System bezstykowej kontroli dostępu

kit AVT-886

PROJEKT Z OKŁADKI

Mamy nadzieję, że ten projekt i artykuł spodoba się Czytelnikom zainteresowanym systemami kontroli dostępu. Sądzimy, że znajdą coś dla siebie zarówno praktycy chcący samodzielnie uruchomić taki minisystem jak i Czytelnicy, którzy pragną jedynie o nim poczytać. Ponadto, piszący oprogramowanie dla sterowników procesorowych znajdą wskazówki, jak poradzić sobie z sortowaniem dużych baz danych.

Zadaniem systemu kontroli dostępu jest identyfikacja obiektu (osoby lub przedmiotu), a następnie podjęcie określonego działania. Za tak ogólną definicją mogą się kryć bardzo różne sposoby działania i zastosowania systemu. Może on pełnić rolę elektronicznego stróża przy drzwiach (wpuszczam tego kogo znam), dyskretnego nadzorcy rejestrującego poruszanie się osób wewnątrz obiektu (biura, zakładu przemysłowego, chronionego obiektu), elektronicznego sprzedawcy, który może wydawać lub wypożyczać towar obliczając należność, a nawet nieubłaganego kadrowca, który pod koniec przedstawi dokładne zestawienie czasu pracy każdego pracownika, bezlitośnie karząc spóźnialskich.

Żeby móc pełnić każdą z tych ról, układ musi najpierw rozróżniać osoby i ich uprawnienia, a następnie wykonywać określone czynności, np. zwalniać rygiel drzwi i ewentualnie zapamiętywać dane wchodzącego. Chociaż ludzi żyjących na Ziemi jest coraz więcej, układ powinien mieć możliwości bezbłędnej identyfikacji osoby. Najnowocześniejsze systemy analizują w tym celu osobiste i niepowtarzalne cechy, z którymi każdy z nas przychodzi na świat. Może to być rysunek linii papilarnych naszego palca, wzór tęczówki oka, a w przyszłości może fragment sekwencji kodu genetycznego. Mniej skomplikowane systemy żądają od kontrolowanej osoby przedstawienia specjalnego identyfikatora, w którym ukryte jest hasło dostępu, najczęściej niepowtarzalny wielocyfrowy numer. Ze względu na wygodę, obecnie tę rolę pełnią plastykowe karty identyfikacyjne znane np. posiadaczom kont bankowych. W kartach tych oprócz dodatkowych informacji zapisany jest tzw. PIN-kod, którego jednoczesne odczytanie z karty i wpisanie przez użytkownika umożliwia np. dostęp do swojego konta i korzystanie z usług bankomatu. Podobnego rodzaju karty i sposób ich stosowania spotykany jest przy różnego typu zamkach szyfrowych. Jednak jeżeli układ kontroli dostępu miałby być zastosowany w miejscach, gdzie przepływ ludzi jest bardzo duży, to taki system nie jest najlepszy. Można sobie wyobrazić tłum kibiców piłkarskich przed wejściem na stadion, gdy każdy z wchodzą-

cych musi przeciągnąć kartę przez szczelinę czytnika, a potem jeszcze wystukać na klawiaturze PIN-kod, który właśnie zapomniał. Awantury i bitwy ze służbami porządkowymi są pewne. W takim przypadku lepiej skorzystać z kart transponderowych przekazujących kod za pomocą pola elektromagnetycznego. Takie karty wymagają jedynie zbliżenia karty w okolicę czytnika bez konieczności potwierdzania kodu. Identyfikacja wchodzących jest równie skuteczna, a przepływ ludzi dużo większy.

Karta transponderowa

W sposób schematyczny budowę karty transponderowej pokazano na **rys. 1**. Głównymi elementami karty są: miniaturowy układ elektroniczny i dołączona do niego pętla anteny. Do działania karty niezbędne jest zewnętrzne zmienne pole elektromagnetyczne. Pole wzbudza w antenie zmienny prąd, który po wyprostowaniu i odfiltrowaniu zasila układ karty. Z kolei układ poprzez modulację pola, z którego pobiera energię, może przesłać do czytnika zakodowaną informację, np. swój numer. Jak z tego widać, cały proces wymiany danych zachodzi pomiędzy antenami czytnika i karty za pomocą pola elektromagnetycznego wytwarzanego przez czytnik. Zazwyczaj częstotliwość generowanego pola wynosi 125kHz, chociaż są systemy, w których ta częstotliwość wynosi kilkanaście megaherców.

Systemy „wewnętrznej elektroniki" karty wytwarzane są masowo przez kilku wielkich wytwórców. Chipy układów elektronicznych są po przetestowaniu łączone z uzwojeniem anteny, a następnie całość zalewana jest elastycznym żelem. Tak przygotowane układy wysyłane są do końcowego producenta, który opakowuje układy w plastikowe wafle. Na tych plastikowych ochronnych płytkach mogą być nadrukowane dane identyfikacyjne odbiorcy, a nawet nazwisko i fotografia końcowego użytkownika karty.

Sposób budowy karty czyni ją znacznie odporniejszą na zniszczenie niż karty z paskiem magnetycznym. Najczęściej, nawet po przypadkowym zagięciu karta może być jeszcze odczytana.

Ze względu na sposób działania, czytnik może prawidłowo zidentyfikować kartę z odległości kilku, kilkunastu centymetrów. Dystans ten zwiększa się do metra lub więcej w przypadku kart, które do swojego zasilania wykorzystują wewnętrzne miniaturowe baterie. Zazwyczaj ze względu na oszczędny sposób korzystania z energii, karty takie mogą pracować przez kilka lat, jednak po wyczerpaniu się baterii nie można już ich dalej wykorzystywać.

