 1992 sieć CAN została zatwierdzona przez ISO jako standard międzynarodowy w normach ISO 11898 oraz ISO 11519-2. Standard CAN dotyczy głównie warstwy drugiej (DL) oraz częściowo warstwy pierwszej (PL), przy czym pierwszy z dokumentów odnosi się do rozwiązań o dużych prędkościach transmisji a drugi - małych. Ponieważ standard się sprawdził i zyskał bardzo dużą popularność, powstało wiele innych standardów definiujących pozostałe warstwy modelu sieci miejscowej. Przykładowo, standard SAE J1850 przeznaczony jest do zastosowań w samochodach osobowych, a SAE J1939 - dla ciężarówek, autobusów i ciężkich pojazdów specjalnych.



## Organizacja węzłów sieci CAN



Zygmunt Kubiak

Protokoły w systemach wbudowanych (12)

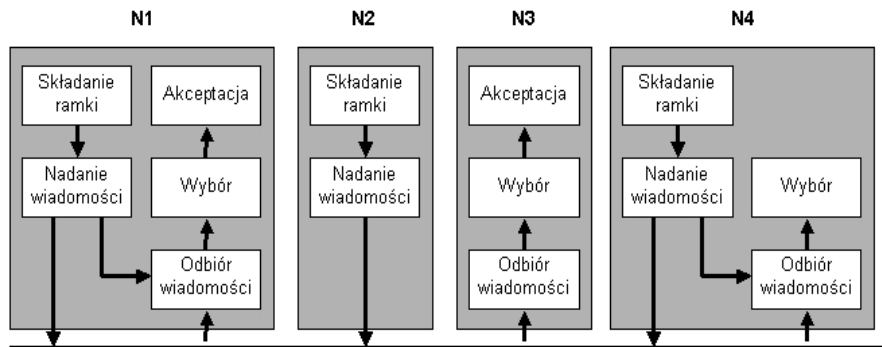
Kontrolery możemy podzielić na dwie podstawowe grupy: specyficzne - realizujące wyłącznie zadania CAN oraz uniwersalne, oparte na znanych mikrokontrolerach wyposażonych w kanały CAN. W pierwszej grupie występuje kilkanaście układów. Do najpopularniejszych należą SJA1000 (Philips), AN82257 (Intel) a także SAE81C91 (Siemens). Druga grupa układów jest znacznie bardziej liczna. Praktycznie każdy z producentów mikroprocesorów ma w swojej ofercie co najmniej jeden uniwersalny mikrokontroler z kanałami CAN. Przykłady: PIC16C185 (Microchip), 8X196CA (Intel), M37632MF (Mitsubishi), SABC164 (Siemens) czy P87C592 (Philips).

Na rysunku przedstawiono dwa ogólne rozwiązania węzłów sieci CAN. Jedno wykorzystuje uniwersalny mikrokontroler z dostępnymi portami CAN. Jest to rozwiązanie szczególnie korzystne dla dużej serii węzłów. W konstrukcjach jednostkowych, prototypowych lepsza jest druga konfiguracja oparta na specjalizowanych kontrolerach CAN i dowolnych, uniwersalnych mikrokontrolerach realizujących zadania warstwy aplikacyjnej.

Magistrala z obu stron powinna być zakończona dopasowującymi impedancjami (terminatory - ok. 120Ω). Jedną z linii oznaczana jest **CAN-H** a druga **CAN-L**. Wyjścia układów sterujących magistralą mogą znajdować się w trzech stanach logicznych: stan wysokiej impedancji, **stan dominujący** i **stan recesywny**. Stan dominujący oznacza, że różnica napięć CAN-H - CAN-L wynosi nie mniej niż 0,9V a dla stanu recesywnego napięcie różnicowe nie przekracza 0,5V. W przypadku jednoczesnego podania bitu dominującego i bitu recesywnego przez nadajniki dwóch różnych węzłów, na magistrali ustali się poziom dominujący. Opracowanych zostało wiele monolitycznych układów nadawczo-odbiorczych realizujących styk z fizyczną magistralą jak: CF150B (Bosch), MTC3054 (Alcatel Mietec), PCA82C250, PCA82C251, PCA82C252, TJA1053 (Philips), TLE6252G (Siemens), Si9200EY, B10011S (Temic Siliconix), SN75LBC031, SN65LBC031 (Texas), UC5350 (Unitrode) itd.



