Bezpieczeństwo systemów

Wykład 3,4

Jarosław Szkoła

Wybrane protokoły komunikacyjne

- RS232
- Modbus
- I2C, IIC

RS-232

- RS-232 jest przeznaczony głównie do komunikacji między dwoma urządzeniami, w których komunikacja nie wymaga wymiany danych w dużej ilości czy też dużego zasięgu komunikacji.
- Może służyć do komunikacji między modułami w obrębie jednej maszyny, czy też jako port komunikacyjny do sterownika.
- Interfejs RS232 jest stosunkowo prosty oraz tani w implementacji.

RS-232

- Standard RS-232/TIA-232 wciąż wykorzystywany jest w szerokim zakresie w aplikacjach, dla których dopuszczalna jest stosunkowo wolna transmisja danych na krótkich odległościach, w szczególności w wysoce zaszumionym otoczeniu.
- Przykłady zastosowania tego interfejsu napotkać można w aplikacjach przemysłowych, robotyce, systemach wbudowanych oraz urządzeniach medycznych

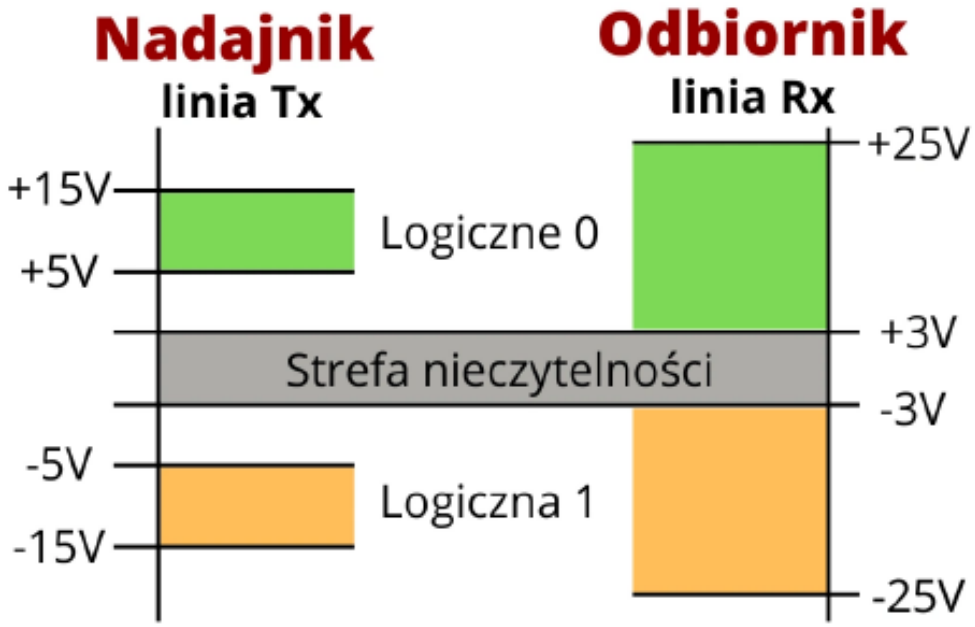
Interfejs RS-232 – Przesyłanie danych

- W standardzie RS232 (*recommended standard) zdefiniowane są dwie grupy urządzeń*
- • DTE (ang. *Data Terminal Equipment) tj. urządzeń końcowych danych np. komputer.*
- • DCE (ang. *Data Communication Equipment), czyli urządzeń komunikacji danych np. modem.*
- RS232 opisuje sposób łączenia urządzeń DTE i DCE.
- Określa on charakterystykę elektryczną (poziomy napięć), jak i fizyczną (normy wtyczek, przewodów czy nazwy sygnałów).

Poziomy logiczne interfejsu RS-232

- Przesyłane zera i jedynki logiczne w RS232 definiuje się za pomocą odpowiednich poziomów napięcia względem wspólnego poziomu masy.
- Należy zaznaczyć, że Interfejs RS232 do poprawnego działania wymaga połączenia masy komunikujących się urządzeń.
- Stan nieaktywny, odpowiadający jedynce logicznej (idle lub MARK), ma ujemny poziom sygnału w zakresie -3 do -15 V.
- Stan aktywny, zero logiczne (active lub SPACE), ma dodatni poziom sygnału w zakresie do 3 do 15 V.

Poziomy logiczne interfejsu RS-232



Poziomy napięć sygnałów w RS232

Interfejs RS-232 – Kabel, prędkość danych i zakłócenia

- Interfejs RS232 zakłada jako medium transmisyjne, skrętkę lub równoległe przewody. Długość kabla ogranicza szybkość transmisji danych i nie zaleca się przekraczać 15 m.
- Chcąc zastosować dłuższe linie komunikacyjne, należy obniżyć prędkość transmisji.
- Ważniejszym parametrem ograniczającym prędkość jest całkowita pojemność elektryczną przewodów.
- W większości zastosowań zaleca się, aby nie przekraczała ona 2500 pF, która pozwala na transmisje o prędkości 20 kbit/s.
- Z powodu niskich prędkości transmisji danych w interfejsie medium transmisyjne nie musi być traktowane jak linia transmisyjna, nie ma zatem konieczności zapewnienia dopasowania impedancji pomiędzy nadajnikiem, linią a odbiornikiem.