Karta i czytnik z rodziny UNIQUE

W projekcie naszego minisystemu kontroli dostępu jako element identyfikujący użyte zostały karty transponderowe z rodziny UNIQUE. Są to karty tylko do odczytu, tzn. że informację, zakodowaną na etapie produkcji w miniaturowej kości każdej z kart, użytkownik może tylko odczytywać. Pod wpływem pola elektromagnetycznego czytnika karta wysyła swój 64-bitowy kod. Składa się on z 9 bitów nagłówka, 40 bitów numeru i 15 bitów kontrolno-korekcyjnych, wykorzystywanych do eliminacji błędów transmisji. Jak gwarantuje producent, 40-bitowy numer jest unikatowy, co znaczy, że nie mogą pojawić się dwie karty o takim samym numerze. Dzięki takiemu założeniu posiadacz karty może być bezbłędnie zidentyfikowany, a potencjalna pojemność bazy numerów gwarantuje, że nawet gdyby obdarowano kartami wszystkich mieszkańców planety, i tak wiele numerów pozostałoby jeszcze nie wykorzystanych.

W zaprojektowanym systemie do odczytu kart wykorzystano zintegrowany czytnik, w którym na jednej, zabezpieczonej przed wpływami atmosferycznymi płytce znajduje się elektronika oraz wytrawione zwoje anteny nadawczo-odbiorczej. (Dostępne są także czytniki bez anteny, którą jako zewnętrzny, samodzielnie wykonany element dołącza się do czytnika.)

Na **rys. 2** pokazano schematycznie wygląd czytnika i rozkład jego wyprowadzeń. Do dwóch z 6 wyprowadzeń podłącza się zasilanie czytnika (+5V), a na pozostałych po odczycie karty pojawia się jej 40-bitowy kod w kilku różnych formatach. Funkcje poszczególnych wyprowadzeń czytnika są następujące:

1. GND.
2. Kod karty odczytywany w formacie *1-Wire* DS1990 firmy Dallas.
3. Kod karty w formacie transmisji RS232 o parametrach:
   - prędkość 2400bd,
   - 8 bitów danych,
   - 1 bit stopu,
   - bez kontroli parzystości.
4. Kod karty w formacie 40 impulsów o różnym czasie trwania. Bitowi 0 odpowiada ujemny impuls o długości 120µs a bitowi 1 impuls 30µs.
5. Pojedynczy ujemny impuls o czasie trwania 120µs poprzedzający początek nowej transmisji 40-bitowego kodu.
6. Zasilanie +5V (średni pobór prądu 35mA).

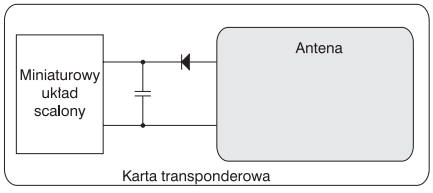
Założenia techniczne i schemat układu

Do stworzenia chociażby najprostszego systemu kontroli dostępu sam czytnik jednak nie wystarcza. Potrzebny jest jeszcze układ sterownika, który będzie decydował, co należy zrobić po odczycie numeru karty oraz sterował układami wykonawczymi. Przy opracowaniu konstrukcji takiego sterownika przyjęto następujące założenia:

1. Sterownik będzie współpracować z zewnętrznym programem, za pomocą którego będzie można ustalać parametry pracy układu kontroli dostępu. Jednocześnie konstrukcja sterownika powinna umożliwić samodzielną pracę układu.

2. Sterownik powinien posiadać blok pamięci nieulotnej, w której byłaby przechowywana baza danych o kartach, ich uprawnieniach, a także gromadzone by były informacje o odczytanych w czasie pracy czytnika kartach.

3. Sterownik współpracujący z czytnikiem kart powinien po każdym odczycie porównywać da-



Rys. 1. Budowa karty transponderowej.

ne karty z informacjami zapisanymi w swojej bazie, a następnie sterować urządzeniem wykonawczym, np. ryglem zamka. Informacja o odczytanej karcie powinna być zapamiętywana do późniejszego wykorzystania przez użytkownika systemu kontroli dostępu.

Na **rys. 3** pokazano schemat sterownika układu kontroli dostępu, spełniający przyjęte wcześniej założenia. Centralną częścią sterownika jest procesor U2, który za pośrednictwem układu U8 i gniazda Zl1 może wymieniać dane z zewnętrznym programem zainstalowanym na komputerze PC. Wszystkie dane gromadzone w czasie pracy systemu przechowywane są w pamięci RAM U3. Nawet jeżeli układ nie jest zasilany, zawartość pamięci podtrzymywana jest dzięki baterii BT1. Układ U11 pełni rolę inteligentnego przełącznika zasilania. Nieprzerwanie monitoruje napięcie +5V zasilające sterownik. W momencie zaniku zasilania, gdy jego wartość spadnie poniżej 4,62V, układ błyskawicznie przełącza zasilanie pamięci na podtrzymanie bateryjne, jednocześnie podając na wejście CS pamięci U3 poziom wysoki. Dzięki temu zablokowana jest możliwość przypadkowego zapisu błędnych danych, co mogłoby się zdarzyć w czasie zaniku napięcia zasilania, gdy działanie procesora może już być zakłócone. Gdy napięcie zasilania ponownie przekroczy poziom 4,62V, bateria zostaje odłączona, napięcie +5V podane na układ pamięci, a możliwość zapisu do pamięci ponownie jest przywracana. Do prawidłowej pracy układu niezbędne jest, aby napięcie baterii podtrzymującej mieściło się w przedziale od +2,5V do +4V.

Z czytnikiem, który przekazuje dane odczytanych kart transponderowych, procesor komunikuje się za pośrednictwem złącza JP1. O odczycie nowej karty procesor jest informowany przez pojawienie się pojedynczego impulsu na złączu JP1-5, poprzedzającego początek każdej transmisji. Następnie ujemne zbocza impulsów strobujących (JP1-4) wyznaczają moment odczytu przesyłanych szeregowo bitów danych linią JP1-3.

