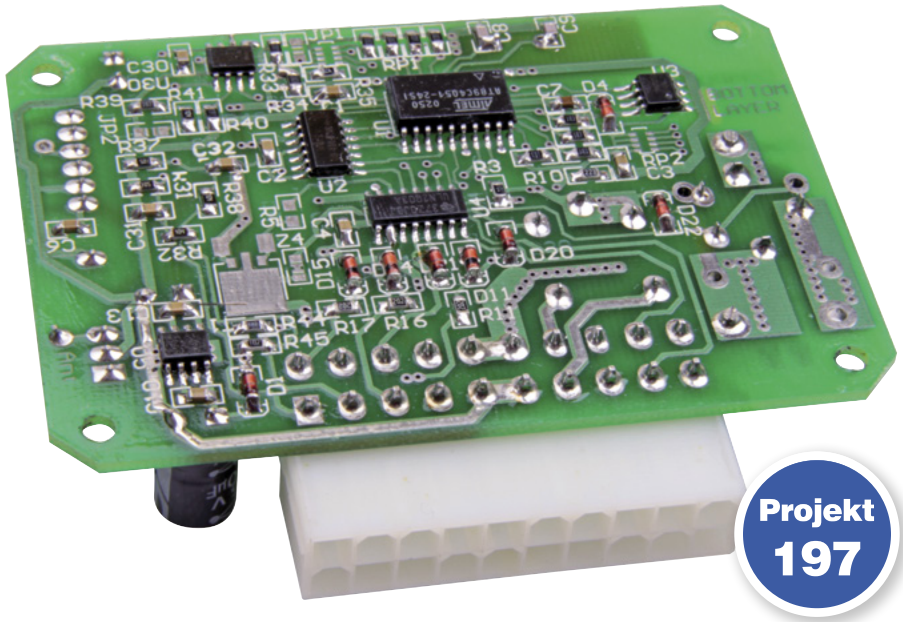
Alarm samochodowy ze zdalnym sterowaniem kodem kroczącym

Współczesne auta naszpikowane są elektroniką. Zdalne sterowanie, centralny zamek, immobilizer, alarm czy elektryczne szyby są obecnie standardem. Posiadacze starszych samochodów lub osoby zajmujące się tuningiem mogą samodzielne wykonać różne urządzenia w celu podniesienia komfortu użytkowania swoich samochodów. W artykule opisano sposób wykonania i dołączenia do instalacji samochodu alarmu z kodowanym sygnałem zdalnego sterowania. Na bazie opisanego urządzenia można wykonać inne ulepszenia i wprowadzić je do auta. Mogą to być na przykład centralny zamek czy system elektrycznego domykania szyb.



Projekt 197

Głównym zadaniem systemu jest zapewnienie autoryzowanego zdalnego dostępu do funkcji alarmu takich jak uzbrajanie czy rozbrajanie. Ważne jest aby rozwiązanie było bezpieczne ponieważ z powyższymi funkcjami na ogół powiązane są funkcje otwierania i zamykania centralnego zamka. W przypadku zbyt słabego rozwiązania można osiągnąć efekt odwrotny do oczekiwanego, gdzie możliwe będzie na przykład podsłuchanie transmisji i nieautoryzowany dostęp, a przy okazji otwarcie na oścież drzwi potencjalnemu złodziejowi.

Rozsądnym wyjściem wydaje się zastosowanie sprawdzonego i funkcjonującego w podobnych urządzeniach, a przez to dostępnego na rynku, rozwiązania. Wybór padł na powszechnie stosowany w układach zdalnego dostępu algorytm KeeLoq firmy Microchip. Jako koder użyty został układ HCS200 (opis układu i programatora w EP 1/2012). Układ został zaprojektowany z myślą o zastosowaniu w nadajnikach zdalnego sterowania. Ogranicza to liczbę dodatkowych elementów pracujących po stronie nadawczej. Ponadto, zoptymalizowano go pod kątem pracy w urządzeniu zasilanym z baterii. Wyposażono go wobec tego w mechanizmy ograniczające pobór prądu do niezbędnego minimum, co wydłuża czas pracy przy zasilaniu z baterii. Ponadto, układ sygnalizuje niskie napięcie baterii, a tym samym konieczność jej wymiany, poprzez przesyłanie wraz z innymi danymi transmitowanymi do odbiornika specjalnej flagi.

Zastosowany algorytm (zwany potocznie kodem kroczącym) zapewnia bezpieczeństwo systemu. Transmisja odbywająca się pomiędzy nadajnikiem a odbiornikiem jest zakodowana. Ponadto, każdy kolejny kod przesyłany drogą radiową jest inny. Zrealizowano to dzięki dodaniu stanu licznika do paczki przesyłanych. Licznik ten jest inkrementowany przy każdej transmisji. Aktualny stan licznika jest zsynchronizowany w obu urządzeniach: nadawczym i odbiorczym.