## Fragment przykładowej sieci CAN



Zygmunt Kubiak

Protokoły w systemach wbudowanych (13)

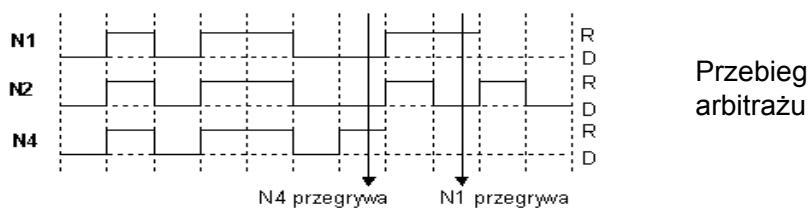
Zgodnie ze specyfikacją Bosch'a warstwa łącza danych dzieli się na dwie podwarstwy: obiektową i transferową. Do zadań podwarstwy obiektowej należy filtracja wiadomości oraz obsługa wiadomości i statusu. Podwarstwa transferu zajmuje się przygotowaniem ramki wiadomości, zatwierdzaniem i rozpakowaniem wiadomości, detekcją i sygnalizacją błędów, arbitrażem oraz prędkością transmisji i zależnościami czasowymi. CAN jest protokołem typu **M-M** (ang. multi-master) to znaczy, że poszczególne węzły sieci mogą jednocześnie żądać dostępu do magistrali. Taka sytuacja wymaga arbitrażu. Przyjęto modyfikację metody CSMA/CD (ang. Carrier Sense Multiple Access with Collision Detect), polegającą na tzw. nieniszczącym arbitrażu, który oznacza, że w przypadku wystąpienia kolizji dostęp do magistrali uzyskuje wiadomość o najwyższym priorytecie.

Dokładniej zasadę arbitrażu wyjaśni przykład. Uwzględnione zostaną cztery węzły sieci o organizacji jak na rysunku.



Identyfikatory wiadomości nadawanych i odbieranych w przykładowej sieci CAN

N1 (nad.+ odb.) - ident.wiad.nadawanych	01011001100 <sub>B</sub> =716 <sub>D</sub> =2CC <sub>H</sub> ,
ident.wiad.odbieryanych	01011001010 <sub>B</sub> =714 <sub>D</sub> =2CA <sub>H</sub> ,
N2 (tylko nad.) - ident.wiad.nadawanych	01011001010 <sub>B</sub> =714 <sub>D</sub> =2CA <sub>H</sub> ,
N3 (tylko odb.) - ident.wiad.odbieryanych	01011001xxx <sub>B</sub> =712 <sub>D</sub> ..719 <sub>D</sub> =2C8 <sub>H</sub> ..2CF <sub>H</sub> ,
N4 (nad.+ odb.) - ident.wiad.nadawanych	01011010010 <sub>B</sub> =722 <sub>D</sub> =2D2 <sub>H</sub> ,
ident.wiad.odbieryanych	01011011xx1 <sub>B</sub> =729 <sub>D</sub> ..735 <sub>D</sub> =2D9 <sub>H</sub> ..2DF <sub>H</sub> .

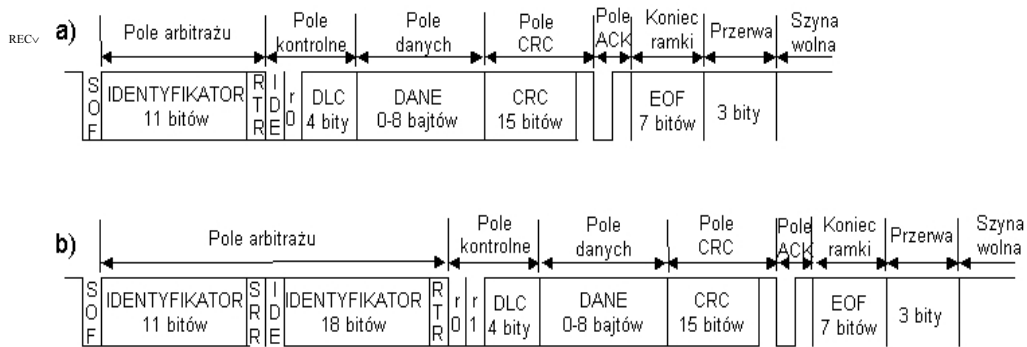


W sieci CAN podstawą transmisji jest wymiana wiadomości.