Procesor może sterować zewnętrznymi układami wykonawczymi, np. ryglem drzwi lub sygnalizacją, za pośrednictwem gniazda JP2. Kiedy odczytana karta posiada odpowiednie uprawnienia, procesor poprzez tranzystor T1 wymusza na wyjściu JP2-1 poziom niski o czasie trwania 0,5s. Oczywiście, sterowanie ryglem zamka, który do swojej pracy potrzebuje dużego prądu, nie jest możliwe przy użyciu jedynie tranzystora T1. Potrzebny jest więc układ pośredniczący np. przekaźnik lub układ Darlingtona (np. ULN2002). Jeżeli odczytana karta nie ma uprawnień do wejścia, na JP2-2 przez ok. 3s występuje poziom niski, który w podobny sposób jak opisany przed chwilą impuls zezwolenia można wykorzystać do sterowania ostrzegawczym sygnałem świetlnym lub dźwiękowym.

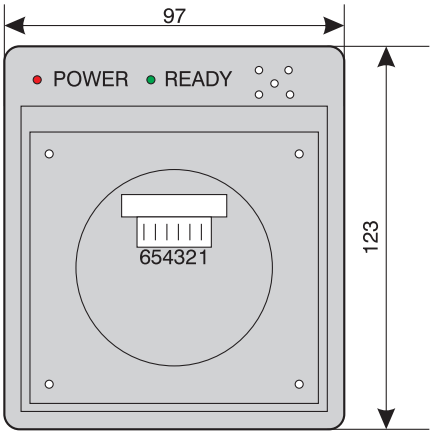
Na płytce sterownika zamontowany jest także układ U9, będący zegarem czasu rzeczywistego, z którego można również odczytywać aktualną datę. Zegar, podobnie jak pamięć danych, jest w czasie zaniku napięcia zasilania podtrzymywany bateryjnie.

Z kolei układ U10 chroni procesor przed zakłóceniami wynikającymi z niebezpiecznego obniżenia się napięcia zasilania. Gdy spadnie ono poniżej wartości krytycznej, procesor jest zerowany. Układ, zarówno funkcjonalnie, jak i rozkładem nóżek, odpowiada podobnemu układowi zerującemu DS1812.

Układ kontroli dostępu może być zasilany zarówno napięciem stałym, jak i zmiennym podawanym za pośrednictwem gniazda JP4. Wartość tego napięcia powinna mieścić się w granicach 8..12V. Napięcie może być nawet wyższe, jednak ze względu na pobierany przez układ prąd ok. 100mA konieczny będzie radiator przykręcany do układu stabilizatora U12.

Sortowanie bazy danych

Nadszedł czas, żeby wspomnieć o oprogramowaniu procesora zarządzającego pracą systemu. Wbrew pozorom jego obowiązki są spore, musi bowiem współpracować z czytnikiem kart, obsługiwać port szeregowy RS232, przeszukiwać bazę danych i sterować urządzeniami wykonawczymi. A wszystko jednocześnie, bez widocznego dla użytkownika spowolnienia szybkości działania.



Rys. 2. Wygląd czytnika i rozkład jego wyprowadzeń.

Praktyka pokazuje, że największe kłopoty sprawia przeszukiwanie bazy numerów zarejestrowanych w systemie kart. Im baza jest większa, tym napotykane kłopoty są większe.

Podstawowym problemem jest czas potrzebny na porównanie numeru odczytanej karty z numerami w bazie, aby stwierdzić, czy jej właściciel posiada prawo do otwarcia drzwi. Dla ilustracji najlepiej posłużyć się przykładem. Opisywany system kontroli ma możliwość zapamiętania do 256 kart w swojej bazie. Przeciętny czas trwania porównania odczytanego przez czytnik 5-bajtowego numeru karty z numerem na kolejnej pozycji w bazie trwa ok. 2 tysięcy cykli, co przy zastosowanym kwarcu procesora daje w przybliżeniu czas 2ms. Jeżeli cała baza zostanie zapisana, a numer odczytanej karty będzie zarejestrowany na ostatniej pozycji, to przy przeszukiwaniu bazy metodą kolejnych porównań należy cały cykl powtórzyć 256 razy, co daje w sumie czas trwania całej operacji równy ok. 0,5s. Nie jest to wiele, a w dodatku można by spróbować zoptymalizować całą procedurę i jeszcze trochę ten czas skrócić. Co jednak zrobić, gdy kart w bazie jest 1000 lub 20000 (a po pewnych zmianach konstrukcyjnych czytnik jest w stanie taką bazę kart obsługiwać)? Założenie, że wchodzący na reakcję urządzenia będzie czekał 4 lub więcej sekund jest nie do przyjęcia. Można co prawda zwiększyć szybkość taktowania

procesora, ale w pewnym momencie i taka możliwość nie wystarczy, tym bardziej, że mamy do czynienia z małymi procesorami jednoukładowymi, a nie potężnymi procesorami do komputerów klasy PC. Jedynym wyjściem jest zastosowanie specjalnej procedury sortującej, która znacząco skróci czas wyszukiwania i porównywania numerów kart. W czytniku zastosowana została metoda wyszukiwania z podziałem przez pół.

Metoda ta jest znana od dawna i stosowana także w komputerach PC do przeszukiwania baz danych. Na początku wymaga tylko przyjęcia jednego założenia: numery kart przechowywane w bazie będą w sposób uporządkowany tzn. od najmniejszego do największego albo odwrotnie, przy czym numery następujących po sobie w bazie kart nie muszą być numerami kolejnymi. Ważne, aby numer karty w bazie był np. „starszy" od numeru go poprzedzającego, a „młodszy" od numeru następnego. Gdybyśmy przykładowo przyjęli bazę o pojemności 200 numerów 1-bajtowych, to mogłaby ona wyglądać następująco: 3, 4, 10, 16, 17, 44 itd. Przystępując do sprawdzenia, czy np. numer 17 występuje w bazie należy jedynie wiedzieć, ile numerów jest już w bazie zapisanych. Kolejne kroki wyszukiwania numeru będą wyglądały następująco:

1. Zmiennej ***lim_l*** należy przypisać „najmłodszy" adres w bazie, czyli 0, a zmiennej ***lim_h*** „najstarszy" wykorzystany adres w bazie.