Dodatkowe materiały na CD/FTP:
ftp://ep.com.pl, user: 18453, pass: 5eyp1854
- wzory płytek PCB
- karty katalogowe i noty aplikacyjne elementów oznaczonych w Wykazie elementów kolorem czerwonym

Aby kody wysłane dotychczas nie mogły zostać ponownie użyte, urządzenie odbiorcze nie dopuszcza autoryzacji poprzednich 32 tysięcy stanów licznika. Autoryzowane są wyłącznie większe wartości licznika, ale z pewnym zastrzeżeniem. Jako bezpieczny uznawana jest wartość licznika z zakresu do 16 większa od ostatnio zapamiętanej przez odbiornik. W wypadku, gdy urządzenie odbiorcze odbierze wartość licznika znacznie wyprzedzającą ostatnio zapamiętaną (o 16…32000) jest wymagana ponowna synchronizacja nadajnika i odbiornika. Operacja ta wymaga odebrania dwóch następujących po sobie wartości licznika. Powyższe zabezpieczenie ma zabezpieczyć urządzenie przed próbą złamania kodu polegającą na wygenerowaniu i wysyłaniu dużej liczby losowych kodów. W takim wypadku odbiornik mógłby zareagować na przypadkowo wygenerowany kod. Opisany scenariusz jest mało prawdopodobny ze względu na ogromną liczbę kombinacji, które należałoby wysłać, jednak producent zabezpieczył odbiornik przed tą metodą ataku. Z drugiej strony, układ musi zapewniać ponowną synchronizację urządzeń. Może się zdarzyć, że nadajnik będzie pracował poza zasięgiem lub też użytkownik będzie zwyczajnie bawił się nim i wyśle 16 kolejnych kodów, które nie zostaną zarejestrowane przez odbiornik. W tym wypadku ponowna synchronizacja jest dosyć intuicyjna. Użytkownik wysyła kod – np. o 20 przewyższający ostatnio zapamiętany w odbiorniku. Centralka odrzuca ten kod i nie reaguje na niego. Naturalną reakcją jest ponowne naciśnięcie przycisku pilota i wysłanie kolejnego kodu różniącego się już o 21. Taka wartość licznika zostanie zaakceptowana przez odbiornik i jednocześnie zapamiętana – urządzenia będą ponownie zsynchronizowane.

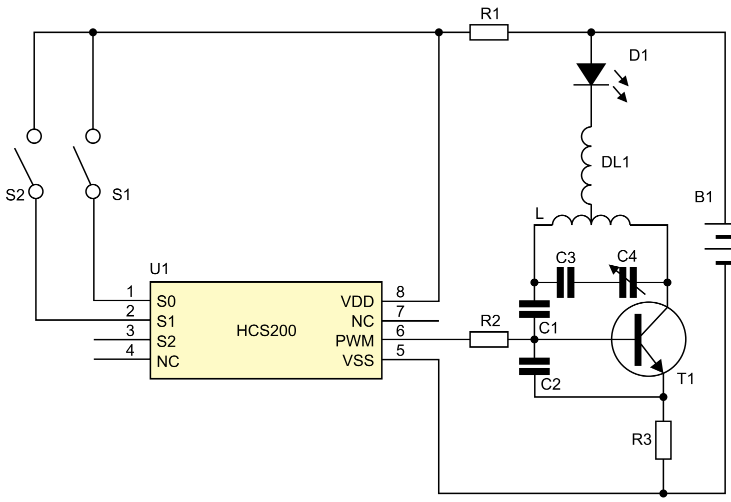
Aby cały system był poprawnie zabezpieczony przed nieautoryzowanym dostępem konieczne jest zachowanie w tajemnicy wartości klucza używanego do kodowania danych. Nadajnik HCS200 spełnia te wymaganie – weryfikacja danych może nastąpić wyłącznie w połączeniu z programowaniem układu – późniejszy odczyt układu jest niemożliwy. W wypadku odbiornika o bezpieczeństwo danych musimy zatroszczyć się sami. Mikrokontroler, w którego pamięci jest zapisany klucz, powinien zostać zabezpieczony. Użyty w układzie typ mikrokontrolera daje taką możliwość. Oczywiście klucz powinien zostać wymyślony samodzielnie i nie należy powielać klucza użytego w tym projekcie. Jest on powszechnie znany, co nie zapewnia bezpieczeństwa systemu.

Pilot

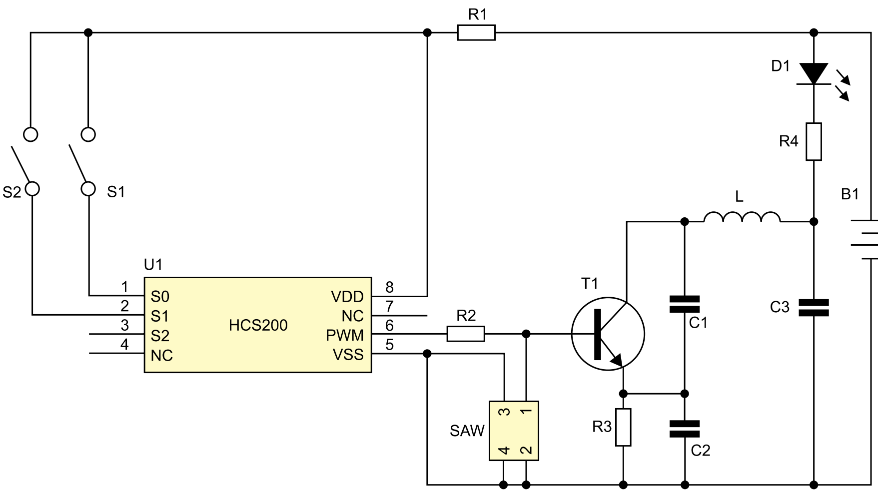
Pilot został wykonany w dwóch wersjach: RLC (**rysunek 1**) i SAW (**rysunek 2**). Pierwsza wersja może być problematyczna w wykonaniu i uruchomieniu w warunkach amatorskich. Przy uruchamianiu należy zestroić generator nośnej, co wymaga posiadania odpowiednich przyrządów (np. analizatora widma). Wobec tego opracowano wersję alternatywną z generatorem SAW. Ponadto, drugi układ może być wykonany na laminacie jednostronnym i dlatego w wersji SAW jest łatwa do wykonania i uruchomieniu w warunkach amatorskich (ale niestety mniej odporna mechanicznie). Schematy oraz rozmieszczenie elementów przedstawiony zostały na poniższych rysunkach.

