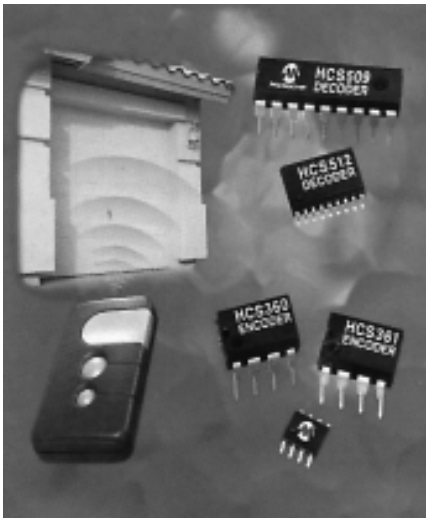
Układy zdalnego sterowania z kodem dynamicznym

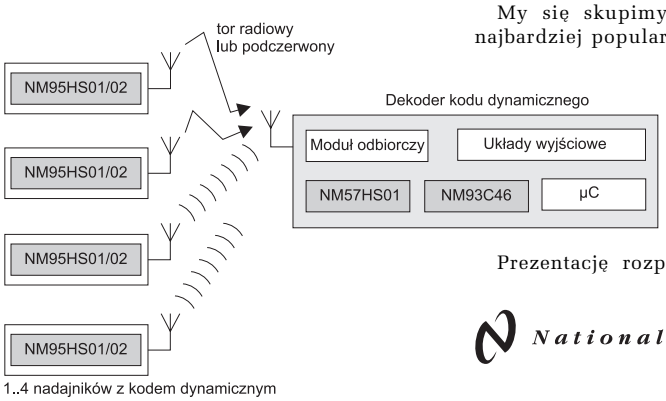
W artykule przedstawiamy trzy najbardziej popularne rodziny układów przeznaczonych do pracy w systemach zdalnego sterowania. Są one stosowane głównie w bezstykowych włącznikach alarmów, zdalnych sterownikach bram i szlabanów automatycznych, sterownikach rygli elektrycznych w sejfach, układach bezstykowej identyfikacji, a także szeregu innych aplikacjach. Prezentowane w artykule układy wyróżniają się niezwykle oryginalnym sposobem szyfrowania przesyłanych poleceń, przez co odporność systemu na próby nieautoryzowanego dostępu jest bardzo wysoka.



Układy zdalnego sterowania wykorzystujące do generowania zmiennego kodu wyjściowego złożone algorytmy implementowane bezpośrednio w strukturę półprzewodnikową produkowane są przez wiele firm na świecie. Przewaga systemów z kodem dynamicznym nad standardowymi rozwiązaniami (np. popularne układy rodziny MC145026..8 lub TEA5500) polega na znacznym ograniczeniu możliwości złamania bariery kodowej poprzez podsłuch radiowy lub proste próby aproksymacyjne.

My się skupimy na omówieniu trzech najbardziej popularnych standardów, opracowanych niezależnie w trzech różnych firmach - National Semiconductor (układy rodziny HiSec), Exel (seria Sure Lok) oraz Microchip (opracowanie firmy KeeLoq).

Prezentację rozpoczniemy od firmy



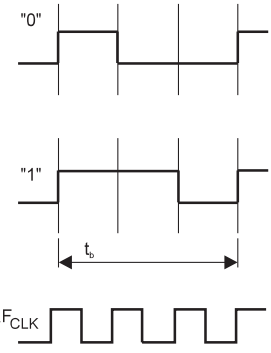
1..4 nadajników z kodem dynamicznym

Rys. 1.

National Semiconductor

Na początku 1994 roku wprowadziła ona do sprzedaży pierwsze układy wchodzące w skład rodziny nazwanej HiSec (z ang. High Security). Charakteryzują się one możliwością pracy w trybach ze zmiennym i stałym kodem, co pozwala dostosować możliwości systemu zdalnego sterowania do wymagań bezpieczeństwa stawianych konkretnej aplikacji.