2. Należy obliczyć adres elementu, który będzie pobrany z bazy do porównań ***compare***. Adres ten zostanie wyznaczony ze wzoru ***compare = (lim_h - lim_l)/2***. Oczywiście, gdy wystąpi część ułamkowa wynik należy zaokrąglić w górę lub w dół tak, aby otrzymać liczbę całkowitą.

3. Z bazy należy pobrać numer spod adresu ***compare***. Następnie numer ten należy porównać z numerem szukanym.

4. Gdy numery są identyczne kończymy procedurę w tym miejscu.

5. Jeśli numer pobrany z bazy jest większy od numeru szukanego, należy wykonać następujące operacje:

a. Przypisać zmiennej ***lim_h*** wartość ***compare***, czyli ***lim_h = compare***.
b. Obliczyć nowy adres ***compare*** korzystając ze wzoru ***compare = lim_l + (lim_h - lim_l)/2***.
c. Skoczyć do punktu 3 kontynuując porównania.

6. Jeśli numer pobrany z bazy jest mniejszy od numeru szukanego, należy wykonać następujące operacje:

a. Przypisać zmiennej ***lim_l*** wartość ***compare***, czyli ***lim_l = compare***.
b. Obliczyć nowy adres ***compare*** korzystając ze wzoru ***compare = lim_l + (lim_h - lim_l)/2***.
c. Skoczyć do punktu 3 kontynuując porównania.

Wykorzystując taki algorytm, z zawężaniem przeszukiwanego obszaru w każdym kroku o połowę, w całkowicie zapełnionej bazie 200-elementowej szukany numer zidentyfikujemy po maksymalnie 8 krokach. Dla bazy o pojemności 2000 elementów potrzeba maksymalnie 11 kroków, a więc oszczędności czasowe są znaczne.

Algorytm ten można przełożyć na fragment programu procesora. Najwygodniej będzie to zrobić posługując się zapisem w języku C.

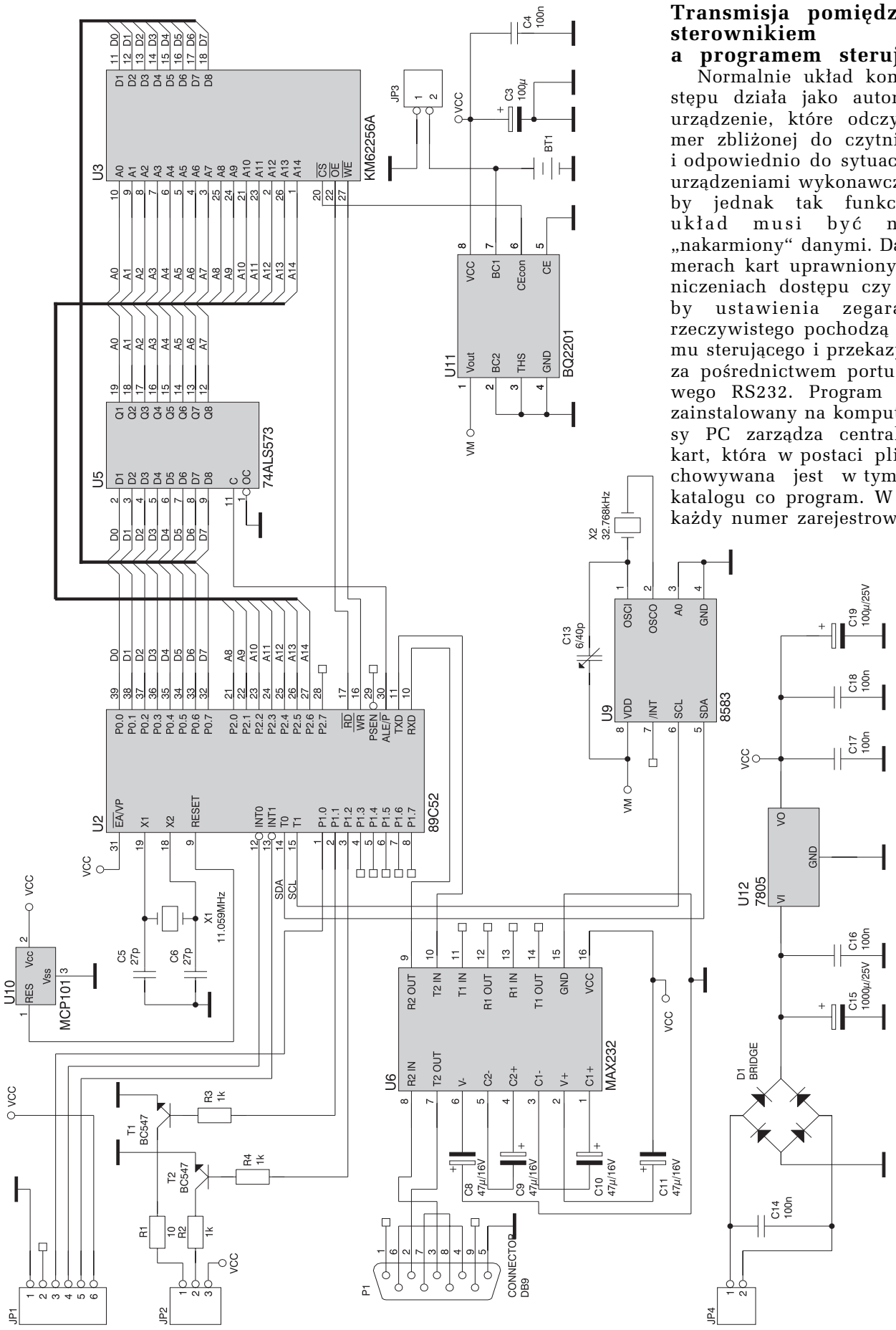
```
//zmienne globalne
unsigned char baza[200];
unsigned char  najstarszy_adres_bazy;
unsigned char szukany_adres;
//Procedura odszukania w bazie pozycji
//adresu szukany_adres
//parametr wyjściowy: odszukana pozycja
//w bazie lub 0xFF gdy element nie występuje /
/w bazie
unsigned char ProceduraSzukania(void)
{
unsigned char compare, lim_l, lim_h;
    lim_l = 0;
    lim_h = najstarszy_adres_bazy;
    wynik = ProceduraPorownania(lim_l);
    if (wynik == 0) return lim_l;
//szukany numer wpisany jest na 0 pozycji bazy
    if (wynik == 1) return 0xFF;
// w bazie nie ma szukanego elementu
    wynik = ProceduraPorownania(lim_h);
    if (wynik == 0) return lim_h;
//szukany numer wpisany jest na ostatniej
//pozycji bazy
    if (wynik == -1) return 0xFF;
//w bazie nie ma szukanego elementu
    compare = (lim_h - lim_l)/2;
    while (compare != 0)
    {
       wynik = ProceduraPorownania(compare);
       if (wynik == 0) return compare;
       if (wynik > 0)
       {
          lim_h = compare;
          compare = lim_l + (lim_h - lim_l)/2;
       }
       if (wynik < 0)
       {
          lim_l =compare;
          compare = lim_l + (lim_h - lim_l)/2;
       }
    }
}
//Procedura porównania numeru z bazy
//z numerem szukanym
//parametr wejściowy: adres elementu z bazy
//użyty do porównań z numerem szukanym
//parametr wyjściowy:
//  0  - numery są sobie równe
//  -1 - numer w bazie jest mniejszy od numeru
//     szukanego
//  1  - numer w bazie jest większy od numeru
//     szukanego
signed char ProceduraPorownania(unsigned char
compare)
{
    if (baza[compare] == szukany_adres) return 0;
    if (baza[compare] < szukany_adres) return -1;
    if (baza[compare] > szukany_adres return 1;
}
```