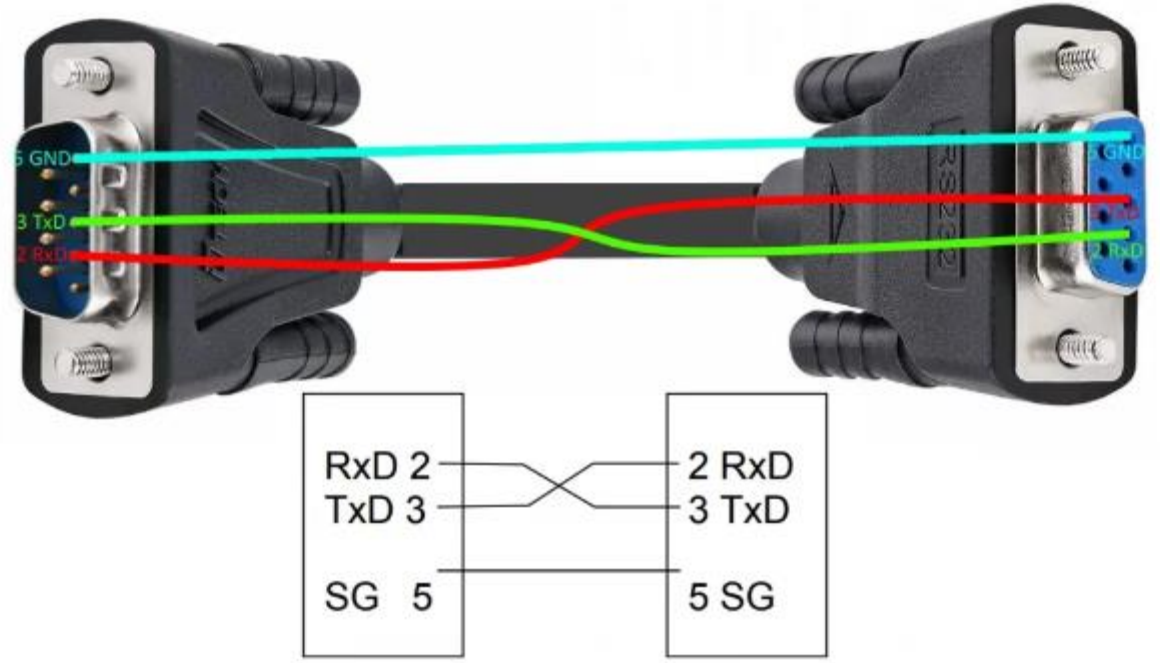
Wymiana danych w interfejsie RS-232

- Z uwagi na fakt, że w standardzie RS232 linia nadawcza Tx i odbiorcza Rx są oddzielone od siebie, wymiana danych może odbywać się w kilku trybach:
  - Tryb *full duplex* pozwala na ciągła wymianę danych na obu liniach transmisyjnych. Inaczej mówiąc, jest to dwukierunkowa transmisja jednoczesna, w tym samym czasie DTE1 – DTE2 i DTE2 – DTE1.
  - *Half duplex*, czyli dwukierunkowa transmisja niejednoczesna np. najpierw DTE1 – DTE2, a następnie DTE2 – DTE1. Czyli komunikacja gdy mamy przykładowo pytanie, a następnie odpowiedź (jak w przypadku protokołu Modbus).
  - *Simplex* to tryb, w którym urządzenie może tylko nadawać, albo tylko odbierać dane. Tylko DTE1 przekazuje dane do DTE2 lub tylko DTE2 przekazuje dane do DTE1

Wymiana danych w interfejsie RS-232

- RS-232 posiada sporą liczbę linii synchronizujących transmisję, które wykorzystywane są głównie podczas komunikacji z modemami. Dlatego realizując komunikację w standardzie RS232, możemy zastosować kilka wariantów połączenia urządzeń.
- **Wariant 3-sygnałowy.**
- Jest to wariant najbardziej podstawowy i obecnie chyba najczęściej stosowany, gdyż łączymy tylko linie Tx, Rx, i GND. Dodatkowe linie nie są potrzebne, ponieważ w obecnych czasach układy elektroniczne przetwarzają dane z tak dużą prędkością, że kontrola wymiany danych nie jest już konieczna.

Wymiana danych w interfejsie RS-232



Wymiana danych w interfejsie RS-232

- **Sprzętowy mechanizm kontroli przepływu danych** wykorzystuje, poza liniami Tx, Rx i GND, dodatkowe 2 sygnały do kontroli przepływu (flow control).
- Mogą to być sygnały RTS i CTS albo DTR o DSR.
- Jeśli nadajnik jest gotowy do wysłania danych, ustawia wtedy sygnał na linii RTS.
- Jeśli odbiornik jest gotowy do odbioru danych, ustawia sygnał na linii CTS.
- Jeżeli jeden z sygnałów nie zostanie ustawiony, przesyłanie danych nie nastąpi.
- Linie DTR, DSR, RTS, CTS i DCD umożliwiają synchronizację transmisji tak, dane były wysyłane zawsze wtedy, gdy urządzenie po drugiej stronie połączenia jest gotowe do ich odbioru.
- Sprzętowy mechanizm kontroli przepływu, z uwagi na dużą szybkość pracy układów elektronicznych nie już zbyt popularny.

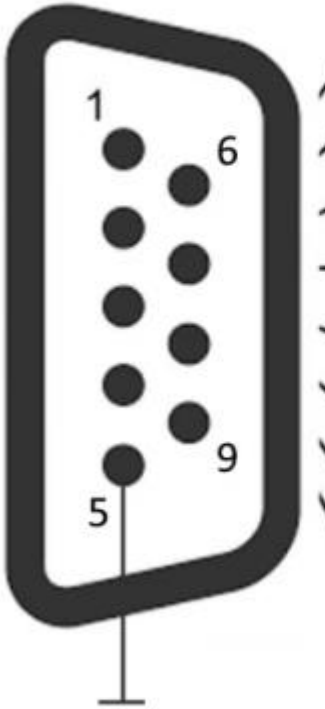
Wymiana danych w interfejsie RS-232

- **Sprzętowy mechanizm kontroli przepływu danych** wykorzystuje, poza liniami Tx, Rx i GND, dodatkowe 2 sygnały do kontroli przepływu (flow control).
- Mogą to być sygnały RTS i CTS albo DTR o DSR.
- Jeśli nadajnik jest gotowy do wysłania danych, ustawia wtedy sygnał na linii RTS.
- Jeśli odbiornik jest gotowy do odbioru danych, ustawia sygnał na linii CTS.
- Jeżeli jeden z sygnałów nie zostanie ustawiony, przesyłanie danych nie nastąpi.
- Linie DTR, DSR, RTS, CTS i DCD umożliwiają synchronizację transmisji tak, dane były wysyłane zawsze wtedy, gdy urządzenie po drugiej stronie połączenia jest gotowe do ich odbioru.
- Sprzętowy mechanizm kontroli przepływu, z uwagi na dużą szybkość pracy układów elektronicznych nie już zbyt popularny.