Przedstawione układy różnią się sposobem generowania fali nośnej. W pierwszym z nich nośna jest generowana poprzez układ RLC. W drugim rozwiązaniu rolę generatora pełni rezonator SAW.

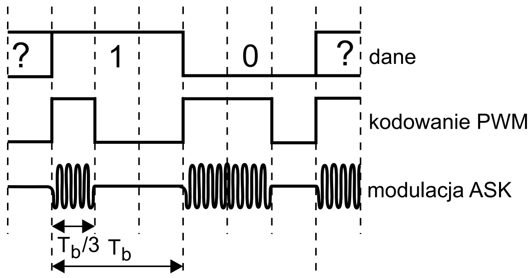
Sercem obu rozwiązań jest układ HCS200. Realizuje on większość funkcji: rozpoznaje, który z przycisków został wciśnięty, pobiera aktualny licznik transmisji i numer seryjny oraz koduje dane za pomocą klucza. Układ formuje również niezbędne dane w paczki łatwe do obróbki po stronie odbiorczej. Są one przesyłane cyklicznie w trakcie naciskania przycisku nadajnika. Paczka zawiera dane pomocnicze potrzebne do zsynchronizowania urządzeń i określenia czasu trwania pojedynczego elementu transmisji oraz treść transmisji w postaci sygnału PWM (dane do wysłania są dostępne na wyprowadzeniu PWM układu). Transmisja tej treści do urządzenia odbiorczego, wybranym przez siebie sposobem (podczerwień, drogą radiową itp.), leży w gestii konstruktora. W opisywanym urządzeniu wybrano transmisję drogą radiową i modulację amplitudową ASK. Sposób kodowania danych oraz modulacji został przedstawiony na **rysunku 3**.



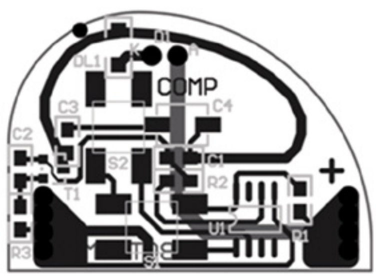
Rysunek 1. Pilot zdalnego sterowania – wersja RLC



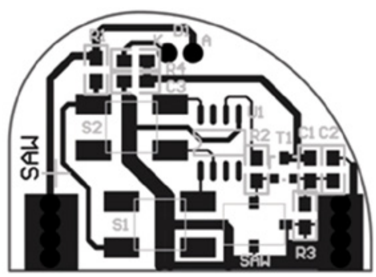
Rysunek 2. Pilot zdalnego sterowania – wersja SAW



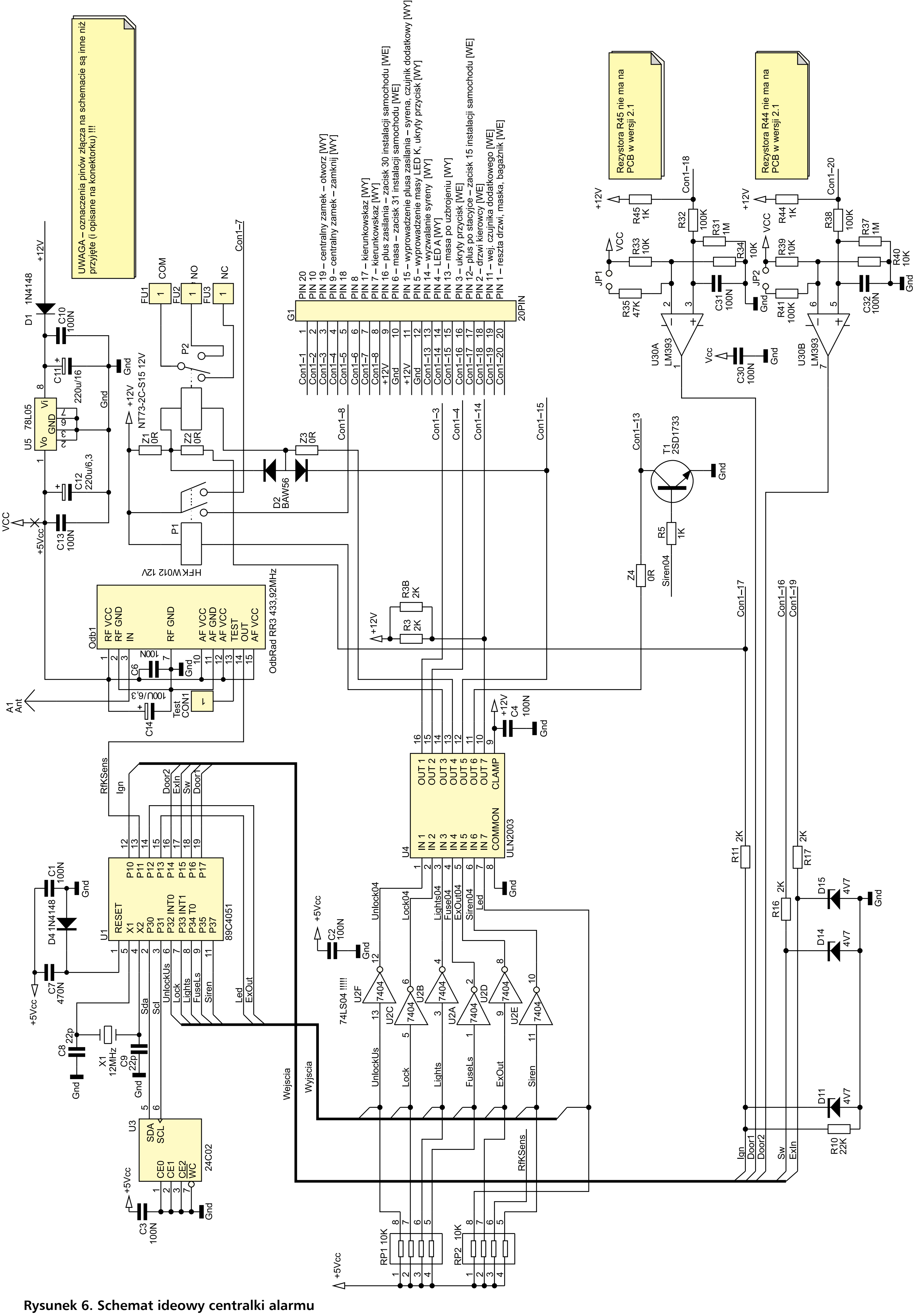
Rysunek 3. Sposób kodowania danychw czasie transmisji