Dany węzeł może odbierać i nadawać wiele wiadomości. Odbiorniki N3 i N4 akceptują po kilka wiadomości. Załóżmy, że jednocześnie startują węzły N1, N2 i N4. Przebieg arbitrażu pokazano na rysunku. W wersji podstawowej CAN, identyfikator wiadomości zawiera 11 bitów (pole arbitrażu). Pierwsza różnica pojawia się dla N4, który wysłał bit recesywny a N1 i N2 generują bity dominujące. Na magistrali ustala się stan dominujący. N4 przegrywa - następuje wyłączenie nadajnika. Nadal rywalizują N1 i N2. Dostęp do magistrali uzyskuje wiadomość nadawana przez węzeł N2. Widać następującą zależność: im niższy numer identyfikatora tym wyższy priorytet wiadomości. Węzły N1, N2, N4 nadają wiadomości, które są odbierane przez N1 i N3. Węzeł N4 analizuje również wiadomości na magistrali ale ich nie akceptuje - oczekuje na inne wiadomości (o identyfikatorach 729<sub>D</sub>..735<sub>D</sub>).



Formaty ramek wiadomości: a) ramka formatu standardowego (CAN 2.0A),  
b) ramka formatu rozszerzonego CAN 2.0B),



Zygmunt Kubiak

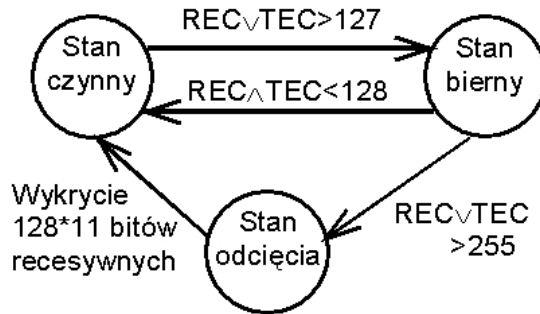
Protokoły w systemach wbudowanych (15)

Wiadomości przekazywane są przy pomocy ramek w formacie standardowym (CAN 2.0A) lub w formacie rozszerzonym (CAN 2.0B). Różnią się identyfikatorem - 11 lub 29 bitów (rys. 5) co pozwala na rozróżnienie bardzo dużej liczby wiadomości. Ograniczenie wynika jedynie z warstwy fizycznej. W praktyce znaczna długość identyfikatorów pozwala na kodowanie dodatkowych informacji dotyczących wiadomości lub węzłów (typ wiadomości, rodzaj sensora czy np. kod producenta). W sieci CAN nie ma adresowania konkretnych węzłów, a każda wysłana wiadomość może być odebrana przez dowolny moduł. Akceptacja danych zależy wyłącznie od ustawienia układu wyboru w odbiorniku węzła.

Ramka rozpoczyna się od bitu dominującego SOF (ang. start of frame). Dalej następuje pole arbitrażu, które jest wykorzystywane przy rozstrzygnięciu ewentualnych konfliktów z dostępem do sieci oraz służy do identyfikacji wiadomości w sieci. Bit RTR rozróżnia ramkę z danymi (bit dominujący) od ramki zdalnej (bit recesywny). Format ramki określany jest przez bit IDE (bit dominujący - ramka standardowa, bit recesywny - ramka rozszerzona). Bit SRR wysyłany jest jako recesywny. Bity rezerwowe r0 i r1 są ustawione jako dominujące. Pole kontrolne definiuje liczbę bajtów danych. Zawartość DCL w zakresie 0..7 bezpośrednio równa jest liczbie bajtów, natomiast wartość 8..15 oznacza 8 bajtów. To umożliwi kodowanie dodatkowych informacji. Szczególne znaczenie ze względu na wiarygodność danych ma pole CRC. Bit 16-ty kończący to pole (ogranicznik) jest recesywny. Kontrola dla pól od SOF do pola danych (jeśli występuje) włącznie, realizowana jest przy pomocy kodu cyklicznego. Pole potwierdzenia (ACK) zawiera 2 bity: ACK i bit ogranicznika. Po wysłaniu ramki nadajnik wysyła 2 recesywne bity pola ACK. Odbiornik, który poprawnie odebrał wiadomość odpowiada w tym samym czasie dominującym bitem ACK. Dzięki temu nadajnik uzyskuje potwierdzenie, że przynajmniej jeden węzeł poprawnie odebrał wiadomość. Pole EOF składa się z 7 recesywnych bitów kończących ramkę.



## Stany węzłów przy obsłudze błędów CAN



## Typy wykrywanych błędów:

- stanu bitu,
- szpikowania bitami,
- kontroli kodowej (CRC),
- potwierdzenia (ACK),
- formatu ramki.