Wymiana danych w interfejsie RS-232

- **Sprzętowy mechanizm kontroli przepływu danych** wykorzystuje, poza liniami Tx, Rx i GND, dodatkowe 2 sygnały do kontroli przepływu (flow control).
- Mogą to być sygnały RTS i CTS albo DTR o DSR.
- Jeśli nadajnik jest gotowy do wysłania danych, ustawia wtedy sygnał na linii RTS.
- Jeśli odbiornik jest gotowy do odbioru danych, ustawia sygnał na linii CTS.
- Jeżeli jeden z sygnałów nie zostanie ustawiony, przesyłanie danych nie nastąpi.
- Linie DTR, DSR, RTS, CTS i DCD umożliwiają synchronizację transmisji tak, dane były wysyłane zawsze wtedy, gdy urządzenie po drugiej stronie połączenia jest gotowe do ich odbioru.
- Sprzętowy mechanizm kontroli przepływu, z uwagi na dużą szybkość pracy układów elektronicznych nie już zbyt popularny.

Wymiana danych w interfejsie RS-232



	OPIS	NAZWA PO POLSKU	NAZWA PO ANGIELSKU
1	DCD	Data carier detect	Wykrycie nośnej
6	DSR	Data set ready	Gotowość modemu
2	RxD	Receive data line	Odbiór danych
7	RTS	Request to send	Żądanie odbioru
3	TxD	Transmit data line	Wysyłanie danych
8	CTS	Clear to send	Gotowość wysyłania
4	DTR	Data terminal ready	Gotowość terminala
9	RI	Ring indicator	Wskaźnik dzwonka

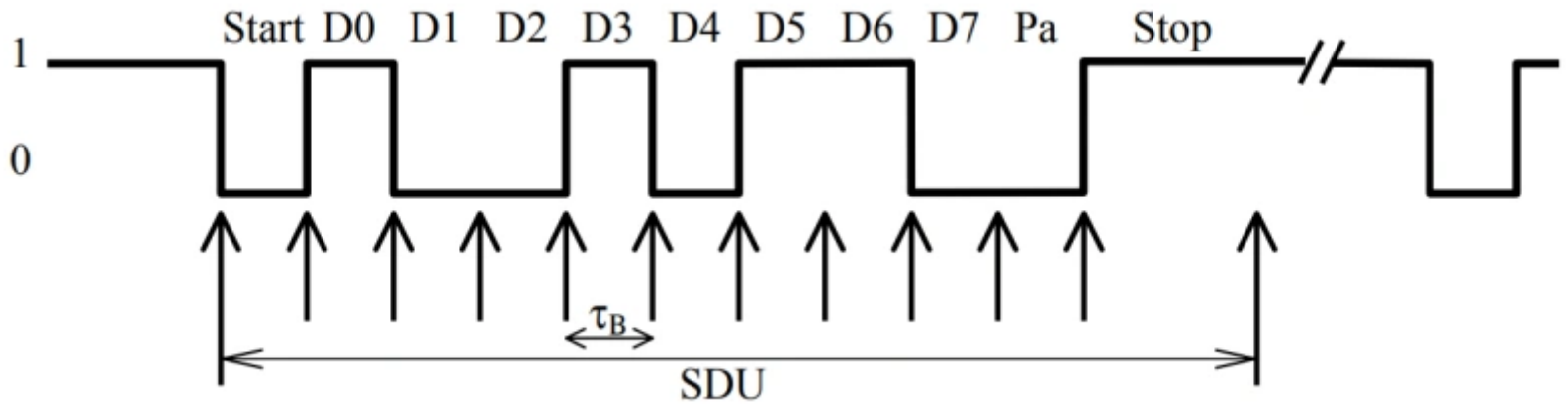
Opis sygnałów sieci RS232 we wtyczce DB9

Z UART do RS-232

- Większość urządzeń do komunikacji przez Interfejs RS232 wykorzystuje układ o nazwie UART (*Universal Asynchronous Receiver Transmitter*).
- UART stanowi wbudowaną część mikrokontrolera, a jego rola polega na konwersji typu transmisji z równoległej na szeregową i odwrotnie. Pozwala to na jednoczesną transmisję do 8 bitów danych.
- UART porządkuje bity, dodaje również uzupełniające informacje pozwalające na zarządzanie transmisją, takie jak bit start/ stop na początku i końcu transmisji, bity parzystości oraz sygnał pozwalający na określenie szybkości transmisji.
- Przesyłane bajty przez UART korzystają z napięć z zakresu TTL, czyli 0- 5V lub 0 – 3,3 V. Nadajnik interfejsu RS232 ma zakres napięć od -15 do +15, dlatego wymagany jest specjalny układ konwertujący napięcia np. MAX232

Z UART do RS-232

- Każdy znak danych zawiera od 5 do 8 bitów i poprzedzony jest bitem START, a zakończony bitem kontroli parzystości (Pa) i 1 do 2 bitami STOP.
- Bity danych wraz z bitem kontrolnym i bitami synchronizacji (start, stop) tworzą tzw. jednostkę informacyjną SDU (Serial Data Unit)



RS-232 podsumowanie

- **Zalety RS232**
  - Największą zaletą standardu RS232 jest jego prostota.
  - Można go bardzo łatwo zastosować w układach elektronicznych opartych o mikrokontrolery.
  - Format danych przesyłanych przez UART pokrywa się z formatem w standardzie RS232.
  - Wystarczy więc dodać niezbyt skomplikowaną przetwornicę napięcia.
  - Port RS232 doskonale sprawdzi jako port do aktualizacji, czy konfiguracji urządzeń jak również jako pomost łączący dwa układy elektroniczne w niedużej odległości.

RS-232 podsumowanie

- **Wady RS232**
  - Silna podatność na zakłócenia, ze względu na brak symetryczności transmisji.
  - Mały dystans transmisji wynoszący około 15 m (w zależności od prękości)
  - Możliwość komunikacji tylko między dwiema urządzeniami.
  - Problematyczność podłączenia. Wielu producentów nie zachowuje zgodności złącza z typem DTE/DCE.
  - Funkcjonowanie wielu wersji RS232 utrudnia ustanowienie połączenia.
  - Ręczna konfiguracja interfejsu szeregowego utrudnia pierwsze podłączenie urządzenia.
  - Wspólna masa sygnałowa sprawia, że istnieje większe ryzyko uszkodzenia portu jeśli nie stosujemy izolacji galwanicznej.
  - Brak możliwości zasilania urządzeń bezpośrednio z portu RS232.