Przedstawiony fragment programu wymaga kilku słów komentarza. Cała procedura składa się z dwóch podprogramów: *ProceduraSzukania()* i *ProceduraPorownania()*. Drugi z podprogramów dokonuje porównania wartości zapisanej w bazie z szukaną wartością i zwraca taki parametr, jak to opisano w komentarzu. Procedury porównań użyte na początku podprogramu *ProceduraSzukania()* mają za zadanie ustalenie, czy szukany numer nie jest wpisany na pierwszej lub na ostatniej pozycji bazy. Jeśli zaś wartość szukanego numeru jest mniejsza od wartości numeru zapisanego na pierwszej pozycji bazy lub wartość ta jest większa od wartości numeru zapisanego na ostatniej pozycji bazy, to wiadomo, że szukanego numeru w bazie nie ma.

Oprogramowanie procesora sterującego układem kontroli dostępu, w części związanej z przeszukiwaniem bazy danych kart, jest zbliżone do przedstawionego powyżej. Różnice polegają na dodaniu kilku zabezpieczeń, np. pusta baza nie jest przeszukiwana. I oczywiście numery kart są 5-bajtowe, przechowywane w zewnętrznej pamięci RAM.

Transmisja pomiędzy sterownikiem a programem sterującym

Normalnie układ kontroli dostępu działa jako autonomiczne urządzenie, które odczytuje numer zbliżonej do czytnika karty i odpowiednio do sytuacji steruje urządzeniami wykonawczymi. Żeby jednak tak funkcjonować, układ musi być najpierw „nakarmiony“ danymi. Dane o numerach kart uprawnionych, ograniczeniach dostępu czy chociażby ustawienia zegara czasu rzeczywistego pochodzą z programu sterującego i przekazywane są za pośrednictwem portu szeregowego RS232. Program sterujący zainstalowany na komputerze klasy PC zarządza centralną bazą kart, która w postaci pliku przechowywana jest w tym samym katalogu co program. W bazie tej każdy numer zarejestrowanej kar-



Rys. 3. Schemat elektryczny sterownika układu kontroli dostępu.

ty (mało czytelny dla osoby obsługującej system) powiązany jest z określeniem tekstowym - nazwą (tzw. aliasem), którą może być np. nazwisko użytkownika karty - Jan Kowalski. Ponieważ sterownikowi aliasy nie są do pracy potrzebne, program sterujący przesyła do czytnika jedynie zestaw numerów kart oraz warunki ograniczeń dostępu, np. od godziny 8 do 16 z wyjątkiem niedziel, w okresie od stycznia do lipca. Program sterujący musi także dbać, aby baza danych w czytniku była identyczna z bazą w komputerze i w przypadku niezgodności powiadamiać o tym użytkownika. Do realizacji tych zadań i wymiany danych ze sterownikiem program sterujący wykorzystuje zestaw rozkazów. Rozkazem jest ciąg bajtów wysyłanych do sterownika, zgodny z określonym formatem. Format ten jest następujący:

```
STR, Ile, Adres, Komenda, Suma
```

Gdzie:

STR - to bajt początkowy, którego wartość wynosi zawsze 02H.

Ile - dwa bajty określające liczbę bajtów w sekwencji Komenda.

Adres - adres czytnika, do którego kierowany jest rozkaz. W przypadku urządzenia w tej wersji zawsze będzie miał wartość 01H.

