Zdalne sterowanie w systemach ochrony mienia

W październikowym numerze EP przedstawiliśmy ogólne założenia programu PR (Produkcja Rozproszona). Zainteresowanie tym pomysłem przeszło wszelkie nasze oczekiwania. Niezwykle ciekawie prezentują się wstępne wyniki ankiety rozpisanej na ten temat. Opublikujemy je wkrótce. Mamy też konkretne i poważne oferty firm dysponujących opracowaniami urządzeń odpowiednich dla tego programu.

Jako pierwszą wybraliśmy ofertę firmy ASHER dotyczącą całej serii urządzeń zdalnego sterowania stosowanych w systemach ochrony mienia. Urządzenia te działają w jednym spójnym systemie ASHER SRC. Jest to jeden z najlepszych systemów znanych redakcji EP. Ma on budowę modułową i jest w ciągłym rozwoju.

Poszczególne moduły i ich aplikacje przedstawimy w cyklu artykułów składającym się z kilkunastu części. W tym artykule przedstawiamy ogólny opis systemu, a w następnym (str. 71) - konstrukcję radiowego pilota zdalnego sterowania - pierwszego z serii kilkunastu modułów. Szczegółowe zasady funkcjonowania programu PR przedstawimy w następnym numerze EP.

Dostępne na rynku urządzenia do zdalnego sterowania to przede wszystkim systemy sterowania odbiorników telewizyjnych, magnetowidów i innych urządzeń powszechnego użytku. Od pewnego czasu upowszechnia się również zdalne sterowanie bram, autoalarmów i innych urządzeń o podobnym charakterze.

Przyrządy tego rodzaju nie tylko umożliwiają zdalne sterowanie, ale również ograniczają uprawnienia sterowania do wybranych „pilotów". Urządzenia te, w przytłaczającej większości przypadków, są projektowane w oparciu o układy scalone MC145026 (koder) i MC145028 (dekoder), TEA5500 (koder/dekoder) i inne, pracujące ze stałym kodem.

Cechą wspólną tych układów scalonych jest rozpoznawanie określonej kombinacji, zaprogramowanej poprzez podłączenie odpowiednich wyprowadzeń układu scalonego do plusa zasilania, minusa, lub pozostawienie niepodłączonych. Każde z wyprowadzeń kodujących może przyjąć jeden z trzech wybranych stanów. N wyprowadzeń umożliwia ustawienie 3^N różnych kodów. Dla MC145026 liczba ta wynosi 19683. Liczbę możliwych kodów zwiększa możliwość przyjęcia różnych prędkości transmisji danych. Przy transmisji radiowej akceptowalne prędkości transmisji są ograniczone do zakresu od 250 do 10000bps. Należy podkreślić, że małe prędkości zwiększają ryzyko zakłócenia odbioru, duże z kolei wymagają szerokiego pasma transmisji (min. 40kHz dla 10kbps dla prostego układu z MC145028). Liczbę możliwych nominalnych prędkości transmisji ogranicza również znaczna odporność dekodera na jej zmiany. Powszechnie stosowane są prędkości transmisji ok. 500, 1000, 2000bps.

Ogólna liczba kombinacji wydaje sie dostatecznie duża, jest wielokrotnie większa od liczby kombinacji typowego zamka bębenkowego. Głębsze wniknięcie w to zagadnienie ujawnia jednak istotne wady takiego systemu. Okazuje się, że np. przy prędkości transmisji 1000bps transmisja kompletnej sekwencji sterującej trwa ok. 57 ms. Oznacza to, że sprawdzenie wszystkich możliwych kombinacji („skanowanie" czyli dobranie wytrycha) zajmie ok. 1122s, czyli ok. 18 minut i 42 sekundy. Uwzględnienie możliwych wariantów prędkości transmisji zwiększa ten czas do mniej więcej jednej godziny. Prostą drogą zwiększenia odporności systemu jest wydłużenie czasu transmisji, utrudnia to jednak posługiwanie się pilotem. Niektóre firmy stosują układy emitujące kod wielobajtowy, którego znaczna część jest zaprogramowana maską podczas produkcji układu scalonego. Stosowane są również inne sposoby, jak np. czasowa blokada odbiornika po odebraniu nieprawidłowego kodu, przy wykorzystaniu której zakłócenia mogą całkowicie unieruchomić system. W nowoczesnych rozwiązaniach tego problemu stosuje się blokowanie odbiornika na pewien czas, po odebraniu kodu różniącego się jednym bitem od kodu właściwego. Rozwiązanie to wydaje się najlepszym spośród stosowanych, jednak skanery pracujące z losowym wybieraniem kodu radzą sobie z tym rozwiązaniem zupełnie nieźle.

