Czytnik-programator kart chipowych, część 1

AVT-835

Po raz drugi na łamach EP wracamy do tematu kart chipowych. Pierwsze opracowane przez nas urządzenie cieszyło się dużym zainteresowaniem wśród Czytelników, ale złośliwość losu sprawiła, że wybrane przez nas karty bardzo szybko przestały być produkowane przez firmę Xicor. Z zaistniałych problemów wyciągnęliśmy wnioski, w związku z czym, przynajmniej na razie kart nam nie zabraknie...

Pojęcie „karta chipowa" jest bardzo ogólne. Praktycznie każdy większy producent półprzewodników oferuje jakąś odmianę kart chipowych, które łączy najczęściej jedno podobieństwo - wygląd zewnętrzny. Zazwyczaj podobne funkcje spełniają ich wyprowadzenia oraz protokół transmisji danych do i z karty, lecz dokładne specyfikacje interfejsów nie zawsze się „pokrywają".

Istotne różnice tkwią we wnętrzu kart. W zależności od wymagań aplikacji dostępne są wersje integrujące (przykłady):

- Mikrokontroler (np. pochodny i51, ST9, AVR) odpowiadający za komunikację z otoczeniem z pamięcią programu i dużą pamięcią danych oraz - bardzo często - kryptokontroler, czyli sprzętowy koprocesor umożliwiający szyfrowanie i deszyfrowanie danych. Jednym z największych producentów tego typu kart są: Atmel, Philips oraz STM.

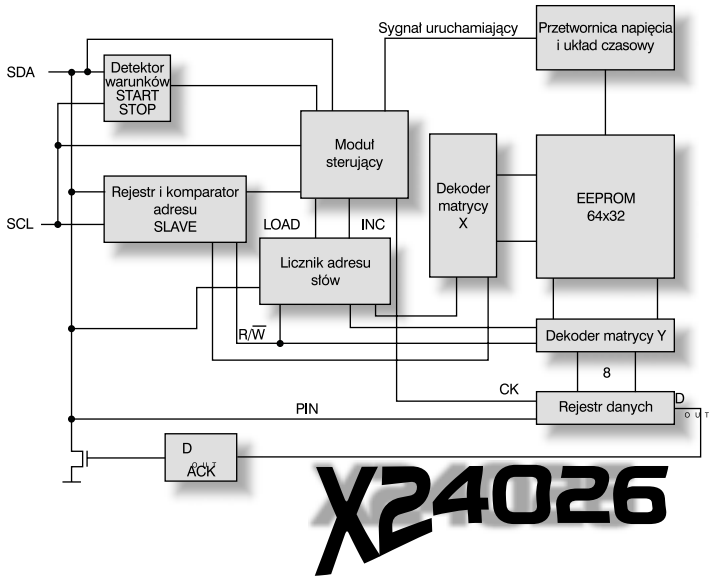
- Nieco prostsze karty z mikrokontrolerami, które procedury szyfrujące mają „zaszyte" we fragmentach pamięci programu. Tego typu karty produkują m.in: Atmel, Philips, STM, Z-Data.

- Karty spełniające bezpiecznych, przenośnych pamięci danych, których integralnym elementem jest moduł weryfikacji hasła i licznik błędnych prób dostępu. Tego typu karty produkują m.in: Atmel, Philips, STM, Xicor, Z-Data.

- Najprostsze karty pamięciowe, których zawartość nie jest zabezpieczona przed dostępem z zewnątrz. Tego typu karty produkują m.in: Atmel, Xicor, Z-Data.