Na **rys.1** przedstawiono uproszczony schemat blokowy układu zdalnego sterowania zrealizowanego przy pomocy układów rodziny HiSec. Układy NM95HS01 lub 02 spełniają rolę generatorów kodu losowego wysyłanego przez nadajniki. W pierwotnie opracowanych systemach możliwe było stosowanie od 1 do 4 niezależnych nadajników. Układ NM57HS01 jest dekoderem kodu losowego, który współpracuje z pamięcią EEPROM magazynującą fragment kodu wykorzystywanego do identyfikacji upoważnionych kluczy. Jako medium transmisyjne można wykorzystać sygnały radiowe lub podczerwień.

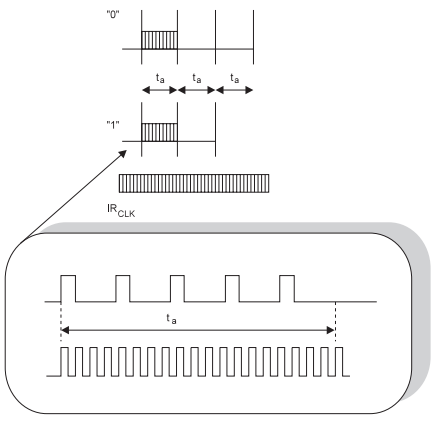


Rys. 2.

Projektanci układów HiSec zastosowali bardzo interesującą metodę synchronizacji nadajnika z odbiornikiem - polega ona bowiem na wyliczaniu przez dekoder w odbiorniku okna dopuszczalnych kodów o szerokości zadanej przez użytkownika. Ponieważ w typowych sytuacjach jest mało prawdopodobne, aby nadajnik wygenerował więcej niż kilkanaście ramek, poza zasięgiem toru transmisyjnego stosuje się typowo okna o szerokości 16, 24 lub 32 ramek. Resynchronizacja nadajnika z odbiornikiem nie jest w żaden sposób widoczna dla użytkownika.

Nieco inaczej wygląda synchronizacja nadajnika i odbiornika w momencie inicjacji systemu lub w przypadku utraty synchronizacji wywołanej „wypadnięciem" generatora losowego nadajnika poza obszar kodów dopuszczalnych przez odbiornik. Niezbędna jest wtedy ingerencja we wnętrze odbiornika - wejście układu NM57HS01, oznaczone RESYNC, należy zewrzeć z masą, co wymusi proces resynchronizacji. W przeciwnym wypadku odbierane ramki danych będą traktowane jako błędne.

Układy odbiorcze HiSec mają wbudowa-



Rys. 3.

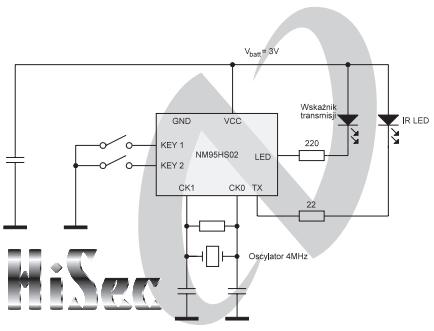
Rys. 4.

ne dodatkowe zabezpieczenie przed systemami skaningowymi, które polega na ograniczeniu liczby możliwych pomyłek i prób nieuprawnionego dostępu. Po przekroczeniu zadanej liczby dopuszczalnych kodów błędnych układ odbiorczy przełącza się w stan ograniczonego dekodowania. Polega ono na dekodowaniu sygnałów przychodzących w odstępach czasu powyżej 30 sek. Dzięki temu złamanie zabezpieczenia wymaga ogromnej ilości czasu, co działa najczęściej zniechęcająco na osoby tym zainteresowane.

Zakodowany sygnał nadawany może być w 11 różnych formatach. Dwa z nich stosowane w typowych aplikacjach - RF PWM w torach radiowych w.cz. (**rys.2**), IR w systemach z nośną z zakresu podczerwieni (**rys.3**).

W zależności od wymagań użytkownika w systemie HiSec możliwe jest przesyłanie dwóch typów ramek danych - krótkiej (57 bitów, w tym 24 kodowane dynamicznie) lub długiej (81 bitów, w tym 36 kodowanych dynamicznie). Formaty tych ramek przedstawiono na **rys.4** i **5**.