Wady takiego systemu sterowania stają się szczególnie dotkliwe przy sterowaniu radiowym, o dużym zasięgu. Możliwe jest „skanowanie" ze znacznej odległości od pojazdu, czy nawet całej ich grupy. Proceder taki ułatwia przyjęcie znormalizowanej częstotliwości pracy pilotów radiowych, wynoszącej w Polsce 430MHz.

Myślę, że po chwili zastanowienia, większość Czytelników zauważy jeszcze jedną bardzo poważną wadę takiego systemu. Mianowicie, każde uruchomienie pilota ujawnia jego kod. Nie jest on widoczny gołym okiem, jednak może on być odebrany przez znajdujące się w pobliżu urządzenie, a następnie odtworzony „z taśmy" pod nieobecność właściciela systemu.

Do czasu kiedy urządzenia tego typu nie były zbyt powszechne, wady te nie miały istotnego znaczenia, jednak obecnie pojawiły się na rynku przestępczym przyrządy realizujące zarówno funkcję skanowania jak i nagrywania oraz odtwarzania kombinacji kodowych.

Wynika stąd niezbicie, że zdalne sterowanie oparte o wyżej opisane zasady, można stosować wyłącznie do obiektów o wymaganym niewielkim poziomie ochrony. Takim zastosowaniem jest np. sterowanie rygla blokującego drzwi wejściowe do budynków wielorodzinnych. Rygle takie, odblokowywane z mieszkania przyciskiem domofonu, a z zewnątrz kluczem, są stosowane powszechnie w blokach. Intensywne używanie zamka przez wielu lokatorów budynku powoduje szybkie jego zużycie i konieczność wymiany. Ponieważ wymiana zamka jest związana z koniecznością wymiany kluczy, jest to rozwiązanie kłopotliwe. Jednocześnie istnienie wielu duplikatów klucza powoduje, że zamek taki nie stanowi istotnego elementu zabezpieczającego. Zastosowanie zdalnego sterowania umożliwia w tym wypadku uniknięcie kłopotów związanych z wymianą zamka.

Zdalne sterowanie bramy garażowej, czy też autoalarmu, wymaga znacznie skutecz-

nejszego zabezpieczenia transmisji. System taki opracowany przez firmę ASHER i nazwany SRC jest właśnie przedmiotem tego artykułu.

System ASHER SRC eliminuje wszystkie zasadnicze wady sterowników ze stałym kodem (MC145026/MC145028, TEA5500....). Istotą systemu jest specjalny format informacji transmitowanej przez pilota do dekodera. Kod sterujący zawiera 11 bajtów informacji i, co najważniejsze, po użyciu kod jest unieważniany, aż do wykorzystania kolejnych 32768 kodów. Eliminuje to problem ujawnienia kodu przez użycie klucza. System ASHER SRC oferuje przeszło miliard różnych kodów klucza, każdy w 65536 wariantach. Złożoność kodu jest tak wysoka, że przełamanie go jest praktycznie niemożliwe. Funkcje systemu realizują specjalnie zaprogramowane procesory, każdy wyposażony we własny kod, a właściwie grupę kodów. Postać transmitowanego kodu jest następująca:

- cztery pierwsze bajty kodu to numer kodowy klucza (kod główny)
- dwa kolejne bajty to nr kolejny emisji kodu,
- następny bajt to kod transmitowanego rozkazu,
- cztery kolejne bajty to pseudolosowy kod kontrolny transmisji (sposób wyliczania tego kodu stanowi tajemnicę firmy ASHER),
- kolejne bajty to opcjonalna informacja dodatkowa.

Transmisja kodu jest poprzedzona sekwencją startową, złożoną z grupy impulsów stabilizujących pracę odbiornika. Generowana reprezentacja kodu jest zbliżona do właściwej dla układu MC145028. Ma to na celu umożliwienie wykorzystania układów nadawczych i przystosowanie do współpracy z układami MC145028 z zegarem 4kHz. Możliwość tę można wykorzystać w tych zastosowaniach, gdzie decydująca jest niska cena pilota, a wymagania co do jakości zabezpieczenia nie są wysokie. Kod główny, emitowany przez procesor nadawczy, jest zaprogramowany w nim na stałe. Kod ten, dla każdego procesora, jest dostępny w 16 wariantach. Umożliwia to bezkolizyjną współpracę jednego pilota z 16 różnymi urządzeniami odbiorczymi. Wariant kodu odzwierciedla się w czterech najmłodszych bitach kodu głównego. Dwa najstarsze bity kodu głównego określają klasę pilota. W systemie ASHER SRC wyróżniono trzy klasy pilotów:

PO - pilot z MC145028,

P1 - pilot z długim kodem (minimum 1 mld kombinacji), ale bez numerowania emisji,

P2 - pilot z numerowaną transmisją.