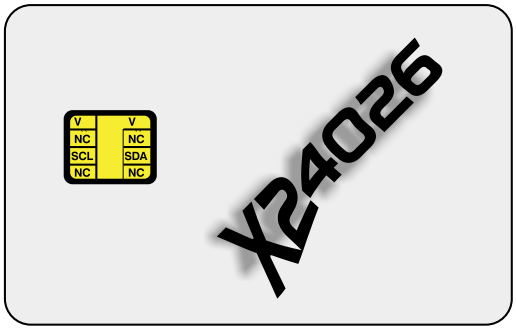
Każda z wymienionych wersji kart jest dostępna z interfejsem synchronicznym (SPI, MicroWire lub I2C) lub asynchronicznym. W zależności od aplikacji matryca pamięciowa może być typu EEPROM (nie zanika po odłączeniu zasilania), EPROM lub RAM. W kartach bankomatowych oraz telefonicznych matryce EEPROM i EPROM są połączone w jeden obszar adresowy. Ponieważ zawartości EPROMu nie można zmodyfikować zapisywane są w nim np. informacje charakteryzujące wydawcę karty, co jest jednym z elementów umożliwiających jej weryfikację. W matrycy EEPROM zapisywane są inne informacje, które muszą zmieniać się w czasie (np. ilość dostępnych impulsów, kod PIN, czy też numer referencyjny użytkownika telefonu).

Czytelnikom zainteresowanym nieco bardziej szczegółowymi informacjami na temat kryptograficznych kart chipowych polecam artykuł, który opublikowaliśmy w EP1/99.

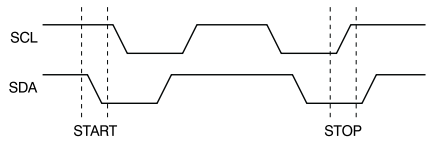


Rys. 1. Schemat wnętrza karty X24026.

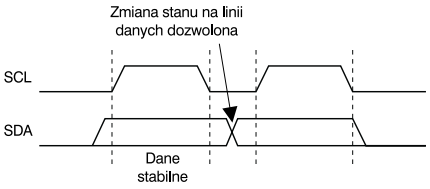
Parametry elektryczne kart X24026:	
Interfejs:	I2C
Maksymalna częstotliwość taktowania:	100kHz
Organizacja:	256 x 8
Napięcie zasilania:	4,5..5,5V
Pobór prądu w stanie aktywnym (odczyt):	1mA
Pobór prądu w stanie aktywnym (zapis):	2mA
Typowy czas trwania zapisu:	5ms
Ilość gwarantowanych cykli zapisu:	100000
Gwarantowany czas przechowywania danych:	100 lat



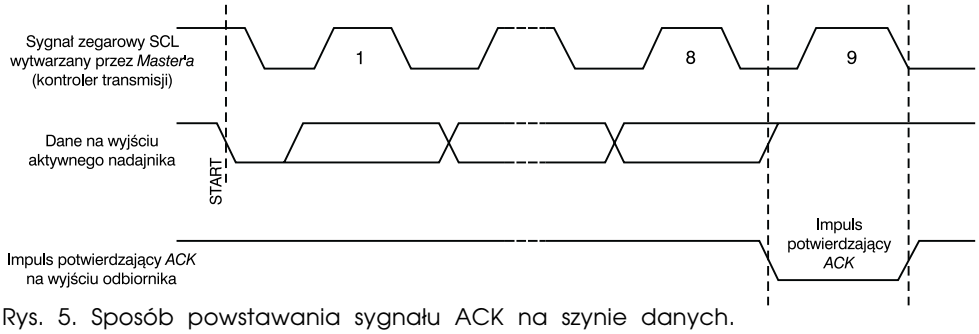
Rys. 2. Obudowa i wyprowadzenia karty X24026Y (skala nie zachowana).



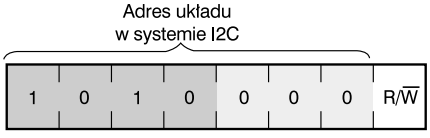
Rys. 3. Warunki Start i Stop.



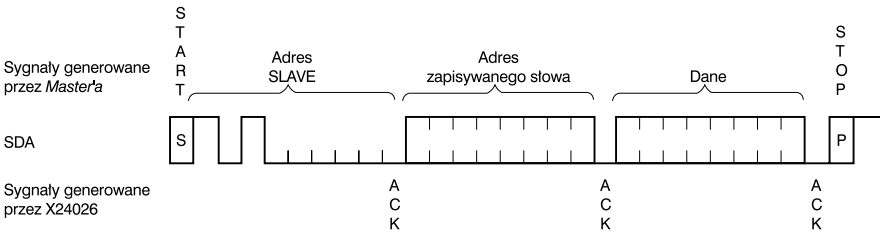
Rys. 4. Sposób taktowania danych.