Preambuła (pole synchronizujące) może zostać indywidualnie zaprojektowana przez użytkownika, a jej zadaniem jest zapewnienie pełnej synchronizacji nadajnika z odbiornikiem. Identyfikator stały wykorzystywany jest w układach stałokodowych, może być także wykorzystany do identyfikacji konkretnego klucza w systemie z kodem dynamicznym. Pozwala to prowadzić w prosty sposób statystykę pracy systemu



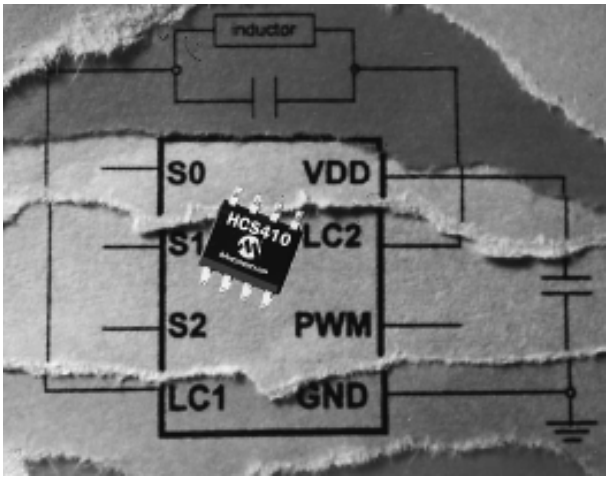
Rys. 7.

strzeżonego przez HiSec. Pole danych o długości 4 bitów informuje odbiornik o numerze wciśniętego w nadajniku klucza, stanie baterii nadajnika oraz o fakcie wysłania ramki synchronizującej zamiast typowej ramki danych. W zależności od formatu ramki pole, poprzez które przesyłana jest modyfikowana część kodu, może mieć długość 24 lub 36 bitów. Wartość tego pola jest modyfikowana po każdym cyklu transmisji danych. W długich ramkach danych obok bitu stopu, którego zadaniem jest jednoznaczne określenie końca przesyłanych danych, przesyłane jest 8-bitowe pole parzystości, które zwiększa bezpieczeństwo przesyłanych danych. Jeżeli odbiornik wykryje błąd parzystości ignoruje całą odebraną ramkę.

Typowym odbiornikiem systemu HiSec

Rys. 5.

jest wspomniany wcześniej układ NM57HS01, który umożliwia odbiór zarówno ramek krótkich, jak i długich i jest przystosowany do pracy z torami radiowymi oraz podczerwonymi. Dzięki bardzo elastycznej konstrukcji układ ten może pra-



cować jako stacjonarna, niezależna centrala odbiorcza lub jako inteligentny odbiornik-dekoder współpracujący z systemem mikroprocesorowym.

Na **rys.6** przedstawiono uproszczony schemat nadajnika systemu HiSec, który wykorzystuje jako medium podczerwień. Jako emiter podczerwieni producent zaleca stosowanie diody TSIP5200 firmy Temic, a optymalnym odbiornikiem jest TFMS1300. Zasięg osiągany z takim zestawem elementów przekracza 5m.

Schemat z **rys.7** przedstawia radiowy nadajnik systemu HiSec, w którym jako wzorzec częstotliwości nośnej wykorzystano filtr z falą powierzchniową.

Na **rys.8** przedstawiono schemat blokowy wnętrza nadajnika systemu HiSec NM95HS01A.

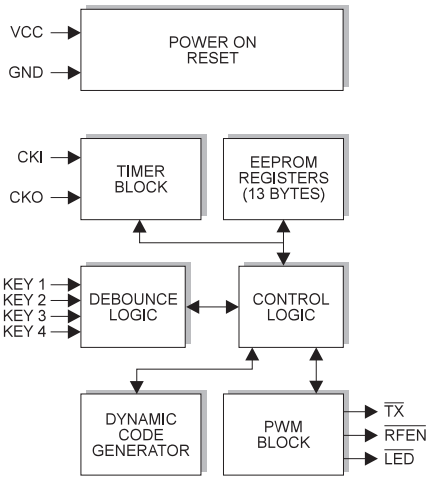
System kodowania dynamicznego KeeLoq opracowany w firmie