RS-485

- RS-485 jest to specyficzna forma przesyłania szeregowo danych. Porównując do RS-232,
- standard ten jest szybszy, odporniejszy na zakłócenia, a największa jego zaletą jest to, że można nim przesyłać nie tylko dane pomiędzy dwoma urządzeniami.
- Umożliwia on tworzenie sieci łączących wiele urządzeń.
- Konfiguracja i specyfikacja standardu RS485 powoduje, że pracuje on bardzo szybko, umożliwiając rozszerzenie zakresu przesyłanych danych, w stosunku do RS232. Maksymalna długość przewodu komunikacyjnego przekracza znacząco 15 m i może wynieść nawet 1200 m.

RS-485

- Kolejną sprawą odróżniającą RS-485 jest brak określonej standardowej końcówki przewodu.
- Z tego powodu do łączenia tej sieci w niektórych aplikacjach spotkać można zwykłe zaciski śrubowe jako sposób podłączenia sygnałów.
- Daje to łatwość łącznia różnych urządzeń w tej sieci. Natomiast za standard, już coraz rzadziej spotykany, uważa się wtyk DB9.
- Kolejną zaletą standardu RS485 jest wspomniane wcześniej możliwość podłączenia wielu urządzeń.
- Generalnie uważa się, że do pojedynczej sieci można podłączyć 32 urządzenia, jednak w pewnych wypadkach ta liczba może być znacznie większa.
- Standard komunikacji RS232 pozwala tylko na łączenie dwóch urządzeń.
- Stosując więc tylko RS-485 można tworzyć duże sieci z dużą liczbą obsługiwanych urządzeń.

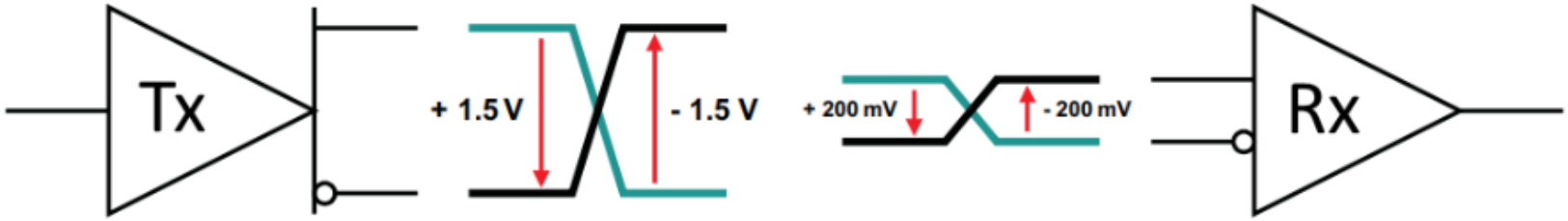
RS-485

- Co istotne, dużą przewagą sieci RS485 jest znacznie większa odporność na zakłócenia względem standardu RS-232.
- Zakłócenia, czy też szumy elektryczne, mogą być źródłem wielu problemów z elektroniką. RS-232 do przesyłania danych jako punkt odniesienia wykorzystuje poziom masy.
- Zakłócenia mają więc w takim przypadku otwartą drogę i mogą dostać się do urządzenia. W RS-485 ta droga jest zamknięta, oraz można dodatkowo ekranować przewód jako dodatkową ochronę.

Poziomy sygnałów standardu RS-485

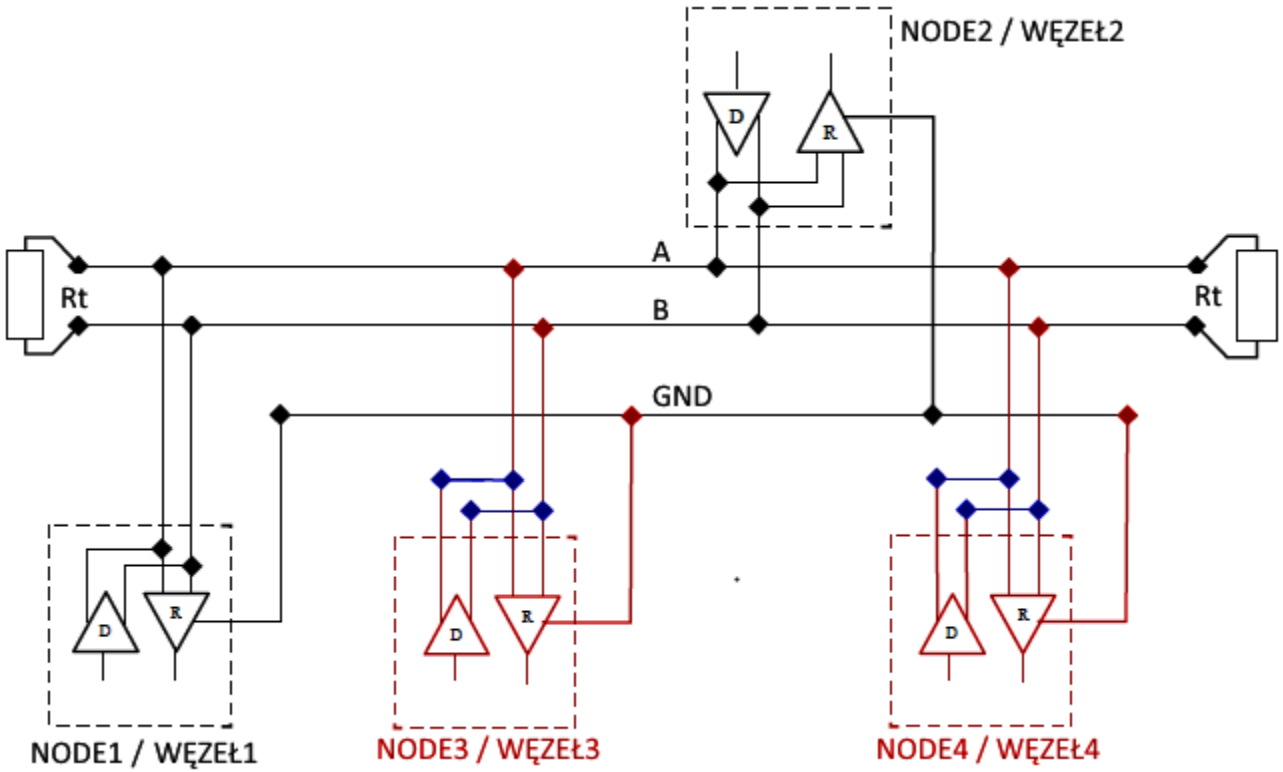
- Urządzenia zgodne ze standardem powinny być w stanie generować, na wyjściach różnicowych, napięcie co najmniej 1,5 V przy obciążeniu 54 Ω.
- Odbiorniki natomiast powinny wykrywać sygnały na wejściu różnicowym rzędu 200 mV.
- Obie wartości zapewniają wystarczający margines dla niezawodnej transmisji danych, nawet przy znacznej degradacji sygnału w przewodzie lub złączach.