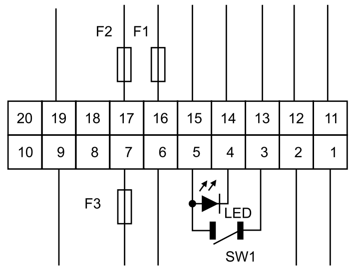
Rysunek 4. Schemat montażowy płytki pilota – wersja RLC



Rysunek 5. Schemat montażowy płytki pilota – wersja SAW



Rysunek 6. Schemat ideowy centralki alarmu

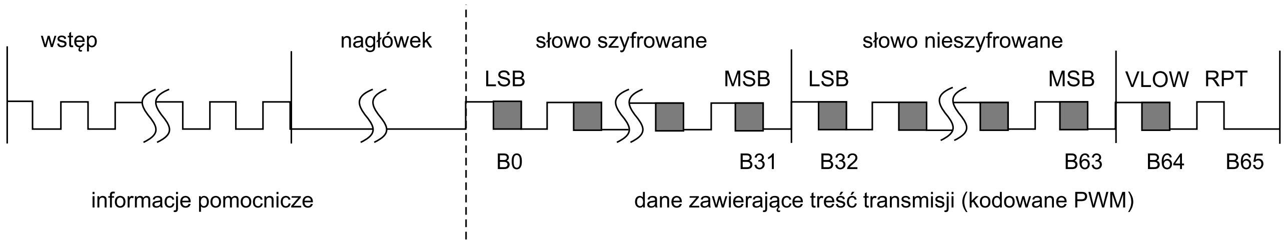


Rysunek 7. Rozmieszczenie doprowadzeń złącza

pięcia wynika z faktu, że w obwodzie mogą pojawić się dodatkowe diody separujące i napięcie na wejściu będzie podniesione o spadek napięcia na złączach półprzewodnikowych. Rolę odbiornika radiowego transmisji ASK pochodzącej z pilota pełni gotowy, zestrojony tor radiowy. Dane pochodzące z odbiornika trafiają bezpośrednio do mikrokontrolera. Rolę półfalowej anteny odbiorczej pełni przewód o długości 34 cm.

Wiązka

Do połączenia urządzenia z instalacją samochodową jest niezbędna wiązka przewodów. Wiązka jest połączona z centralką poprzez 20-pinowe złącze, rozmieszczenie doprowadzeń którego pokazano na **rysunku 7**. Do złącza należy wpiąć piny, do których lutujemy lub zaciskamy 10 przewodów (masa 0,75 mm^2, pozostałe 0,5 mm^2), kolejne 3 przewody zawierające wkładki bezpiecznika oraz dwa dwużyłowe przewody (0,25 mm^2