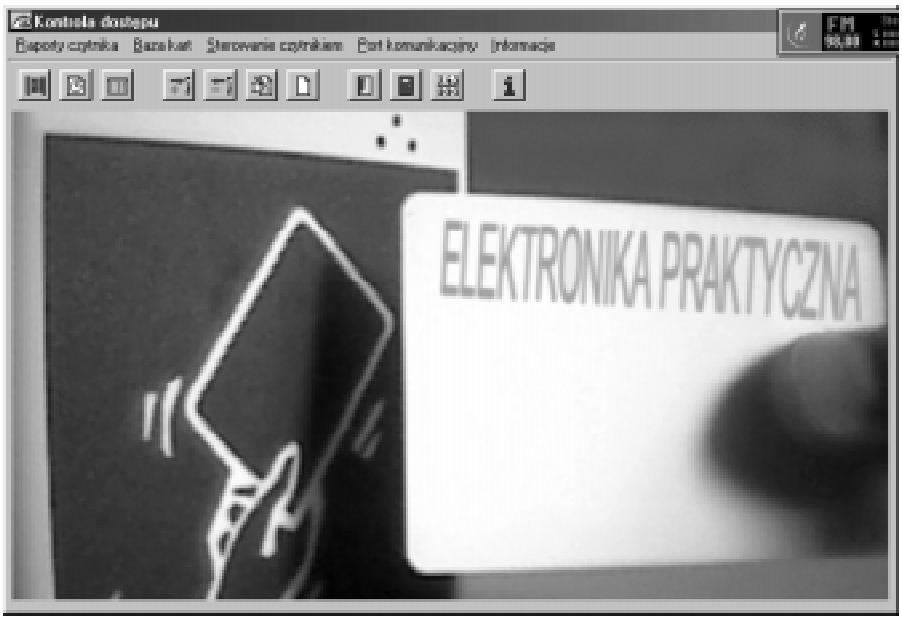
Komenda - w sekwencji komendy wysyłany jest bajt kodu komendy i ewentualnie dodatkowe bajty danych.

Suma - dwa bajty sumy kontrolnej zabezpieczającej przekaz przed przekłamaniami w czasie transmisji. Do obliczenia sumy kontrolnej użyte są bajty Ile, Adres i Komenda traktowane jako liczby 2-bajtowe. Jeżeli użyta do obliczenia sumy kontrolnej liczba bajtów jest nieparzysta, na potrzebę sumowania jako ostatni bajt dodaje się liczbę 00H. Z kolei gdy obliczona wartość sumy przekracza 2 bajty kontrolne, najstarszy bajt sumy jest odrzucany. Dla przykładu, komenda otwierająca czytnik do czytania kart będzie miała postać: 02H, 00H, 01H, 01H, A7H, 01H, A8H.

Lista rozkazów, na które reaguje czytnik jest dość obszerna. Składają się na nią m.in. *rozkazy bezpośrednio sterujące czytnikiem*:
A7H - otwieranie czytnika;
AAH - zamykanie czytnika;
AFH - rozkaz zerowania czytnika.
Komendy przesyłania danych:
A4H - przesyłanie czasu do zegara czytnika;
A5H - odczyt czasu z zegara czytnika;
ADH - dopisanie nowego numeru karty do bazy czytnika;
A2H - rozkaz odczytu kolejnej pozycji logu zdarzeń, czyli daty i czasu odczytu kolejnych kart.
Rozkazy pomocnicze:
B5H - rozkaz odczytu 9 bajtów zawierających dane techniczne odpytywanego czytnika;
B4H - odczyt 2 bajtów sygnatury pozwalających określić, czy baza danych czytnika jest identyczna z zawartością bazy w komputerze.

Wszystkie rozkazy przesyłane są z szybkością 19200 bodów w formacie 8 bitów danych i 1 bitu stopu bez bitu parzystości.

Może się wydawać, że sposób sterowania czytnikiem jest zbyt skomplikowany jak na zadania, które ma spełniać. Trzeba przyznać, że ta wersja systemu powstała poprzez uproszczenie systemu w wersji bardziej skomplikowanej. Ponieważ układ pierwotny sprawdził się w praktyce, wydawało się sensowne uprościć wypróbowane już urządzenie (nawet zachowując nadmiarowość jego funkcji), niż tworzyć od nowa układ z nieznaną liczbą błędów nie wykrytych w fazie testowania.



Rys. 4. Widok okna programu.

Program sterujący

Do obsługi układu kontroli dostępu napisany został program sterujący, który działa na komputerze z okienkami WIN9x. Opisanie poszczególnych funkcji programu najlepiej pokaże możliwości urządzenia. Trzeba zaznaczyć, że prawie dla wszystkich funkcji programu jest wymagane, aby czytnik był włączony i połączony z komputerem

Po uruchomieniu programu użytkownik ma do dyspozycji menu główne składające się z 5 opcji (**rys. 4**). Każda opcja związana jest z inną grupą funkcji układu.

1. Raporty czytnika

Ta część menu związana jest z przeglądaniem i edycją informacji odczytywanych z układu w formie raportów. Raporty przekazują dane o efektach pracy układu. Możliwe są do wyboru dwie podopcje:

a. Odczyt raportów
b. Edycja logu zdarzeń

Odczyt raportów

Po wybraniu tej funkcji wyświetlane jest okienko z kilkoma informacjami, które cyklicznie odczytywane są z układu (jeżeli czytnik nie jest włączony, wyświetlana zostanie informacja o błędzie transmisji). W górnej części okienka można odczytać czas i datę zapisane w zegarze czasu rzeczywistego PCF8583, który jest zamontowany na płytce sterownika. Ustawienia te można

zmienić przez wysłanie do czytnika czasu systemowego komputera. Nastąpi to po naciśnięciu znajdującego się obok symbolu przycisku.

W drugiej sekcji okienka wyświetlany jest stan dwóch liczników czytnika: licznika liczby wejść uprawnionych i licznika wszystkich prób wejść. Różnica wskazań obu liczników polega na tym, że drugi z nich wyświetla także liczbę prób wejść z kartami, które nie miały uprawnień i czytnik zarejestrował odczyt takiej karty jako próbę wejścia bez uprawnień.

Trzecia od góry sekcja zawiera jeden klawisz, którego naciśnięcie spowoduje rozpoczęcie odczytu logu zdarzeń czytnika. Więcej informacji o logu podamy dalej.

Wreszcie ostatnia sekcja zawiera także jeden klawisz, po naciśnięciu którego oba liczniki i zapis logu w czytniku zostaną wyzerowane. Taką operację można przeprowadzić po zakończeniu pewnego okresu działania czytnika: dnia, tygodnia lub miesiąca pracy.