Oczywiście, najwyższy poziom zabezpieczenia zapewnia pilot typu 2. Zakładając losowe skanowanie procesora odbiorczego, przystosowanego do współpracy z takim pilotem, odkrycie właściwej kombinacji bitów wymaga emisji ok. 570.000.000.000.000.000 kombinacji. Ponieważ analiza przesłanego kodu, razem z transmisją, trwa ok. 0,3 sekundy, to przewidywany czas skanowania wyniesie parę miliardów lat. Wymaga to niezwykłej wprost cierpliwości i stawia bardzo wysokie wymagania dotyczące trwałości zarówno skanera, jak i skanującego. System jest również odporny na „ujawnienie kodu". Znając wyemitowany kod można oczywiście wyznaczyć kolejny numer emisji, ale trzeba wtedy przeskanować kod kontrolny transmisji. Wymaga to wyemitowania ponad 4 miliardów wariantów sekwencji sterującej. Przy założeniu, że emisja i analiza wariantu trwa ok. 0,3 sekundy, skanowanie zajmie około 40 lat. Czas ten znacznie przekracza przewidywaną żywotność urządzenia zabezpieczającego (od 5 do 10 lat). Z rachunku prawdopodobieństwa wynika, że odkrycie właściwej kombinacji nastąpi przeciętnie po połowie oszacowanego okresu, jednak 20 lat to też kawał czasu. Warto podkreślić, że przytoczony rachunek zakłada ciągłą pracę skanera, bez przerw na wymianę baterii i inne czynności obsługowe.

Najsłabszym punktem systemu ASHER SRC jest wyczerpywanie się licznika transmisji. Licznik ten, o pojemności 16 bitów, po 65536 emisjach zaczyna powtarzać już wykorzystane kombinacje. Ponadto, dla umożliwienia właściwej pracy systemu pomimo przypadkowego uruchomienia pilota, odbiornik akceptuje każdy z następnych 32768 kolejnych numerów emisji. Powoduje to, że po 32768 użyciach pilota, sekwencja wyemitowana za pierwszym razem staje sie ponownie ważna. Inaczej mówiąc, licznik emisji pracuje w kółko, a ostatnia pozycja licznika jakby poprzedza pierwszą. Przeciętna częstość korzystania z pilota wynosi ok. 8 razy dziennie. Oznacza to, że po ok. 10 latach sekwencje użyte w początkowym okresie eksploatacji systemu ponownie staną się ważne. Czas ten jednak odpowiada przyjętej żywotności systemu. Jeśli jednak ktoś uzna, że jest to zbyt krótki okres czasu, zawsze może przed jego upływem zmienić pilota, lub tylko wykorzystywany wariant kodu. Należy podkreślić, że każdy wariant kodu posiada niezależny licznik emisji. Oznacza to, że wykorzystanie tego samego pilota do kilku autoalarmów, otwierania bramy, drzwi garażowych itd. nie powoduje szybszego wyczerpania się licznika emisji, pod warunkiem, że każde z tych urządzeń będzie wykorzystywało inny wariant kodu.

Kod kontrolny transmisji jest kodem pseudolosowym, wyznaczanym jednak na podstawie wszystkich transmitowanych bajtów. Procesor odbiorczy, po odebraniu sekwencji sterującej, sprawdza kod główny i numer emisji, a następnie wyznacza kod kontrolny według takiego samego mechanizmu jak procesor nadawczy. Jeśli kod główny jest zarejestrowany w procesorze i pozostałe dane są zgodne z przewidywanymi, to następuje zwiekszenie licznika emisji, pamiętanego wraz z kodem głównym, oraz wykonanie rozkazu.