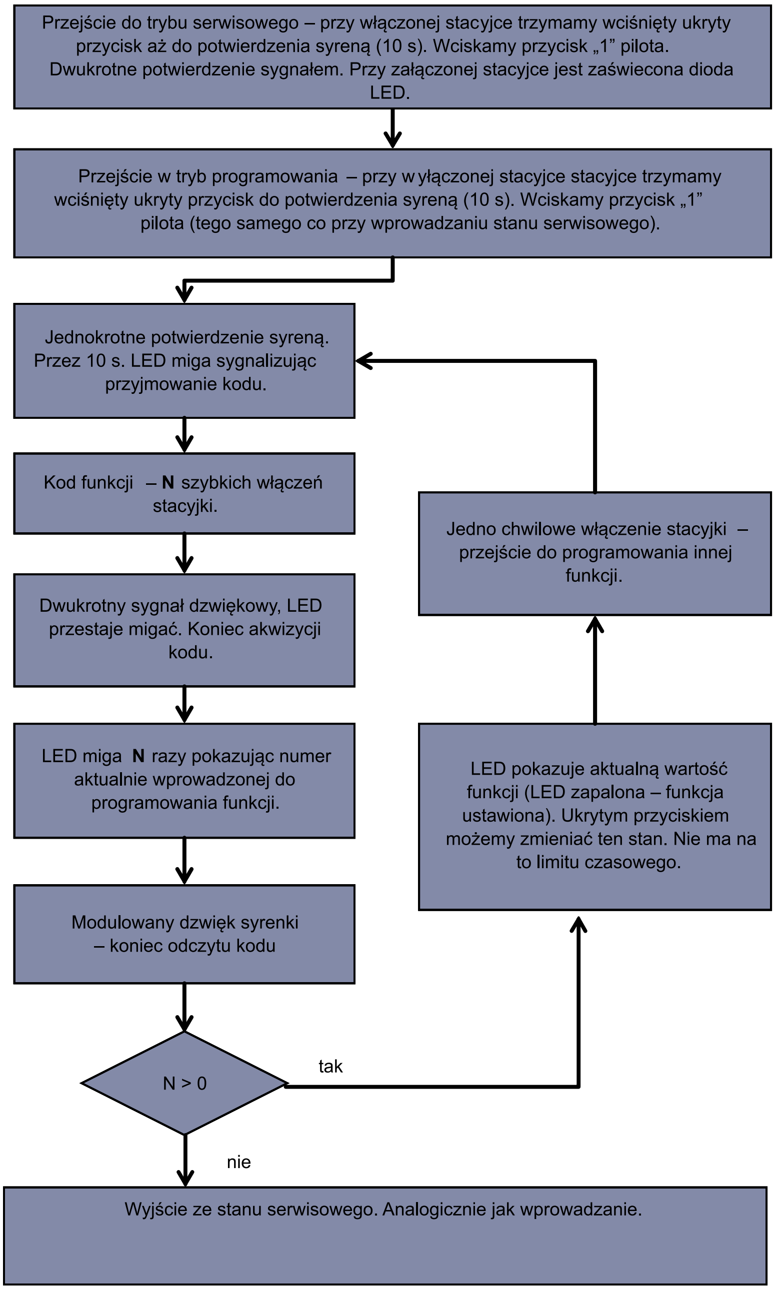
Rysunek 8. Ramka danych

Kodowanie PWM upraszcza akwizycję danych w urządzeniu odbiorczym. Ponieważ każdy bit jest kodowany na trzech elementach, gdzie pierwszy z nich przyjmuje zawsze poziom wysoki a ostatni zawsze poziom niski, jest możliwa synchronizacja odbiornika z każdym bitem, nawet w wypadku, gdy są przesyłane długie ciągi samych zer lub jedynek. Środkowy element zakodowanego sygnału niesie ze sobą informacje – przy czym jest on zanegowany w stosunku do danych niekodowanych.

Płytkę drukowaną nadajnika należy zaprojektować samodzielnie, odpowiednio do stosowanej obudowy. Płytki zastosowane przez autora artykułu pokazano na **rysunku 4** (w wersji RLC) i **rysunku 5** (w wersji SAW).

Centralka

Schemat ideowy centralki umieszczono na **rysunku 6**. Program centralki jest wykonywany przez mikrokontroler AT89C4051. Układ umożliwia zabezpieczenie przed odczytem pamięci wewnętrznej, zawierającej numer producenta. Pamięć zewnętrzna EEPROM służy do przechowywania numerów seryjnych oraz liczników synchronizacji pilotów. Oprócz tego w pamięci są przechowywane informacje o ustawionych funkcjach dodatkowych oraz aktualny stan centralki. Urządzenia sterowane są za pośrednictwem układów 74LS04 i ULN2003. Obciążalność wyjścia wyzwalania syreny alarmowej można opcjonalnie zwiększyć dodając tranzystor T1. Układy wejściowe są połączone z mikrokontrolerem w dość prosty sposób – poprzez rezystory 2 kΩ. Diody Zenera zabezpieczają wejścia przed wystąpieniem zbyt wysokich napięć. Wyjątkiem są wejścia dla wyłączników drzwi i maski, gdzie zastosowano komparatory. Potrzeba wyzwalania wyższym progiem na-



Rysunek 9. Algorytm działania programu

na LED i ukryty przycisk). Optymalną długością przewodów wystarczającą do wykonania wszystkich połączeń w kabinie jest 1,5 m. Wyprowadzenia syrenki (piny 14 i 15) powinny być dłuższe (2,5 m), ponieważ muszą dosięgnąć do przedziału silnika, gdzie na ogół instaluje się syrenkę. Do zacisku 5 należy zarobić wspólnie po 1 żyle przewodów dwużyłowych. Pozostałe dwa przewody dołączamy do pinów 3 i 4. Do przewodów dwużyłowych podłączamy diodę LED oraz przycisk.

Oprogramowanie

Program centralki pierwotnie napisany został w większości w języku C (poza obsługą przerwań krytycznych czasowo). Wraz z rozwijaniem kodu o kolejne funkcje, ze względu na ograniczoną pojemność pamięci wewnętrznej mikrokontrolera oraz na wymagania czasowe większość procedur została przepisana na asembler. Ostatecznie tylko główna pętla programu pozostała w C ze względu na częstość i łatwość modyfikacji (w porównaniu z asemblerem). Kod źródłowy składa się z następujących plików:

- Alarm.c – główna pętla programu.
- Decrypt.a51 – dekodowanie danych transmitowanych z pilota przy użycia klucza wygenerowanego z numeru seryjnego oraz kodu procudenta (ładowanego w procedurze *LOAD_MKEY*).
- Eei2c.a51 – obsługa pamięci EEPROM.
- Iotim.a51 – periodyczna obsługa wejść i wyjść (co wielokrotność 5 ms w zakresie 5…1280 ms).
- Rf_rec.a51 – akwizycja danych pochodzących z toru radiowego (przerwanie co 120 µs).
- Sysctrl.a51 – warstwa pośrednia pomiędzy kodem w C a kodem w asemblerze.