Zygmunt Kubiak

Protokoły w systemach wbudowanych (16)

Ważnym zadaniem warstwy łącza danych jest obsługa błędów. Gdy którykolwiek z węzłów wykryje błąd generowana jest specjalna ramka błędu, zawierająca flagę błędu (6 bitów dominujących). Bity dominujące flagi błędu powodują nadpisanie uszkodzonej ramki i wymuszają powtórzenie transmisji. Każdy z węzłów przeprowadza kontrolę bitów.

Błąd stanu bitu występuje, jeśli nadajnik wyśle bit dominujący a odbierze recesywny albo wyśle recesywny a odbierze dominujący. Wyjątkiem od tej zasady jest sekwencja arbitrażu.

Błąd szpikowania zachodzi wtedy, gdy w ciągu bitów między SOF a ogranicznikiem CRC pojawi się więcej niż 5 takich samych bitów - odbiornik stwierdza naruszenie zasady szpikowania.

Odbiornik na podstawie ciągu CRC sprawdza czy w ramce nie nastąpiło przekłamanie. Mimo znacznej odległości Hamminga równej 6, kod wykorzystywany jest wyłącznie do wykrywania błędów a nie do korekcji.

Odbiornik, który poprawnie odbierze dane ustawia bit ACK jako dominujący. W ten sposób nadajnik uzyskuje potwierdzenie poprawnej transmisji; w przeciwnym wypadku nadajnik wysyła ramkę błędu.

W ramce występują bity, które mają znane wartości. Zmiana tych bitów oznacza błąd formatu ramki.

W celu odróżnienia błędów chwilowych od trwałych kontrolery CAN wyposażone są w dwa liczniki: licznik błędów odbioru (**REC** - Receive Error Counter) oraz licznik błędów nadawania (**TEC** - Transmit Error Counter). Liczniki zwiększają swoją zawartość przy błędzie odpowiedniej operacji i zmniejszają ją przy poprawnej operacji. W zależności od stanu licznika może zmienić się stan węzła. Węzły mogą znajdować się w trzech stanach – stan czynny, stan bierny, stan odcięcia. Stan czynny ( $REC = TEC < 128$ ) jest normalnym stanem węzłów - są w pełni aktywne. Gdy sieć działa bez zakłóceń  $REC = TEC = 0$ . W stanie pasywnym ( $127 < REC < TEC < 255$ ) węzły nadal nadają i odbierają wiadomości. Różnica polega na tym, że w przypadku błędu, węzeł czynny wysyła czynną ramkę błędu (z czynną flagą błędu - 6 bitów dominujących) a węzeł bierny wysyła bierną ramkę błędu (z bierną flagą błędu - 6 bitów recesywnych). Przekroczenie zawartości  $REC > TEC > 255$  powoduje przejście węzła do stanu odcięcia.