Poziomy sygnałów standardu RS-485

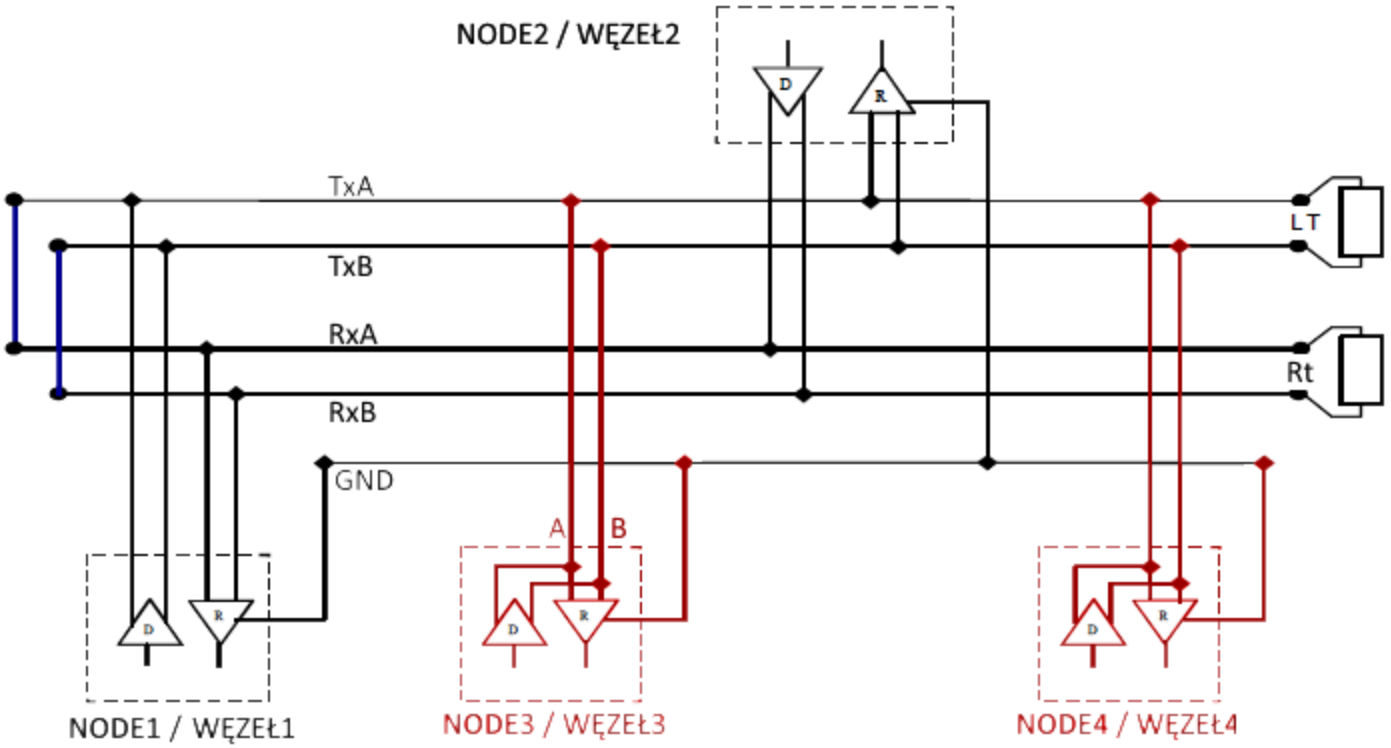


- Właściwości te powodują, że standard RS-485 sprawdza się w zastosowaniach długich sieci, w których mogą występować znaczne straty sygnału oraz zewnętrzne zakłócenia.
- Napięcie występujące pomiędzy sygnałami linii danych A i B interfejsu RS-485 nazywany napięciem wspólnym.
- Dozwolony zakres napięcia sygnału wspólnego **CMVR *(Common mode voltage range)*** wynosi od -7 V do +12 V.

Przykładowe konfiguracje sieci typu RS-485



Przykładowe konfiguracje sieci typu RS-485



Podsumowanie RS-485

- RS-485 nie jest protokołem a standardem definiujący interfejs połączenia elektrycznego.
- Do tworzenia magistrali należy stosować „skrętkę” będącą zbalansowanym kablem połączeniowym.
- Dwie linie A i B MUSZĄ wykorzystywać JEDNĄ skręconą parę w skrętce.
- Komunikacja RS-485 jest odpowiednią dla otoczenia, w którym występują zakłócenia. Odporność na zakłócenia zyskuje dzięki różnicowej transmisji sygnału, zakłócenie indukują się obu parach przewodów i są odejmowane w odbiorniku.
- Topologia magistrali jest liniową topologią punkt-punkt, dzięki czemu może być rozszerzona na wiele punktów.
- Połączenie w “gwiazdę” lub “równoległe” jest nieprawidłowe, gdyż prowadzi do nadmiernie wysokich odbić lub niskiej impedancji.