Rozkazy transmitowane przez pilota systemu ASHER SRC dzielą się na dwie kategorie: systemowe i użytkowe. Rozkazy użytkowe sterują pracą aplikacji i ich znaczenie definiuje właśnie ona. Do sterowania aplikacją przewidziano rozkazy od 1 do 5. Rozkazy te powodują włączenie lub wyłączenie urządzenia, jak również obsługę jego funkcji dodatkowych. Jako zasadę przyjęto, że rozkaz nr 1 włącza urządzenie (np. autoalarm) lub zamyka dostęp (np. zamyka bramę), podczas gdy rozkaz nr 2 wyłącza lub otwiera. Rozkazy systemowe nie zależą od aplikacji:

6 - zarejestruj klucz
7 - wyrejestruj klucz
8 - zarejestruj klucz nr...
9 - wyrejestruj klucz nr...
10 - odczytaj blok użytkownika
11 - zapisz blok użytkownika
12 - zapisz dane systemowe
13 - odczytaj dane systemowe
14 - kasuj wszystkie klucze
15 - odczytaj klucz nr...
16 - odczytaj blok użytkownika jeśli był alarm

Rozkazy 6, 7, 8, 9, 11, 12, 13, 14 i 15 mogą być zlecone tylko przez dwa klucze, zarejestrowane jako pierwsze. Zainicjowanie rejestracji pierwszego klucza odbywa się w sposób właściwy dla konkretnej aplikacji, najczęściej przez naciśnięcie odpowiedniego przycisku. Kolejne klucze należy rejestrować wykorzystując rozkaz nr 6 lub 8. Odebranie rozkazu nr 6 powoduje, że procesor odbiorczy czeka do 5 sekund na kolejną emisję. Emisja ta, po weryfikacji kodu kontrolnego, jest traktowana jako kod rejestrowanego klucza. Rozkaz 8 zawiera kod rejestrowanego klucza w dodatkowo transmitowanych bajtach. Rozkazy 7 i 9 zapewniają możliwość wyrejestrowania klucza, czyli jego unieważnienia. Rozkaz 9 zawiera w dodatkowo transmitowanych bajtach kod unieważnianego klucza, podczas gdy rozkaz 7 wymaga wyemitowania kodu przez klucz unieważniany, przed upływem 1,2 sekundy do odebrania rozkazu nr 7. Rozkaz nr 10 powoduje wyemitowanie przez odbiornik bloku informacji użytkownika. Blok ten zawiera (opcjonalnie) dane takie jak stan urządzenia oraz informacje zapisane w pamięci rozkazem 11. Rozkaz 10 jest wykonywany nawet jeśli pochodzi z pilota nie zarejestrowanego, z tym, że musi to być pilot klasy P1 lub P2. Rozkaz 16 wykonywany jest tylko w przypadku jeśli aplikacja jest w stanie alarmu - jest on ważny wyłącznie dla urządzeń alarmowych. Podobnie jak rozkaz nr 10, rozkaz 16 jest akceptowany również dla pilotów nie zarejestrowanych. Rozkazy 10, 11 i 16 umożliwiają nadanie urządzeniu cech redukujących celowość ich kradzieży, przez wpisanie np. nazwiska właściciela. Podobną funkcję pełnią rozkazy 12 i 13 - umożliwiają one wpisanie cech producenta urządzenia, jak również umożliwiają odczyt typu procesora.

Rozkaz 14 unieważnia wszystkie klucze. Rozkaz 15 umożliwia odczyt kodu klucza, zarejestrowanego na pozycji podanej w dodatkowym bajcie rozkazu. Zależnie od wersji procesora, maksymalna liczba kluczy waha się od kilku do kilkudziesięciu. Pro-

cesory współpracujące z pamięcią ST24CO2 umożliwiają pamiętanie 36 różnych kluczy i kilkudziesięciu bajtów informacji dodatkowej.

Typowe piloty, wyposażone w jeden lub kilka przycisków, mogą wysyłać tylko rozkazy od 1 do 7. Sposób spowodowania emisji zależy od konstrukcji pilota. Rozkazy od 8 do 16 są zarezerwowane dla specjalnych kontrolerów systemu, pełniących funkcje zarówno nadajnika jak i odbiornika. Również urządzenia sterowane, które mają realizować rozkazy 10, 13, 15 i 16, muszą być wyposażone w urządzenie nadawczo-odbiorcze.

Standard ASHER SRC przewiduje również klasyfikację urządzeń sterowanych.