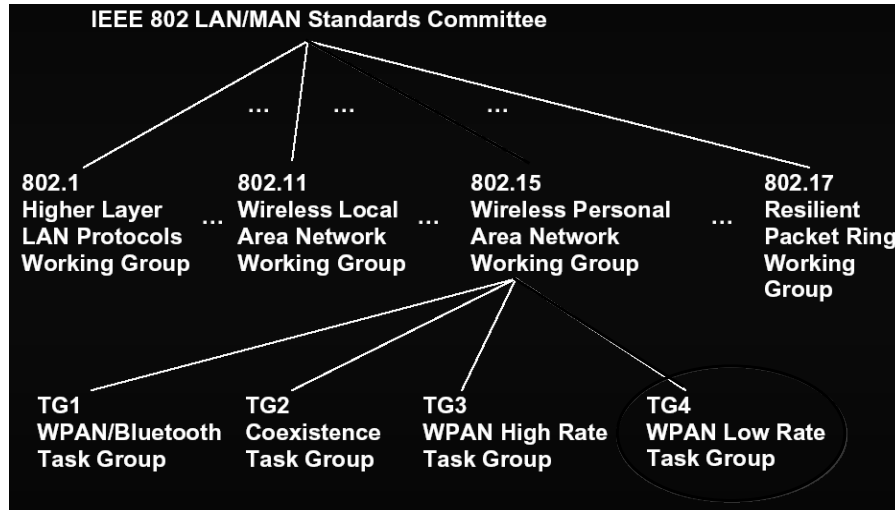




## Zestawienie przykładowych sieci miejscowych

Sieć	AS-i	CAN	LonWorks	Modbus	Profibus DP
Medium fizyczne	spec. dwużyłowy kabel bez ekranu	skrętka + zasilanie	skrętka, światłowód, sieć elektrycz.	skrętka + zasil. RS-485	skrętka, światłowód + zasilanie.
Topologia	magistrala, gwiazda	magistrala	magistrala, gwiazda	magistrala	magistrala
Szybkość trans	167kbit/s	1Mbit/s	1,25Mbit/s.	19,2kbit/s.	12Mbit/s
Standard	EN 50295	ISO 11898 i ISO 11519-2			EN50170
Rok wprov.	1994	1994	1991		1994
Metoda dostępu do sieci	odpytywanie (M.-S.)	priorytetowy CSMA (M.-M.)	CSMA/CD, priorytet (M.-M.)	odpytywanie (M.-S.)	przesyłanie znacznika (M.-S.)
Liczba węzłów	31 (62 dla v.2.1)	255	32385	247	127
Rozmiar segmentu	100m., (300m z regeneratorem)	1000m. przy ≤ 50kbit/s	1200m. przy ≤ 78kbit/s	1800m	1200m. ≤ 93,75kbit/s

Porównywanie różnych sieci z reguły jest trudne ze względu na ich specyfikę. Można jednak znaleźć cechy, które dostarczają informacji. Należą do nich: Topologia, Szybkość transmisji, Metoda dostępu. Inne jak Liczba węzłów czy Rozmiar są już bardziej kłopotliwe do określenia ze względu np. na możliwość tworzenia złożonych sieci z segmentów.



Bluetooth

UWB

ZigBee

Zygmunt Kubiak

Protokoły w systemach wbudowanych (18)

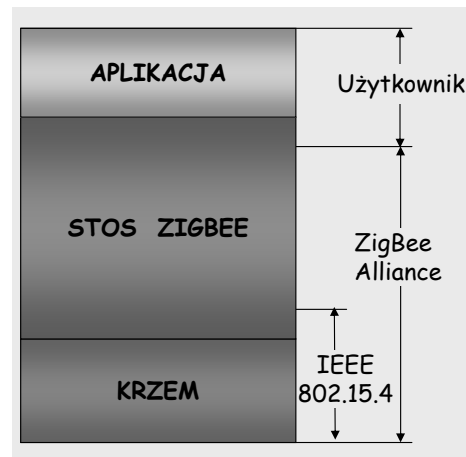
Prace nad standaryzacją bezprzewodowych sieci sensorów rozpoczęła grupa Zigbee Alliance w roku 1998. ZigBee Alliance jest stowarzyszeniem firm działających dla opracowania i rozwijania otwartego standardu dotyczącego transmisji bezprzewodowej niskiej mocy, efektywnej pod względem kosztów. W roku 2001 prace dotyczące warstw niższych zostały oddzielone od prac nad protokołami warstw wyższych. Specyfikacja dotycząca niższych warstw została wydana w 2003 r., a ZigBee w 2005 r.



## Sieć bezprzewodowa ZigBee / IEEE 802.15.4

◆ ZigBee Alliance jest stowarzyszeniem skupiającym aktualnie ponad 150 uczestników. Promotorzy ZigBee: Chipcon, Ember, Freescale, Honeywell, Mitsubishi, Motorola, Philips i Samsung

- ZigBee Alliance
  - Definiuje górne warstwy stosu protokołów: styk warstwy sieciowej z aplikacją, zadania warstwy sieciowej, bezpieczeństwo transmisji
- IEEE 802.15.4
  - Definiuje dolne warstwy stosu protokołów: warstwa MAC (Medium Access Control Layer) oraz warstwa fizyczna PHY (Physical Layer)



Zygmunt Kubiak

Protokoły w systemach wbudowanych (19)