MICROCHIP

ma nieco odmienną od HiSeca architekturę - przedstawiono ją na **rys.9**. Układy koderów kodu dynamicznego wchodzące w skład rodziny KeeLoq (HCS2XX, HCS3XX i HCS4XX) generują słowo o długości 66 lub 67 bitów, z czego 28/32 bity stanowią niepowtarzalny numer seryjny, a 32 bity ulegają modyfikacji po każdej transmisji (fragment kodowany dynamicznie). Oprócz tego w nadawanym słowie zawarta jest informacja o numerze przyciśniętego w nadajniku przycisku, napięciu baterii oraz suma kontrolna. Ramka przesyłanego sygnału jest uzupełniana o startowe bity synchronizujące, dzięki czemu transmisja asynchroniczna może przebiegać bez zakłóceń.

Na **rys.10** przedstawiono schemat blokowy jednego z najbardziej popularnych układów kodujących serii KeeLoq - HCS300. We wnętrzu tego układu znajduje się pamięć EEPROM o pojemności 12 słów 16-bitowych. Jest ona wykorzystywana do przechowywania czterech 16-bitowych kluczy kodowych (po jednym dla każdego z przycisków), wykorzystywanych przez generator kodu kroczącego do tworzenia słowa wyjściowego. Słowo to jest modyfikowane po każdej transmisji w sposób nieliniowy, dzięki czemu „podsłuchanie" jednej (czy nawet kilku) transmisji nie pozwala potencjalnemu włamywaczowi określić jaki będzie kolejny kod.

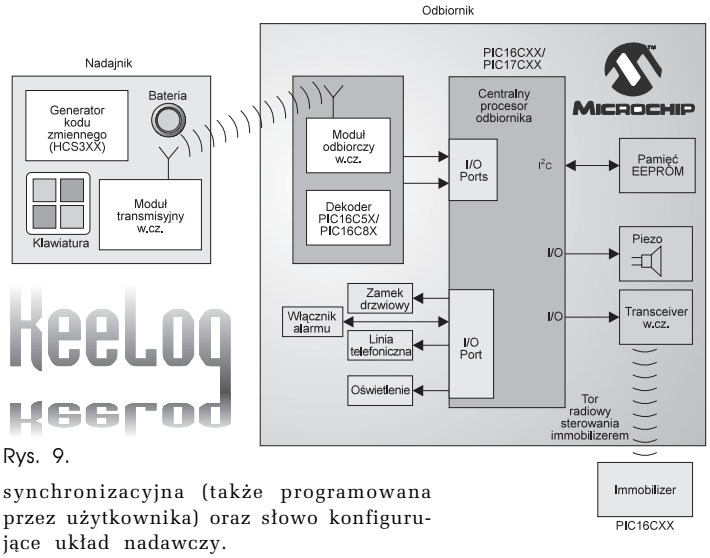
Ogromną zaletą układów KeeLoq jest fakt, że



Rys. 8.

użytkownik może samodzielnie wybrać i zaprogramować słowa - klucze i w dowolnym momencie je zmienić.

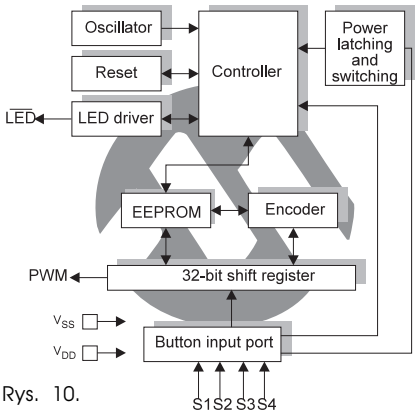
W pamięci EEPROM oprócz słów - kluczy przechowywana jest wzorcowa ramka



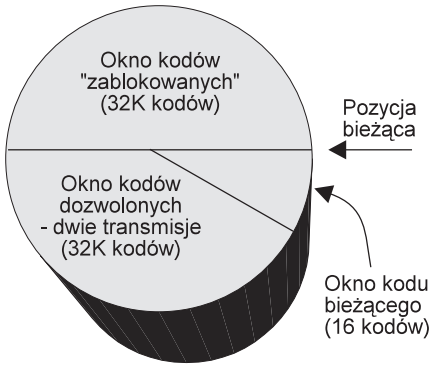
Rys. 9.

synchronizacyjna (także programowana przez użytkownika) oraz słowo konfigurujące układ nadawczy.