Ponadto, projekt zawiera jeszcze pliki dedykowane dla środowiska: pliki projektu oraz plik startup.a51. Przy samodzielnej kompilacji należy zwrócić uwagę na zmianę kodu producenta na własny, pozostający w tajemnicy. Kod jest ładowany procedurze *LOAD_MKEY* znajdującej się w pliku decrypt.a51. Istotną kwestią przy projektowaniu urządzenia i kodu było zapewnienie stabilnej komunikacji radiowej. Wymusiła ona pewne decyzje projektowe – między innymi napisanie procedury obsługi toru radiowego (plik Rf_rec.a51) w asemblerze. Format danych pochodzących z odbiornika RF przedstawiony został na rysunku.

Czas pojedynczego elementu pojawiającego się w sygnale RF jest określony na 400 µs (jeden bit jest kodowany PWM na trzech elementach). Próbka jest pobierana co 120 µs co pozwala na trzykrotne lub czterokrotne sprawdzenie pojedynczego elementu, przy założeniu, że trwa on 400 µs. Rzeczywisty czas może odbiegać od podanego – dokumentacja definiuje ten czas w granicach 280…620 µs.

Listing 1. Definiowanie klucza szyfrowania

```
;;;  41:4c:41:6d:72:61:6c:61
LOAD_MKEY:
  MOV DKEY0, #061H
  MOV DKEY1, #06CH
  MOV DKEY2, #061H
  MOV DKEY3, #072H
  MOV DKEY4, #06DH
  MOV DKEY5, #041H
  MOV DKEY6, #04CH
  MOV DKEY7, #041H
  RET
```

W paczce danych pokazanej na **rysunku 8** przesyłane są kolejno:

- Wstęp – sygnał prostokątny, który przygotowuje odbiornik do akwizycji danych.
- Nagłówek – na jego podstawie odbiornik może określić prędkość transmisji. Czas trwania nagłówka jest równy czasowi dziesięciu elementów bazowych.
- Słowo szyfrowane.
- Słowo nieszyfrowane.

Akwizycja danych rozpoczyna się od pomiaru czasu trwania nagłówka, a dokładniej od określenia liczby próbek przypadających na jeden element. Pobieranie bitów zakodo-

Wykaz elementów:

Pilot zdalnego sterowania (wersja RLC)

Rezystory: (SMD 0805)
R1: 1 kΩ
R2: 10 kΩ
R3: 10 Ω
Kondensatory: (SMD)
C1…C3: 2,2 pF (0805)
C4: trymer 3…30 pF (1210)
Półprzewodniki:
U1: enkoder HCS200 (obudowa SO-8)
T1: BFS17 (obudowa SOT-23)
D1: Dioda LED 3 mm czerwona
Inne:
DL1: dławik 10 μH (SMD, 1210)
B1: bateria 12 V A23
S1, S2: przycisk SMD 6,2 mm×6,2 mm×5,0 mm
Obudowa KM5
Blaszki stykowe
Zawieszka

Pilot zdalnego sterowania (wersja SAW)

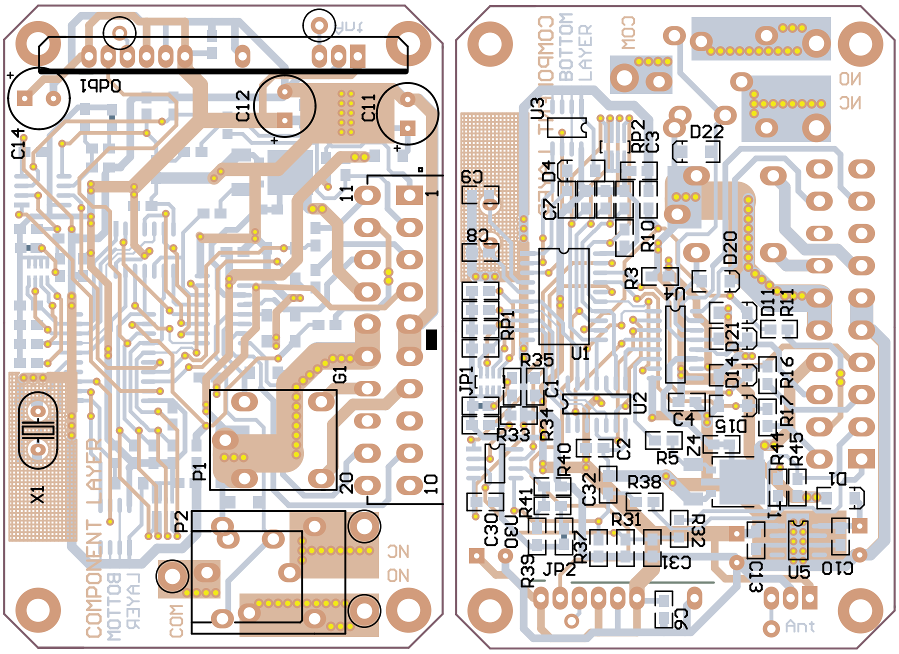
Rezystory: (SMD 0805)
R1: 1 kΩ
R2: 47 kΩ
R3: 220 Ω
R4: 22 Ω
Kondensatory: (SMD 0805)
C1: 2,2 pF
C2: 12 pF
C3: 470 pF
Półprzewodniki:
U1: enkoder HCS200 (obudowa SO-8)
T1: BFS17 (obudowa SOT-23)
D1: Dioda LED 3 mm czerwona
Inne:
SAW: Oscylator SAW 433,92 MHz
B1: bateria 12 V A23
S1, S2: przycisk SMD 6,2 mm×6,2 mm×5,0 mm
Obudowa KM5
Blaszki stykowe
Zawieszka