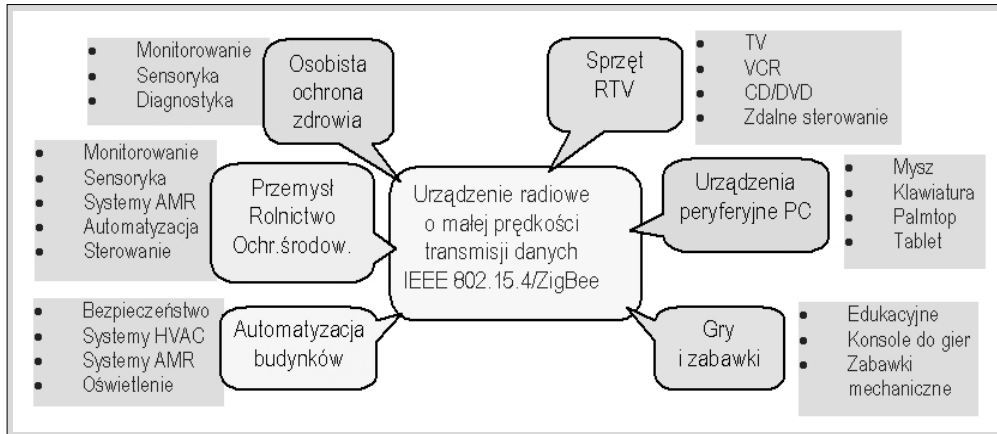
ZigBee jest stosem protokołów opartych na standardzie IEEE 802.15.4, opisującym warstwę fizyczną (PHY – Physical Layer) oraz warstwę dostępu do medium (MAC – Medium Access Control Layer). Zatwierdzony w roku 2003 standard IEEE 802.15.4, definiuje prosty lecz silny protokół pakietowy o następujących właściwościach:

- wysoka niezawodność poprzez potwierdzanie odbioru,
- mechanizmy zapewniające integralność i poufność transmisji,
- transmisja z rozpraszaniem widma metodą sekwencji bezpośredniej,
- łączność oparta na priorytetach,
- zdolność zmiany częstotliwości dla uniknięcia interferencji

Norma IEEE 802.15.4 pozwala stosować 16-bitowy adres skrócony węzła lub 64-bitowy adres rozszerzony.

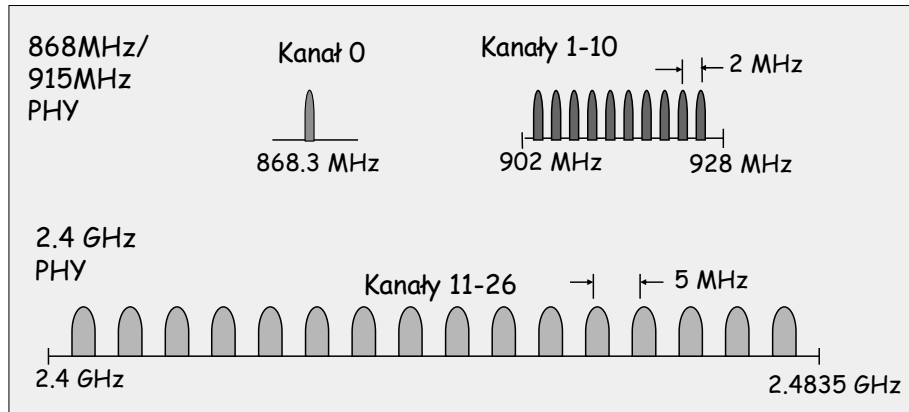
ZigBee rozszerza możliwości protokołu IEEE 802.15.4 o zagadnienia realizacji różnych struktur sieciowych, bezpieczeństwa transmisji oraz organizuje interfejs z warstwą aplikacyjną. To co wyróżnia rozwiązania ZigBee wśród innych sieci bezprzewodowych to następujące parametry:

- bardzo niski pobór mocy (baterie starczą od 6 miesięcy do kilku lat);
- urządzenie ZigBee ma tylko dwa tryby pracy: albo jest active (nadawanie/odbieranie) albo sleep; w przypadku Bluetooth występuje wiele różnych trybów co zdecydowanie utrudnia optymalizację poboru mocy;
- niski koszt urządzeń, instalacji i eksploatacji;
- możliwa duża gęstość węzłów sieci;
- prosty protokół i łatwa implementacja; stos kodu protokołu jest szacowany na około ¼ w stosunku np. do Bluetooth;
- niezawodny transfer danych;
- wysoki poziom bezpieczeństwa transmisji.