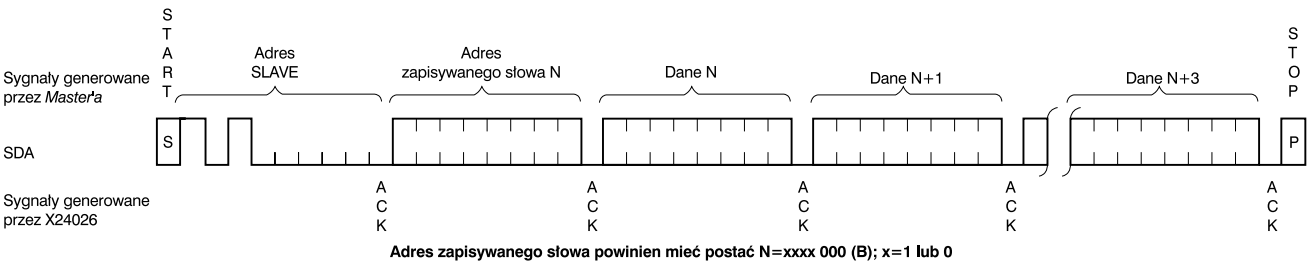
Rys. 5. Sposób powstawania sygnału ACK na szynie danych.



Rys. 6. Bajt adresowy karty i pamięci X24026.



Rys. 7. Sposób adresowania wybranej komórki pamięci EEPROM.



Rys. 8. Sekwencyjny dostęp do pamięci EEPROM.

Nasza karta

Z powodu znacznych trudności z kupieniem kart chipowych z zabezpieczonym dostępem i matrycą EEPROM postanowiliśmy obniżyć nieco poprzeczkę i wykorzystać w projekcie najprostsze karty pamięciowe (EEPROM) z interfejsem I2C. Budowę i sposób programowania wykorzystanej przeze mnie karty X24026 firmy Xicor omówię szczegółowo, co pozwoli wielu naszym Czytelnikom samodzielnie wykonać dla niej programator.

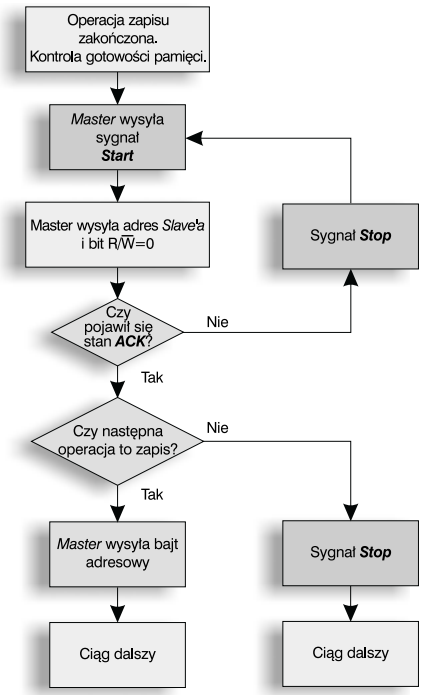
Schemat blokowy karty znajduje się na **rys. 1**. Jest to - jak widać - standardowa pamięć EEPROM z interfejsem I2C, ze zintegrowaną w strukturze przetwornicą napięcia programującego oraz timerem. Jedyną różnicą w stosunku do wersji dostępnych w każdym sklepie elektronicznym jest jej obudowa, która jest po prostu plastikową kartą z wyprowadzonym stykowym złączem (**rys. 2**), zgodnym ze standardem ISO7816.

We wnętrzu karty X24026 znajdują się wszystkie elementy niezbędne do jej poprawnej pracy: kompletny interfejs szeregowy I2C pracujący w trybie *Slave* (z detektorem warunków *Start* i *Stop*, komparatorem adresu *Slave* oraz generatorem potwierdzenia *ACK*), licznik-rejestr adresowy z dekoderami matrycy pamięciowej EEPROM (ma ona organizację 64 słowa x 32 bity), a także dwukierunkowy, przesuwny rejestr danych, który odpowiada za konwersję szeregowo-równoległą i odwrotnie.