Centralka alarmu

Rezystory:
RP1, RP2: RPACK 4×10 kΩ
R3, R3B, R11, R16, R17: 2 kΩ
R5: 1 kΩ (opcjonalnie)
R10: 22 kΩ
R32…R34, R38…R41: 10 kΩ
R31, R37: 1 MΩ
R35: 47 kΩ
R44, R45: 1 kΩ
Kondensatory:
C1…C4, C6, C10, C13, C30…C32: 100 nF
C8, C9: 22 pF
C7: 470 nF
C11: 220 μF/16 V
C12: 220 μF/6,3 V
C11: 100 μF/6,3 V
Półprzewodniki:
U1: AT89C4051 (SOL-20)
U2: 74LS04 (SO-14)
U3: 24C02 (SO-8)
U4: ULN2003A (SO-16)
U5: 78L05A (SO-8)
U30: LM393 (SO-8)
T1: 2SD1733 (opcjonalnie)
D1, D4: 1N4148
D2: BAW56
D11, D14, D15: dioda Zenera 4,7 V
Inne:
Odb1: RR3-433.92MHz Telecontrolli
X1: kwarc 12 MHz
P1: przekaźnik 12 V HFKW012
P2: przekaźnik 12V NT73-2C-S15
G1: złącze kątowe 20 pin MRX6920
A1: antena (przewód o długości 34 cm)
Obudowa KM54, wkręty

Wiązki przewodów

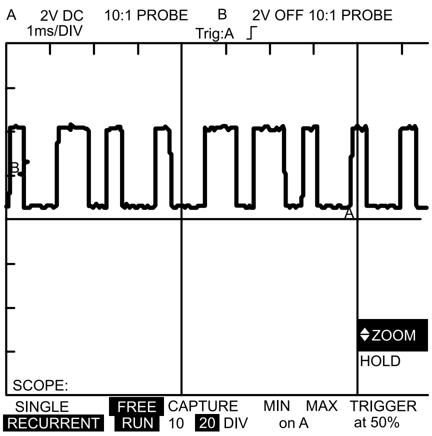
LED: dioda LED ø5 mm czerwona
SW1: przycisk SMD 12 mm×12 mm×4,3 mm
F1: bezpiecznik 15A
F2, F3: bezpiecznik 7,5A
Złącze MRX6920
Pin MRX69 – 16 szt.
Przewód z gniazdem bezpiecznika 0,75 mm² – 3 szt. po 1,5 m
Przewód jednożyłowy 0,75 mm², 1,5 m – 1 szt.
Przewód jednożyłowy 0,5 mm² – 7 szt. po 1,5 m i 2szt. po 2,5 m
Przewód dwużyłowy 0,25 mm² – 2 szt. po 1,5 m



Rysunek 10. Schemat montażowy centralki

Listing 2. Fragment kodu programu zawierający tablicę z kluczem szyfrowania

```
Offset(h) 000102030405060708090A0B0C0D0E0F
00000770  85332F532F0F2275346175356C753661   …3/S/."u4au5lu6a
00000780  75377275386D753941753A4C753B4122   u7ru8mu9Au:Lu;A"
```



Rysunek 11. Przesłanie bitu

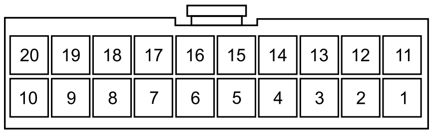
wanych PWM polega na sprawdzeniu czy pierwszy element ma wartość „1", pobraniu do bufora zanegowanej wartości drugiego elementu, sprawdzeniu czy trzeci element ma wartość „0" i ostatecznie na synchronizacji ze zboczem rosnącym rozpoczynającym kolejny bit.

Graf ilustrujący algorytm funkcjonowania programu pokazano na **rysunku 9**.

Uruchomienie układu

Schemat montażowy centralki alarmu pokazano na **rysunku 10**. Projekt płytki drukowanej można znaleźć w plikach zawierających materiały dodatkowe do projektu, zapamiętanych na płycie CD-EP2/2012 oraz na serwerze FTP.

Uruchomienie całego systemu najlepiej rozpocząć od zaprogramowania mikrokontrolera oraz enkoderów HCS200. Aby układ działał poprawnie koder oraz dekoder muszą używać



Pin	Funkcja
1	Wyłączniki maski i bagażnika (zwierane do masy)
2	Wyłączniki drzwiowe (zwierane do masy)
3	Ukryty przycisk (zwierany do masy)
4	Dioda LED (anoda)
5	Wyprowadzenie masy dla ukrytego przycisku i diody LED (katoda)
6	Masa – zacisk 31 instalacji samochodu
7	Kierunkowskaz
8	-
9	Sterowanie centralnym zamkniem – zamykanie – sygnał masy 500ms (12 sek. – domykanie)
10	-
11	Wyzwalanie (masą) z dodatkowego czujnika (ultradźwiękowego)
12	Plus po stacyjce – zacisk 15 instalacji samochodu
13	Masa po uzbrojeniu dla dodatkowe czujnika (ultradźwiękowego)
14	Sterowanie syreną alarmową (masą)
15	Wyprowadzenie zasilania dla dodatkowego czujnika i syrenki alarmowej
16	Plus zasilania – zacisk 30 instalacji samochodu
17	Kierunkowskaz
18	-
19	Sterowanie centralnym zamkniem – otwieranie – sygnał masy 500ms
20	-