Klawisz „Zamknij" powoduje zamknięcie bieżącego okienka.

Edycja logu zdarzeń

Okienko edycji logu zdarzeń pozwala przeglądać plik logu przesłany uprzednio z układu kontroli dostępu. Log zawiera informacje związane z odczytanymi przez czytnik kartami od czasu ostatniego kasowania liczników i logu. Wyświetlane są informacje o stanie obydwu liczników w momencie odczytu logu oraz dane wszystkich kart, z którymi próbowano wejść. Dane kart zawierają status (karta uprawniona, próba wejścia z kartą bez uprawnień, próba wejścia z kartą, która nie jest zarejestrowana w bazie), alias karty oraz datę i czas jej odczytu. Informacje o kartach można wyświetlać selektywnie według wybranego statusu lub wszystkie jednocześnie w kolejności w jakiej zostały odczytane. Dodatkowo zawartość logu może zostać wydrukowana na drukarce.

Ostatnim elementem menu Raporty czytnika jest „Koniec". Jak łatwo się domyślić, jej wybranie powoduje zakończenie działania programu sterującego.

2. Baza kart

Ta część menu głównego związana jest z tworzeniem, edycją i przesyłaniem bazy kart rozpoznawanych przez układ kontroli dostępu. Do wyboru są następujące opcje:

a. Zarejestuj kartę
b. Wyrejestruj kartę
c. Edycja bazy
d. Kasuj bazę

Zarejestruj kartę

Opcja dodawania do bazy nowej karty spowoduje wyświetlenie okienka, w którym można ustalić wszystkie parametry karty.

Najpierw należy wpisać jej 5-bajtowy numer w kodzie heksadecymalnym. Ponieważ zazwyczaj jest to trudne zadanie, można je uprościć wybierając wariant automatycznego zapisu numeru. Wystarczy wtedy zbliżyć rejestrowaną kartę do czytnika, a jej numer zostanie wyświetlony w odpowiednim miejscu. Pole aliasu należy wypełnić samodzielnie, wpisując nazwisko użytkownika (pseudonim, stanowisko) lub pozostawić je puste. Dalej następuje sekcja ograniczeń podzielonych na 4 kategorie.

Można ustalić ograniczenie liczby wejść użytkownika posługującego się kartą w zakresie od 1 do 254. Działanie ograniczenia jest proste: po wyczerpaniu limitu wejść karta utraci swoje uprawnienia.

Dalej można ograniczyć porę, w jakiej użytkownik karty może wejść na teren obiektu. Na przykład, gdyby system funkcjonował jako system kontroli dostępu do biura, właściciel może sobie zażyczyć, aby wstęp na teren był możliwy jedynie w godzinach np. 7-19, poza tymi godzinami upoważnienia karty byłyby zablokowane.

Kolejnym ograniczeniem jest zezwolenie na dostęp w określone dni tygodnia i działanie tej funkcji jest podobne jak opisanej powyżej.

Ograniczenie daty dostępu także nie wymaga komentarza.

Każdy rodzaj ograniczenia można osobno wyłączyć lub w ogóle nie nakładać na użytkowanie karty żadnych ograniczeń. Ograniczenia są uwzględniane, gdy spełniają warunek sumy logicznej. Jeżeli w danym momencie chociaż jeden rodzaj ograniczenia będzie aktywny, karta nie uzyska uprawnień do wejścia.

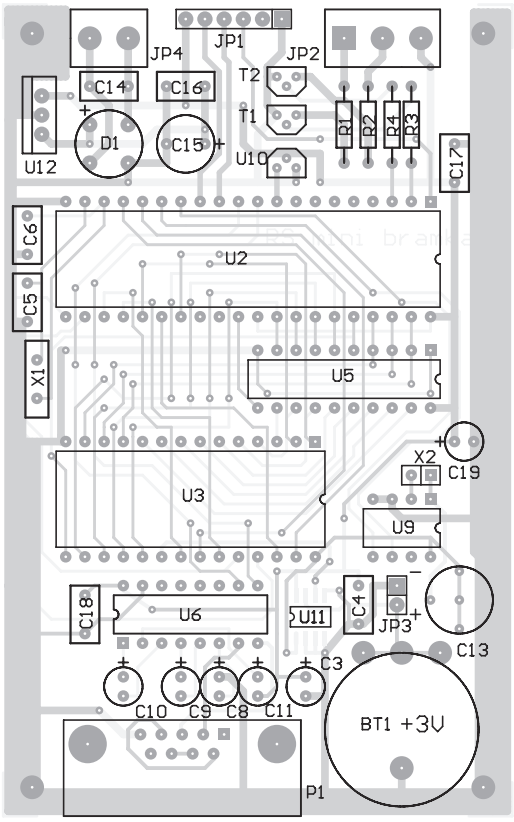
Po zakończeniu dobierania wszystkich ustawień, kartę można dodać do bazy zarejestrowanych kart. Zmodyfikowana baza jest automatycznie przesyłana do podłączonego czytnika.

Wyrejestruj kartę

Opcja pozwala usuwać wybraną kartę z bazy kart. Po wyświetleniu zawartości bazy należy wskazać kliknięciem wybraną kartę, nacisnąć przycisk „Usuń" i potwierdzić swój zamiar.

Edycja bazy

Parametry karty zapisanej w bazie mogą być zmieniane po wybraniu tej opcji menu. Z wyświetlonego zestawienia zarejestrowanych kart należy wybrać dwoma kliknięciami nas interesującą. Wyświetlone zostanie okienko podobne do tego, które jest wyświetlane w czasie rejestracji nowej karty. Wszystkie pola będą wyświetlały parametry edytowanej karty. Parametry - poza numerem karty - można dowolnie zmieniać. Po zakończeniu edycji nowe paramet-



Rys. 5. Rozmieszczenie elementów na płytce drukowanej.

ry karty mogą być zapamiętane w bazie kart i przesłane do czytnika.

Kasuj bazę

Skasowanie dotychczasowej bazy pozwala założyć nową bazę zarejestrowanych kart.