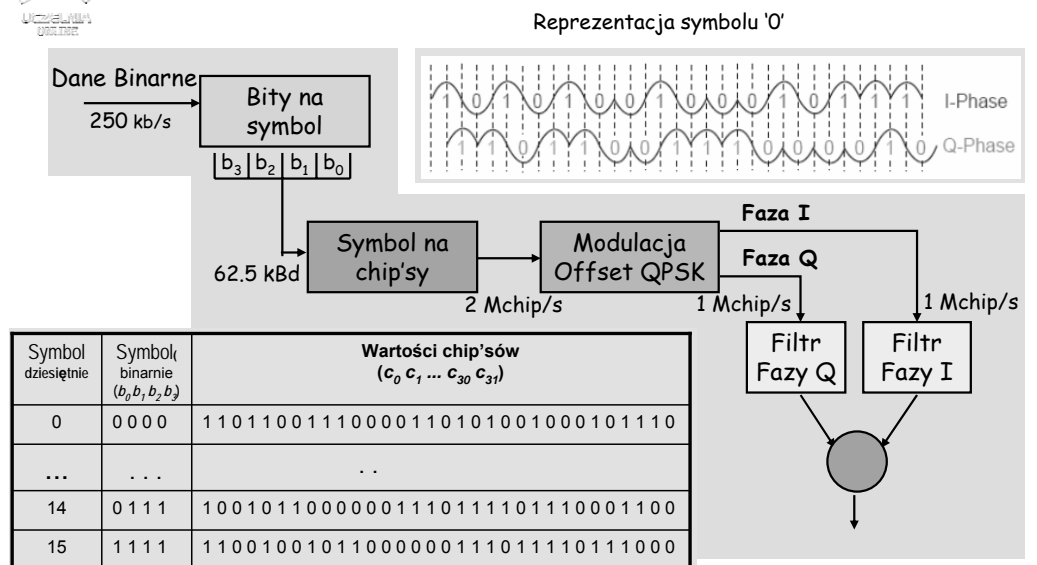
Obszary zastosowań rozwiązań IEEE 802.15.4/ZigBee; oznaczenia: AMR (ang. Automatic Meter Reading) – automatyczny odczyt liczników, HVAC (ang. Heating, Ventilation and Air Conditioning) - klimatyzacja

ZigBee uważany jest za standard, który ma szansę stać się globalnym rozwiązaniem dla wielu zastosowań. Obszary zastosowań obejmują bardzo różne dziedziny od przemysłu, rolnictwa, ochrony środowiska, automatyzacji budynków, poprzez ochronę zdrowia, obsługę sprzętów domowych po gry i zabawki.



Pasma ISM - Industrial Scientific Medic  
Europa - 868 MHz, 2,4 GHz

W warstwie fizycznej standardu IEEE zdefiniowano trzy pasma częstotliwości: 2,4GHz, 915MHz (USA) i 868MHz (Europa). W pasmach tych wydzielono łącznie 27 kanałów, ponumerowanych od 0 do 26. Szesnaście kanałów dostępnych jest w paśmie 2,4GHz, 10 w 915MHz i 1 w 868MHz (pasma ISM – Industrial Scientific Medic). Pasma te nie wymagają licencji. W Europie dostępne są dwa pasma – 868 MHz (tylko jeden kanał) i 2,4GHz. Dla celów przemysłowych, zdecydowanie lepszym pasmem jest 2,4GHz – duża liczba kanałów, większa szybkość transmisji oraz skuteczniejsza modulację (w sensie wymaganej energii na 1 bit).

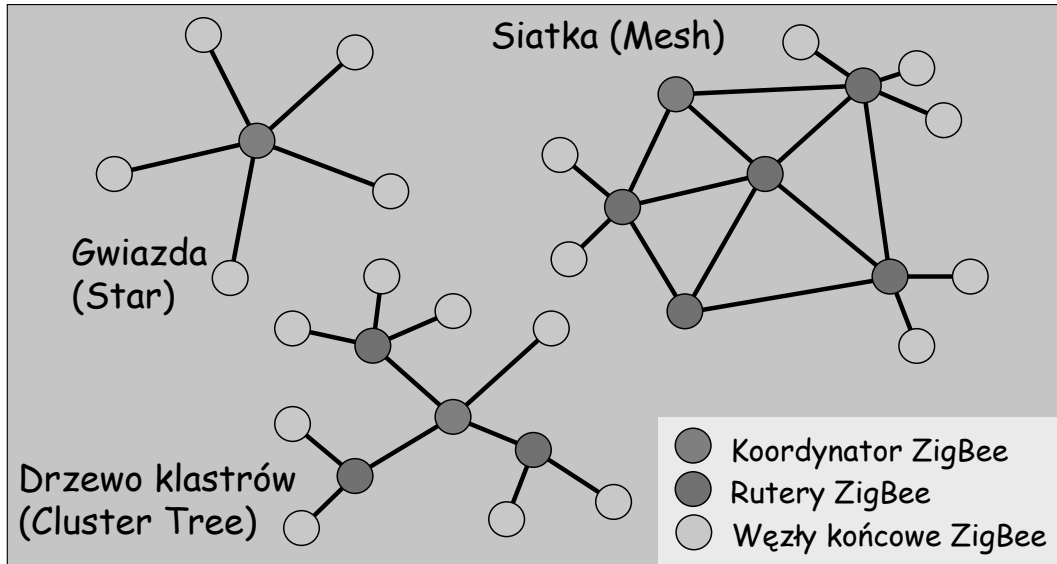


Zygmunt Kubiak

Protokoły w systemach wbudowanych (22)