Synchronizacja nadajnika z odbiornikiem odbywa się na drodze podobnej jak w układach HiSec, z tą jednak różnicą, że układ odbiorczy nie wylicza po każdej prawidłowo odebranej transmisji okna o zadanej szerokości. Synchronizacja i kontrola odebranego kodu w układzie odbiorczym wygląda następująco - z odebranego ciągu bitów wyliczany jest faktycznie przesłany numer (który został zaszyfrowany według kodu - klucza), po czym następuje kontrola, czy mieści się on w oknie o szerokości 16 słów. Jeżeli tak nie jest, ale odebrany kod jest w oknie „kody dozwolone“ (**rys.11**)



Rys. 10.



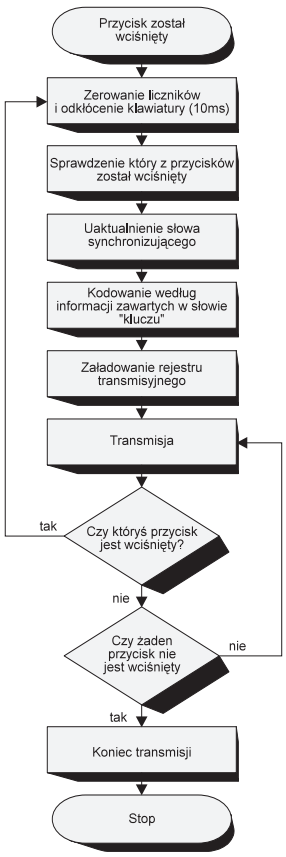
Rys. 11.

rozpoczyna się procedura resynchronizacji odbiornika z nadajnikiem. Polega ona na zapamiętaniu w rejestrze pomocniczym odebranego kodu i porównanie go z kolejnym. Jeżeli liczba przekazana w drugiej transmisji jest taka, jak wynika to z algorytmu szyfrowania, następuje synchronizacja nadajnika z odbiornikiem i wykonywane jest przesłane polecenie. Jeżeli natomiast odebrany kod będzie się znajdował w oknie kodów zablokowanych konieczna będzie resynchronizacja sprzętowa, co wiąże się najczęściej z koniecznością ingerowania we wnętrzu odbiornika.

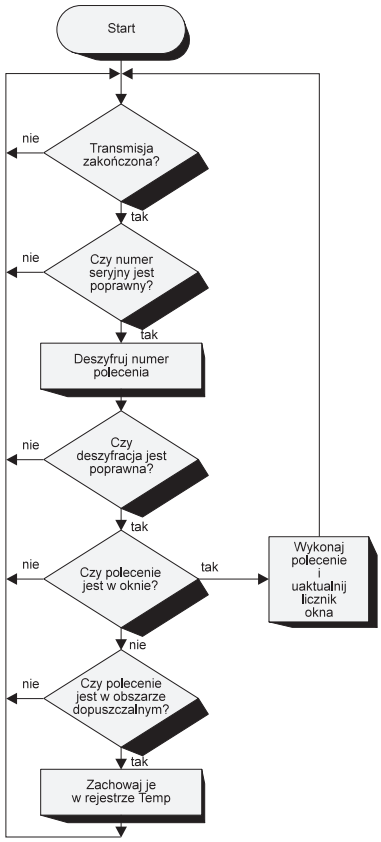
Jak widać proces resynchronizacji zastosowany w układach serii KeeLoq jest bardzo niezawodny i zwalnia użytkownika z konieczności umiejętnego korzystania z gotowego urządzenia.

Na **rys.12** przedstawiono algorytm pracy układów nadawczych serii HCS, a na **rys.13** przedstawiony został algorytm pracy układu odbiorczo - dekodującego. Do niedawna najczęściej układy dekodujące wykonywane były na procesorach PIC, co nie stanowi zbytniej trudności ponieważ program realizujący algorytm dekodowania jest udostępniany przez Microchip firmom produkującym układy zdalnego sterowania.