3. Sterowanie czytnikiem

Ta część menu posiada 3 opcje:

a. Otwórz czytnik
b. Zamknij czytnik
c. Zerowanie całego czytnika

Dwie pierwsze opcje zezwalają lub zabraniają czytnikowi na odczyt kart. Normalnie po zerowaniu czytnik jest otwarty. Trzecia opcja umożliwia zerowanie całego czytnika wymazując zawartość liczników wejść, logu i bazy kart (chodzi oczywiście o bazę kart zapisaną w czytniku).

4. Port komunikacyjny

Przedostatnia opcja menu pozwala na wybór portu COM komputera, za pośrednictwem którego będzie się komunikował z czytnikiem.

5. Informacje

Ostatnia opcja pozwala wyświetlić dane techniczne czytnika. Po naciśnięciu przycisku „Odczyt parametrów czytnika" odczytane zostaną z podłączonego czytnika jego podstawowe dane techniczne: numer seryjny i wersja, pojemność bazy kart, pojemność bazy logu, a także zakres obydwu liczników wejść.

Montaż i uruchomienie układu kontroli dostępu

Jeżeli ktoś chciałby zainstalować system kontroli dostępu wykorzystując opisany wcześniej układ i program sterujący, to wykonanie i uruchomienie systemu jest bardzo proste. Na dwustronnej płytce drukowanej (schemat montażowy przedstawiamy na **rys. 5**) należy zamontować jedynie kilka układów scalonych i nieco elementów biernych. Wyjątkowo, ze względu na niewielkie rozmiary, należy jako pierwszy wlutować montowany powierzchniowo układ U11. Jeżeli chodzi o pozostałe układy scalone, gorąco polecam zastosowanie podstawek dla U2, U3 i U9. Następnie należy zamontować pozostałe elementy. Jako złącza JP2 i JP4 proponuję przystosowane do druku kostki zaciskowe do przewodów typu ARK. Złącze RS to 9-pinowe gniazdo szufladowe („żeńskie"), najlepiej do druku. Baterię podtrzymującą najlepiej zamontować na samym końcu, aby przez przypadkowe zwarcie nie doprowadzić do jej nagłego rozładowania. Podczas testów do złącza JP2 można podłączyć diody LED (obie anody do wyprowadzenia JP2-3). Zasilanie (8..12V napięcia stałego lub zmiennego) podłączamy do JP4. Na wszelki wypadek lepiej sprawdzić, czy stabilizator U12 dostarcza prawidłowo napięcie +5V, a dopiero potem zamocować pozostałe układy w podstawkach i wlutować baterię. Układ U11 sprawia, że napięcie podtrzymania na wybranych układach pojawi się dopiero po pierwszym włączeniu i wyłączeniu zasilania całego układu.

Pierwszym sygnałem, że układ działa poprawnie będzie mignięcie i zgaszenie diod LED dołączonych do JP2. Dla normalnej pracy układu należy podłączyć do gniazda JP1 czytnik kart, a do gniazda RS standardowy kabel łączący sterownik z komputerem. Połączenie sterownika z czytnikiem kart można wykonać 6-żyłowym przewodem; wyprowadzenie JP1-1 sterownika powinno łączyć się z wyprowadzeniem 1 czytnika itd.

Po uruchomieniu programu sterującego należy wybrać opcję odczytu raportów. Jeżeli wszystkie połączenia są prawidłowe, na ekranie powinien ukazać się czas zegara sterownika odliczający kolejne sekundy. Po naciśnięciu klawisza synchronizacji czas systemowy komputera zostanie przepisany do zegara czasu rzeczywistego czytnika.

W zależności od wariantu czytnika kart może on mieć postać płytki drukowanej z wytrawioną anteną lub cały czytnik może już być opakowany w plastykową, estetyczną obudowę nadającą się do zamontowania np. przy drzwiach. Montaż czytnika, sterownika oraz ich zasilanie zależą od potrzeb użytkownika i konkretnych warunków. Trzeba jednak pamiętać, że powinien istnieć dostęp do gniazda RS w celu okresowego odczytu logu i ewentualnie modyfikacji bazy kart.

Żywotność baterii podtrzymującej zasilanie jest związana z długością okresów, kiedy układ kontroli pozostaje wyłączony. Układy wykonane w technologii MOS (pamięć i zegar) normalnie nie pobierają wiele prądu, jednak gdy zewnętrzne zasilanie jest wyłączone czerpią prąd wyłącznie z baterii podtrzymującej, co stopniowo ją rozładowuje. Pomiar poziomu napięcia baterii można wykonać korzystając ze złącza JP3 (uwaga na przypadkowe zwarcia!).

Ryszard Szymaniak, AVT
ryszard.szymaniak@ep.com.pl

Wzory płytek drukowanych w formacie PDF są dostępne w Internecie pod adresem: ***http://www.ep.com.pl/pcb.html*** *oraz na płycie CD-EP10/2000B w katalogu* ***PCB****.*

WYKAZ ELEMENTÓW

Rezystory
R1: 10Ω
R2..R4: 1kΩ
Kondensatory
C3: 100µF/16V
C4, C14, C16..C18: 100nF
C5, C6: 27pF
C8..C11: 47µF/16V
C13: 6/40pF trymer
C15: 1000µF/25V
C19: 100µF/25V
Półprzewodniki
M1: mostek prostowniczy
T1, T2: BC547
U2: 89C52 (zaprogramowany)
U3: KM62256A pamięć RAM
U5: 74ALS573
U6: MAX232
U9: PCF8583 zegar czasu rzeczywistego
U10: MCP101 układ resetu procesora
U11: BQ2201 przełącznik zasilania bateryjnego
U12: 7805
Różne
BT1: bateria 3V
JP1: tzw. goldpiny
JP2: kostka zaciskowa do druku typu ARK3
JP4: kostka zaciskowa do druku typu ARK2
ZI1: złącze DB9 żeńskie do druku
X1: 11,059MHz
X2: 32,768kHz