Stosowana jest złożona modulacja fazowa z rozpraszaniem widma metodą sekwencji bezpośredniej DSSS (ang. direct sequence spread spectrum). W przypadku modulacji O-QPSK (ang. offset quadrature phase-shift keying) cztery kolejne bity informacyjne, tworzące tzw. symbol zastępowane są odpowiednio dobraną (1 z 16) sekwencją 32 bitów (ang. chips). Daje to możliwość pracy przy słabym współczynniku S/N (ang. signal to ratio, stosunek sygnału do szumu), wynikającym albo z powodu zakłóceń albo niskiej mocy nadajnika.

Dla wielobajtowych pól danych najpierw transmitowany jest bajt najmłodszy. Każdy bajt dzielony jest na czterobitowe symbole. Młodszy symbol transmitowany jest jako pierwszy. Następnie symbolowi przyporządkowywana jest 32-elementowa reprezentacja. Jako pierwszy transmitowany jest najmłodszy chip  $c_0$ . W modulacji O-QPSK, każdy komponent (chip) reprezentowany jest w postaci połówki sinusoidy. Dokładniej, zamiast jednego ciągu komponentów stosowane są dwa przesunięte względem siebie o 90 stopni. Komponenty o numerach parzystych nazywane są fazowymi (ang. in-phase (I)), natomiast nieparzyste - kwadraturowymi (ang. quadrature (Q)).



ZigBee umożliwia tworzenie złożonych sieci logicznych z komunikacją wielokrotnych przeskoków (ang. multi-hop), co oznacza, że nie wszystkie stacje znajdują się we wzajemnym zasięgu, a zatem może się zdarzyć, że transmisja będzie wymagała wykorzystania węzłów pośredniczących, przekazujących ruch od nadawcy w kierunku odbiorcy. Wymaga to realizacji algorytmów trasowania. Jednym z rozwiązań jest algorytm rutowania obsługi drzewa klastrów; drugi to wersja algorytmu AODV (ang. Ad hoc On Demand Distance Vector).

## Systemy wbudowane



## Sieć bezprzewodowa ZigBee / IEEE 802.15.4

Nazwa Standard	GPRS/GSM 1xRTT/CDMA	WiFi™ 802.11b/ag	Bluetooth™ 802.15.1	ZigBee™ 802.15.4	UWB™ 802.15.3
Pasma (GHz)	0,9 / 1,8	2,4 / 5	2,4	0,868 (Europa) 0,915 (Ameryka) 2,4	3,1 – 10,6
Zasoby systemu	>16MB	>1MB	>250kB	4kB – 32kB	<30kB
Zasilanie bateryjne (dni)	1 - 7	0,5 - 5	1 - 7	100 – 1000+	<3
Rozmiar sieci	1	32	7	255 / 65 000 ~ nielimitowany	236
Topologia	Punkt- punkt	Punkt- wielopunkt	Ad hoc piko sieci	Ad hoc, gwiazda, peer-to-peer, siatka	Peer-to-peer
Szybkość transmisji (kb/s)	64 – 128+	11k / 54k	720	20 - 250	100k – 500k
Zasięg (m)	>1000	1 - 100	1 – 10+	1 – 100+	<10m
Główne zalety	Zasięg, jakość	Szybkość, elastyczność	Koszt, wygoda	Niezawodność, moc, koszt	Szybkość, koszt
Podstawowe zastosowania	Przekazywanie głosu i danych	Web, email, wideo	PC Zamiast kabli	Monitorowanie I sterowanie	Domowy sprzęt RTV, PC, USB

Zygmunt Kubiak

Protokoły w systemach wbudowanych (24)

W przedstawionym zestawieniu warto zwrócić uwagę na trzy parametry, tzn. Zasilanie bateryjne, Rozmiar sieci, Szybkość transmisji oraz Główne zalety.