Wyróżniono następujące klasy:

O0 - Wyposażone tylko w odbiornik, współpracujące z pilotami klasy P0, P1, P2

O1 - Wyposażone tylko w odbiornik, współpracujące z pilotami klasy P1 i P2

O2 - Wyposażone tylko w odbiornik, współpracujące z pilotami klasy P2

T0 - Wyposażone w transceiver, współpracujące z pilotami klasy P0, P1 i P2

T1 - Wyposażone w transceiver, współpracujące z pilotami klasy P1 i P2

T2 - Wyposażone w transceiver, współpracujące z pilotami klasy P2

Klasyfikacja nie określa częstotliwości nośnej systemu, domyślnie wynosi ona 430 MHz. Jeśli częstotliwość pracy systemu odbiega od podanej, oznaczenie powinno określać ten parametr. Oznaczenie klasy urządzeń z kwarcową stabilizacją częstotliwości nośnej powinno być poprzedzone literą „X". Jeśli transmisja realizowana jest za pomocą promieniowania podczerwonego, to oznaczenie klasy urządzenia należy poprzedzić literą „O". Powyższe uwagi dotyczą również oznaczania rodzaju pilota...

Urządzenia produkowane w oparciu o system ASHER SRC nie są tak tanie jak rozwiązania klasyczne, jednak ich wyjątkowe walory powodują, że ceny wydają się obiektywnie niskie w porównaniu z cenami gotowych wyrobów dostępnych na rynku, opartych na zasadach opisanych na początku artykułu. Co wiecej, ASHER SRC jest jednym z niewielu systemów rzeczywiście trudnych do przełamania, a jego skuteczność można porównywać tylko z najdroższymi na rynku systemami, opartymi na transmisji dwukierunkowej. W systemie takim odbiornik, po przyjęciu rozkazu, transmituje pewien kod do pilota, który z kolei przetwarza go według specjalnego algorytmu i wysyła do odbiornika. Odbiornik porównuje ten kod z kodem przetransformowanym we własnym zakresie i zależnie od wyniku wykonuje rozkaz lub nie. Systemy takie, przy porównywalnej skuteczności, są znacznie droższe od przedstawionego.

Poszczególne procesory systemu ASHER SRC omówione zostaną przy okazji publikacji urządzeń, które je wykorzystują. Planowany cykl artykułów obejmuje następujące moduły:

- radiowy (430MHz) pilot zdalnego sterowania oparty o MC145028 (w tym numerze EP),
- moduł odbiornika radiowego na 430MHz (w EP 1/94),
- moduł transceivera na 430MHz,
- sterownik rygla oparty o MC145026 (w EP 1/94),
- prosty autoalarm oparty o MC145026,
- radiowy pilot zdalnego sterowania systemu ASHER SRC,
- uniwersalny moduł procesora odbiorczego systemu ASHER SRC,
- sterownik rygla w systemie ASHER SRC,
- autoalarm w systemie ASHER SRC,
- sterownik do napędu z silnikiem komutatorowym w systemie ASHER SRC (otwieranie bram, drzwi garażowych, sterowanie szlabanów itp.),
- indywidualna centralka alarmowa w systemie ASHER SRC,
- centralka alarmu towarzyskiego w systemie ASHER SRC.

AVT

Odrębnego wyjaśnienia wymagają zasady, na których firma ASHER udostępniła nam licencję produkcyjną na system SRC.

1. Znak firmowy ASHER jest zastrzeżonym znakiem towarowym. Właściciel znaku nie wyraża zgody na używanie tego znaku do oznaczania wyrobów innych firm, poza nastepującymi przypadkami:

1.1 Znak towarowy ASHER może być użyty przez producenta w celu określenia stopnia kompatybilności produkowanego urządzenia z systemem ASHER SRC, pod warunkiem, że urządzenie jest produkowane w oparciu o procesory programowane przez firmę ASHER. Znak towarowy ASHER nie może być umieszczony na obudowie urządzenia, ani też na jego opakowniu.

1.2 Umieszczenie znaku towarowego ASHER na obudowie lub opakowaniu urządzenia wymaga uzyskania osobnego zezwolenia firmy ASHER.

1.3 Wykorzystanie znaku towarowego ASHER w celach reklamowych wymaga uzyskania osobnego zezwolenia firmy ASHER.

2. Jeśli producent wykorzystuje znak towarowy ASHER, z uwzględnieniem warunków punktu pierwszego, to jest tym samym zobowiązany do czytelnego oznaczenia klasy urządzenia w/g zasad opisanych w tym artykule.

3. Koncepcja systemu zdalnego sterowania, opisana w tym artykule, stanowi wyłączną własność firmy ASHER. Właściciel koncepcji nie wyraża zgody na wykorzystanie tej koncepcji przez inne firmy.

4. Oprogramowanie realizujące funkcje systemu ASHER SRC stanowi wyłączną własność firmy ASHER. Właściciel oprogramowania wyraża zgodę na rozpowszechnianie tego oprogramowania wyłącznie w postaci procesorów zaprogramowanych w firmie ASHER.