Przewidywane jest jednak wprowadzenie do masowej produkcji w najbliższym czasie specjalizowanych układów dekodujących dla systemu KeeLoq. Układy te wchodzą w skład serii HCS5XX. Schemat ideowy najprostszego układu odbiorczego wykonanego w oparciu o układ HCS512 przedstawiono na **rys.14**.



Rys. 12.



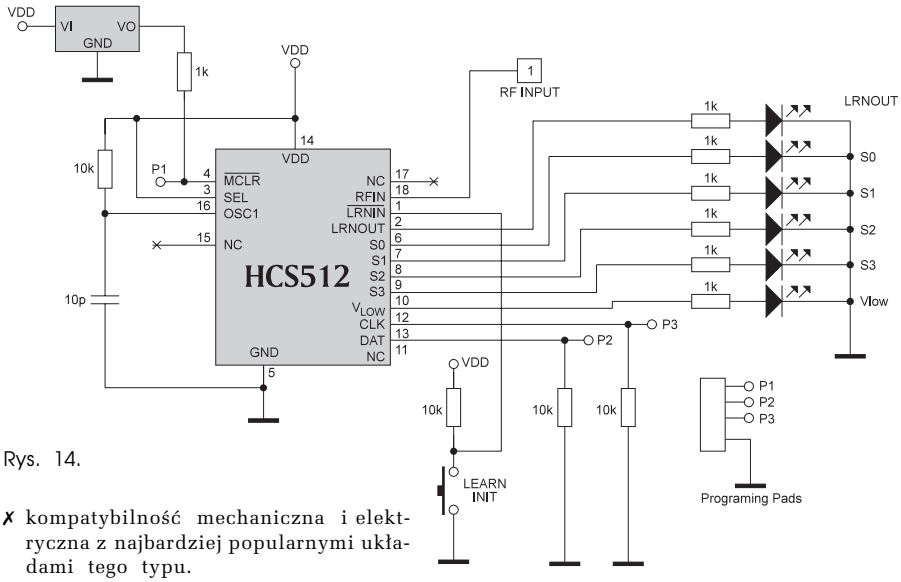
Rys. 13.

Dość interesującą, lecz mało znaną rodziną układów - generatorów kodów dynamicznych są produkowane przez amerykańską firmę

układy SureLok. Pod względem skuteczności algorytmu kodującego układy te są bardzo zbliżone do serii KeeLoq firmy Microchip. Są one podobne zewnętrznie do układów firmy Microchip, bardzo zbliżone są także ich aplikacje.

Najważniejsze cechy charakterystyczne układów SureLok to:

- ✗ słowo wyjściowe ma długość 65 bitów, z czego 32 są kodowane dynamicznie, 28 spełniają rolę niezmiennego identyfikatora serii, a pozostałe wykorzystywane są do przesłania informacji o stanie baterii oraz o numerze aktualnego cyklu generatora kodu zmiennego;
- ✗ słowo - klucz, stanowiące bazę do wyliczania kolejnych kodów ma długość 64 bitów;
- ✗ zastosowanie trzech wejść dwustanowych, które binarnie określają numer wysyłanego rozkazu;



Rys. 14.

- ✗ kompatybilność mechaniczna i elektryczna z najbardziej popularnymi układami tego typu.

Niestety nie udało się nam zdobyć dokładnych informacji o sposobie działania (zwłaszcza synchronizacji) tych układów. Trudności te wynikają z faktu, że prezentowane w artykule układy dopiero wchodzą na rynek i większość dostępnych w końcu grudnia 1996 roku specyfikacji nosiła nagłówek „wstępne dane".

Tak więc do tematu układów generujących kody zmieniające się w czasie jeszcze wrócimy na łamach EP.

Tymczasem wszyscy zainteresowani najnowszymi informacjami na temat układów firm Microchip, National Semiconductor i Exel mogą zajrzeć do ich serwisu WWW, pod adresami:

- Microchip: www.microchip.com;
- National Semiconductor: www.natsemi.com;
- Exel: www.exel.com.

Piotr Zbysiński, AVT

Artykuł opracowano na podstawie materiałów dostarczonych przez firmy Elbatex i Gamma.