Trochę banałów na początek

Zacznę od omówienia zagadnień pozornie oczywistych, czyli sposobu wymiany przez kartę informacji z otoczeniem. Dzięki zastosowaniu interfejsu I2C protokół transmisji danych do i z karty jest, z małymi wyjątkami, identyczny, jak w innych układach I2C. Każda ramka danych rozpoczyna się od znaku *Start*, a kończy się znakiem *Stop* (**rys. 3**). Linia *SCL* spełnia rolę zegara wyznaczającego szybkość pracy transmisji. Na **rys. 4** widoczny jest sposób taktowania danych i obszary (w czasie), w których stan linii danych może się zmieniać. Każda paczka danych (najczęściej bajt) jest kwitowana przez układ odbierający impulsem potwierdzającym *ACK*, który pojawia się na szynie danych *SDA* podczas dziewiątego impulsu zegarowego *SCL* (**rys. 5**). Jest to najprostsza z możliwych forma zwrotnego porozumiewania się odbiornika z nadajnikiem, który w przypadku braku impulsu *ACK* może np. podjąć próbę ponownego przesłania danych do odbiornika.

Nadajnik inicjujący transmisję danych zawsze rozpoczyna od znaku *Start* i następnie wysyła adres odbiornika, dla którego będą przekazywane lub skąd będą odbierane informacje oraz informację określającą rodzaj operacji przewidzianej do wykonania (zapis/odczyt). Na **rys. 6** znajduje się ilustracja prezentująca budowę ramki adresowej. Cztery najstarsze bity (podkreślone ciemniejszym



Rys. 9. Algorytm odpytywania o koniec zapisu matrycy EEPROM.

kolorem szarym) określają adres układu, trzy kolejne (podkreślone kolorem jasnoszarym) są zarezerwowane. W sumie wynikowy adres układu określa wszystkie 7 bitów. Najmłodszy bit ramki przenosi informacje o tym, czy nastąpi zapis do zaadresowanego układu, czy też odczyt z niego.

Dzięki organizacji matrycy pamięciowej w 64 komórki 32-bitowe możliwe są dwa sposoby jej zapisu:

- Standardowy, o dostępie losowym. Nadaje się on idealnie do zapisywania pojedynczych bajtów lub wielu bajtów ulokowanych pod oddalonymi adresami. Taki sposób zapisu wymaga każdorazowego wysłania do pamięci adresu zapisywanej komórki (**rys. 7**).

- Stronicowany, o dostępie sekwencyjnym. Ten tryb pracy pozwala na skrócenie czasu zapisu danych do matrycy pamięciowej, ponieważ zapisywane jest jednocześnie jej 32 bity, które użytkownik wpisuje w postaci czterech bajtów. Na **rys. 8** widoczny jest przebieg obrazujący cały proces wpisu. Jak łatwo zauważyć podczas wpisu stronicowanego tylko raz jest wysyłany adres karty (*Slaveía*), początkowy adres wpisu (N), pomijane są także znaki *Stop* po każdej przesłanej danej. Biorąc dodatkowo pod uwagę, że czas programowania matrycy EEPROM trwa w sumie 5 ms (czyli tyle samo, ile podczas zapisu pojedynczego bajtu), szybkość operacji na pamięci znacznie się zwiększa.

Pewnym problemem podczas zapisywania pamięci jest sprawdzenie, czy jest ona gotowa do dalszej pracy, czyli, czy minął czas niezbędny do poprawnego zaprogramowania matrycy EEPROM. Ponieważ czas trwania wewnętrznego impulsu programującego ulega zmianie w zależności od wartości napięcia zasilającego, temperatury otoczenia i sumarycznej liczby wszystkich wcześniejszych zapisów pamięć wyposażono w generator sygnału aktywności. Na **rys. 9** znajduje się algorytm odpytywania karty o gotowość po dowolnym wpisie. Realizację tego algorytmu można oczywiście pominąć, zastępując go programowym licznikiem czasu, który odmierzy bezpieczny - z punktu widzenia dopuszczalnych wartości parametrów czasowych karty - okres 10..12 ms.

Piotr Zbysiński, AVT
piotr.zbysinski@ep.com.pl