Podsumowanie RS-485

- Magistrala RS-485 musi mieć tylko dwa końce i muszą być zakończone terminatorami, dzięki czemu unikamy efektu odbić sygnału.
- Magistrala RS-485 można wykonywać jako 2-przewodową lub 4-przewodową. (Moduł TD2 oferuje opcję 2-przewodową).
- Linie danych magistrali powinny być wyrównane do potencjałów +5 V i GND. Ma to na celu uniknięcie efektu „pływającego” potencjału i zapewnia bezpieczną pracę, zmniejszając wrażliwość na zakłócenia.

Protokół Modbus

- Jest to jeden z najstarszych protokołów komunikacyjnych. Zaprojektowany do komunikacji między wieloma urządzeniami poprzez skręconą parę przewodów. Pomimo że Modbus został opracowany i wprowadzony do użytku ponad 40 lat temu, jest wciąż popularny i wykorzystywany w przemyśle.
- Popularność protokołu Modbus wynika następujących powodów:
  - Idea działania jest stosunkowo prosta,
  - łatwy w implementacji,
  - łatwo dostosować go do zmian w projekcie,
  - niedrogi w implementacji,
  - uniwersalny — Modbus posiada bardzo mało ograniczeń w kwestii wymiany danych między urządzeniami.

Protokół Modbus

- Standard Modbus umożliwia obsługę praktycznie wszystkich najpopularniejszych mediów transmisyjnych wykorzystywanych w rozwiązaniach przemysłowych np:
  - Skrętki-TP,
  - Ethernetu,
  - modemów telefonicznych,
  - komunikacji bezprzewodowej,
  - sieci GSM.

Protokół Modbus

W standardzie Modbus RTU dane komunikatu zapisywane są w kodzie binarnym. Każdy bajt danych kodowany jest jednym bajtem komunikatu (bajtem w ramce).
To rozwiązanie doskonale nadaje się do wykorzystania z medium transmisji w kanałach RS-232 i RS-485, z szybkościami transmisji od 1200 do 115 kbit/sek.
Najczęściej stosowane szybkości to 9600 i 19 200 bit/sek.
Modbus RTU jest najczęściej stosowanym obecnie protokół w sieciach automatyki przemysłowej i dlatego też większość informacji zamieszczonych w niniejszym artykule będzie dotyczyć aplikacji i zastosowań tego właśnie rodzaju protokołu.

Protokół Modbus

Modbus TCP to nic innego jak protokół Modbus z transmisją przez sieć Ethernet. Zamiast adresów sieciowych urządzeń automatyki, do komunikacji z modułami Slave wykorzystuje się bezpośrednio adresy IP, a dane komunikatów Modbus tunelowane są w ramkach pakietów TCP/IP. W ten sposób każda sieć bazująca na protokole Ethernet może być wykorzystana jako medium transmisji komunikatów Modbus.

Protokół Modbus

Modbus TCP to nic innego jak protokół Modbus z transmisją przez sieć Ethernet. Zamiast adresów sieciowych urządzeń automatyki, do komunikacji z modułami Slave wykorzystuje się bezpośrednio adresy IP, a dane komunikatów Modbus tunelowane są w ramkach pakietów TCP/IP. W ten sposób każda sieć bazująca na protokole Ethernet może być wykorzystana jako medium transmisji komunikatów Modbus.

Ramka danych protokołu Modbus

Modbus RTU charakteryzuje się 8-bitowym kodowaniem danych. Dane przesyłane są asynchronicznie. Każdy przesyłany bajt wymaga przesłania 11 bitów z bitami startu i stopu. Jeśli nie chcemy kontrolować bitu parzystości, wówczas wykorzystujemy dwa bity stopu.

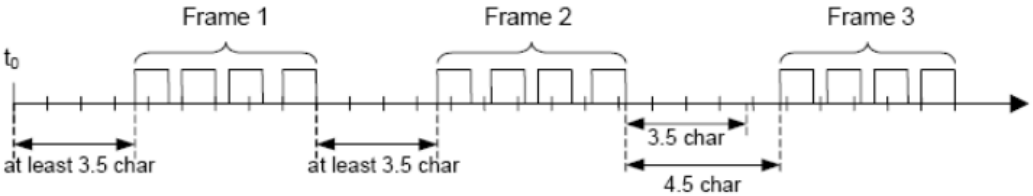
START	BIT 1	BIT 2	BIT 3	BIT 4	BIT 5	BIT 6	BIT 7	BIT 8	**STOP**	STOP

Ośmiobitowy bajt danych bez kontroli parzystości

START	BIT 1	BIT 2	BIT 3	BIT 4	BIT 6	BIT 7	BIT 8	**PARITY**	STOP

Ośmiobitowy bajt danych z kontroli parzystości

Każdą wiadomość rozpoczyna i kończy tzw. cisza na łączu. Jest to czas bezczynności, trwający 3,5 x czas pojedynczego znaku.



Zalecenia sieci RS485

Do realizacji sieci RS-485 zaleca się stosować skrętkę ekranowaną dwużyłową, kabel LiYCY lub dwu parową skrętkę ekranowaną (2×2 skręcone przewody, gdzie druga para jako rezerwa) kabel Li2YCY. Zalecane parametry kabla:

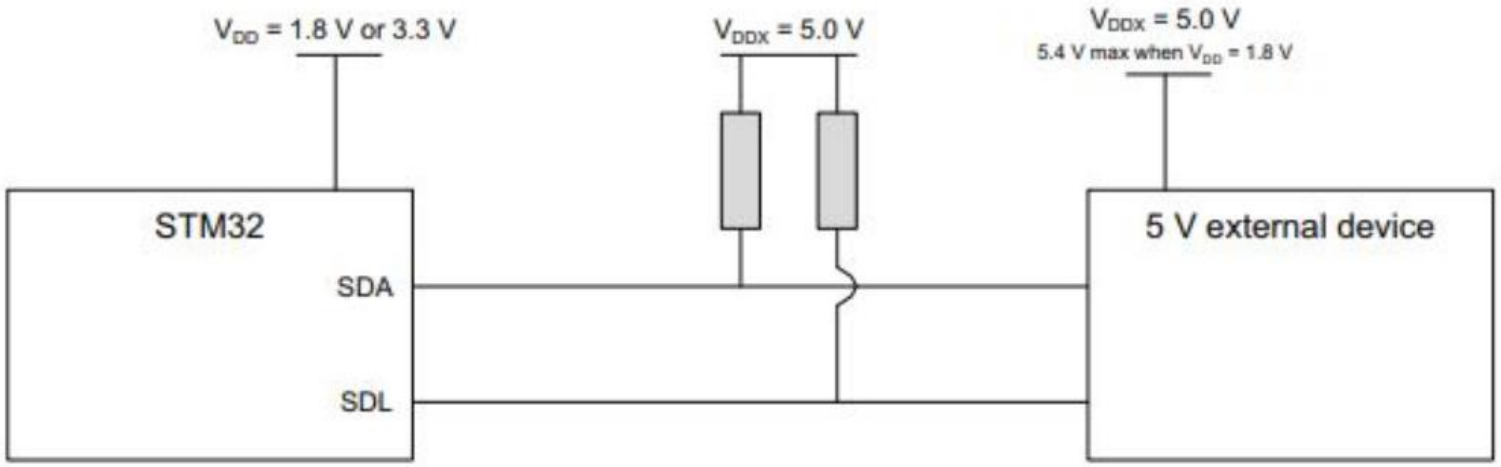
- Impedancja falowa przy f>100 kHz: od 100 do 130 Ohm,
- pojemność: 100 pF/m,
- przekrój: 0,75 mm^2 lub 0,8 mm^2.

Protokół I2C

- Interfejs I2C (Inter-Integrated Circuit) to dwukierunkowa magistrala szeregowa przeznaczona do przesyłania danych.
- Wykorzystuje do komunikacji dwie linie: linię zegarową (SCL) oraz linię danych (SDA). Umożliwia komunikację dwustronną.
- Ze względu na to, że wykorzystuje tylko jedną linię danych, nie jest możliwe przesyłanie informacji w obu kierunkach jednocześnie.
- W komunikacji I2C wyróżnia się dwa typy urządzeń: **master oraz slave.** Te określenia są spotykane najczęściej, chociaż wg najnowszego standardu urządzenia te określane są jako controller oraz target

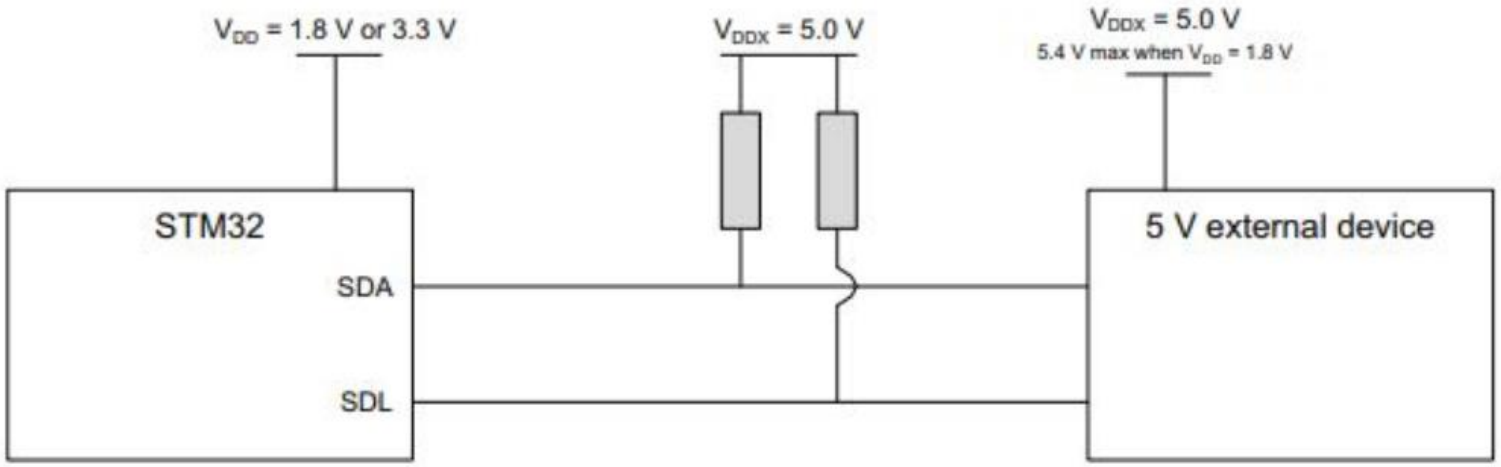
Protokół I2C

- Poziomy napięć w standardach CMOS i TTL dla stanu niskiego i wysokiego pozwalają na komunikację między urządzeniami o 3,3 V oraz 5 V bez potrzeby stosowania dodatkowych konwerterów.



Protokół I2C

- Poziomy napięć w standardach CMOS i TTL dla stanu niskiego i wysokiego pozwalają na komunikację między urządzeniami o 3,3 V oraz 5 V bez potrzeby stosowania dodatkowych konwerterów.

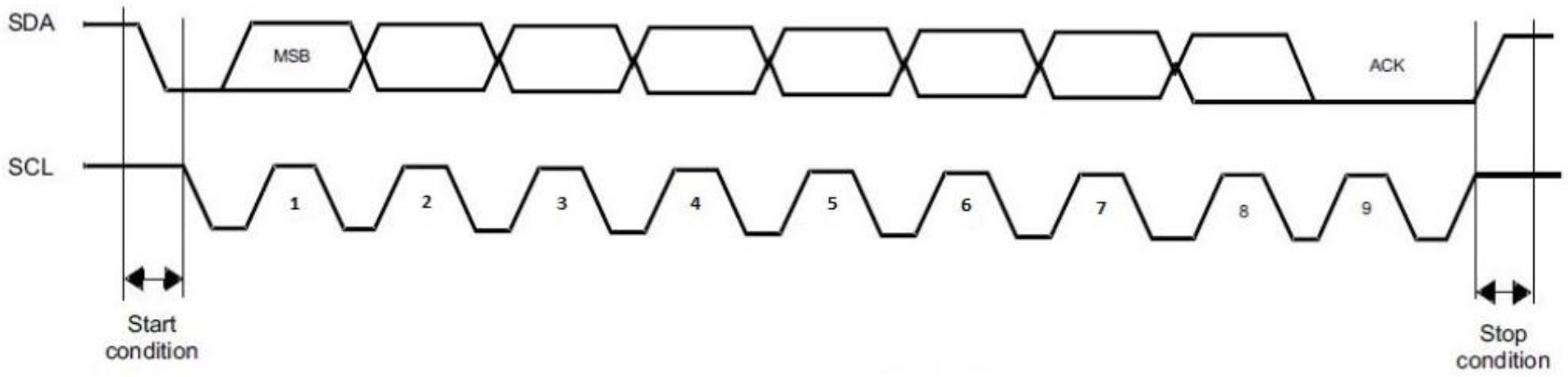


Protokół I2C

- I2C wykorzystuje logikę dodatnią, co oznacza, że stan wysoki to logiczna “1”, a stan niski “0”.
- W trakcie bezczynności na liniach SDA i SCL jest stan wysoki.
- Warto zauważyć, że w trakcie przesyłania danych stan na linii SDA zmienia się tylko w momencie, gdy na linii SCL jest stan niski.
- Jedynie w przypadku sygnałów START i STOP

  zmiana stanu następuje przy stanie wysokim na SCL.
- To pozwala odróżnić rozpoczęcie i zakończenie transmisji od przesyłania danych.

Protokół I2C



- Warto zauważyć, że w trakcie przesyłania danych stan na linii SDA zmienia się tylko w momencie, gdy na linii SCL jest stan niski.
- Jedynie w przypadku sygnałów START i STOP zmiana stanu następuje przy stanie wysokim na SCL.
- To pozwala odróżnić rozpoczęcie i zakończenie transmisji od przesyłania danych.

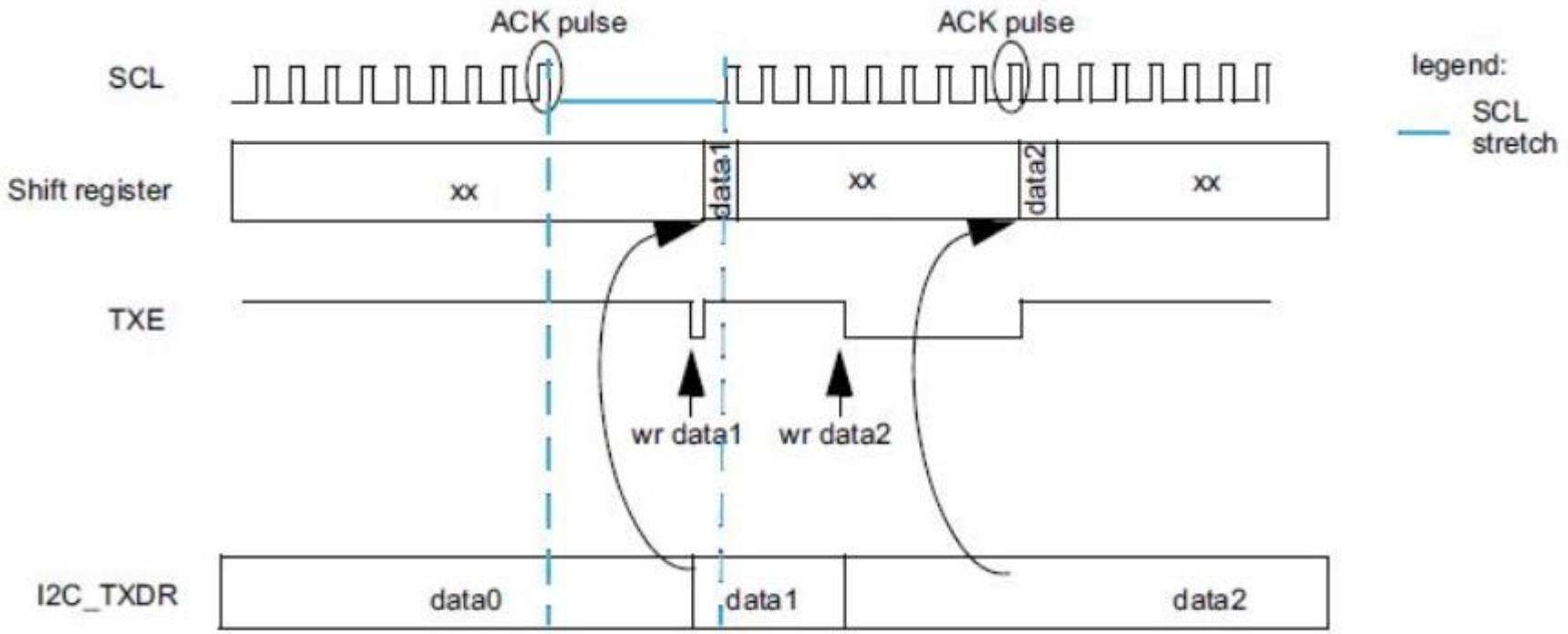
Tryby pracy I2C

- W przypadku magistrali I2C wyróżnia się dwa typy urządzeń: master oraz slave.
- Urządzenie master odpowiada za generowanie sygnału zegarowego i nadzoruje całą komunikację, czyli rozpoczyna i kończy transmisję oraz steruje kierunkiem (zapis, odczyt).
- Urządzenie slave jest podrzędne w procesie komunikacji. Ma nadany własny adres, dzięki czemu można podłączyć do jednej linii wiele urządzeń.
- Slave odpowiada na żądania wysyłane przez mastera.

Wysyłanie i obieranie danych w I2C

- Transfer danych jest zarządzany przez dwa rejestry danych – nadawczy i odbiorczy – oraz rejestr przesuwny.
- Przychodzące bity wpisywane są do rejestru przesuwnego aż do momentu odebrania całego bajtu danych. Wtedy, jeżeli poprzednie dane zostały odczytane i rejestr odbiorczy jest pusty, dane z rejestru przesuwnego kopiowane są do rejestru odbiorczego.
- Jeżeli rejestr RX nie jest pusty, komunikacja zostaje wstrzymana i sygnał SCL nie jest generowany (SCL stretch).
- Pozwala to uniknąć przypadkowej utraty danych.

Wysyłanie i obieranie danych w I2C



Dziękuję za uwagę