Rysunek 12. Opis wyprowadzeń złącza

tego samego klucza. Klucz jest generowany z numeru seryjnego oraz kodu producenta. O ile numer seryjny może być bez trudu poznany – jest zapisany w pamięci EEPROM, ponadto jest jawnie przesyłany w niekodowanym słowie transmisji radiowej, numer producenta powinien być numerem unikalnym i tajnym. Jeśli zdecydowaliśmy się na samodzielne skompilowanie kodu należy zmodyfikować procedurę *LOAD_MKEY* znajdującą się w pliku decrypt.a51. Wpisujemy tam nasz własny kod producenta (**listing 1**).

W wypadku, gdy nie mamy chęci bądź możliwości skompilowania kodu, pozostaje edycja kodu maszynowego. Czynności tej dokonujemy dowolnym edytorem hexadecymalnym. Tablica symboli wygenerowana przez linker przy konsolidacji modułu określa adres procedury *LOAD_MKEY* na 0x0777. Pod tym adresem rozpoczynają instrukcje MOV wpisujące kolejne bajty kodu producenta do pamięci

Oczywiście w wypadku samodzielnego kompilowania konsolidator może przydzielić dla opisywanej procedury inny adres w pamięci. Przy użyciu tego samego numeru producenta, które zapisaliśmy w kodzie mikrokontrolera, należy wygenerować klucz, który zostanie zapisany w pamięci EEPROM enkodera HCS200. Oprócz numeru producenta do wygenerowania klucza potrzebny jest numer seryjny. Jest to unikalny numer enkodera. Do zaprogramowania pilota możemy użyć programatora opisanego w EP 1/2012. Program generujący klucz oraz obsługujący programator jest uruchamiany z linii poleceń a ilość parametrów została ograniczona do niezbędnego minimum (program nie daje możliwości parametryzacji danych konfiguracyjnych enkodera – stosuje takie jakie są potrzene w omawianym systemie). Argumentami są kolejno: nazwa wirtualnego portu szeregowego, 64-bitowy numer producenta i 28-bitowy numer seryjny:

```
C:\hcsprog>hcsprog.exe com8
41:4c:41:6d:72:61:6c:61 0:00:00:01
```

W przypadku, gdy chcemy zaprogramować układ innym narzędziem należy w danych konfiguracyjnych samodzielnie ustawić odpowiednie flagi (bitrate na 400 μs). Aby wstępnie sprawdzić działanie centralki oraz poprawność zaprogramowania mikrokontrolera podłączamy centralkę do zasilacza 12 V (pin 6 – masa, pin 16 – plus zasilania). Ponadto podłączamy diodę LED (anoda – pin 4, katodą do masy). Zwieranie styków ukrytego wyłącznika (pin 3 do masy) powinno powodować szybkie miganie diody LED. Świadczy to o poprawnej pracy części układów oraz o realizowaniu programu zapisanego w mikrokontrolerze. Do programowania pilotów niezbędne będzie jeszcze przygotowanie wyprowadzenia plusa pojawiającego się po przekręceniu stacyjki (pin 12; na razie z niczym nie zwieramy) oraz sygnału dźwiękowego. Zastępczo, zamiast syrenki można użyć buzzera 12 V (lub 5 V poprzez rezystor 220 Ω) włączonego pomiędzy plusem zasilania a pinem 14. Dokładne sprawdzenie działania obwodów centralki będzie prostsze do wykonania po zaprogramowaniu pilotów. Przechodzimy zatem do uruchomienia pilotów i toru radiowego.

Przy sprawdzaniu i strojeniu (wersja RLC) pilotów przydatnym przyrządem jest analizator widma ustawiony na częstotliwość 433,92 MHz. W wypadku pilota, w którym użyto rezonatora SAW, sprawa sprowadza się do weryfikacji na przyrządzie czy pilot nadaje na żądanej nośnej. Pilot z generatorem RLC wymaga zestrojenia. Do strojenia należy użyć stroika wykonanego z tworzywa sztucznego – metalowy wkrętak nie nadaje się do zestrojenia generatora. Stroikiem ustawiamy trymer C4 w ten sposób aby ustawić prążek na zadaną częstotliwość nośnej. Należy sprawdzić czy po usunięciu stroika z układu częstotliwość nośnej zbytnio nie zmieniła się. Gdy nie mamy do dyspozycji analizatora widma jakość transmisji można zweryfikować w centralce, na wyjściu toru radiowego. Należy użyć do tego celu oscyloskopu zwracając uwagę na fakt, że czas trwania pojedynczego elementu (nie bitu!) wynosi około 400 μs (dokumentacja przewiduje dosyć duży rozrzut, ponadto może być zaprogramowany czas 200 μs, jeśli układ HCS200 pracował w innym urządzeniu). Transmisja jednego bitu kodowanego przy użyciu PWM zajmuje wobec tego około 1,2 ms (trzy elementy bazowe). Przykładowy oscylogram przedstawiono na **rysunku 11**.

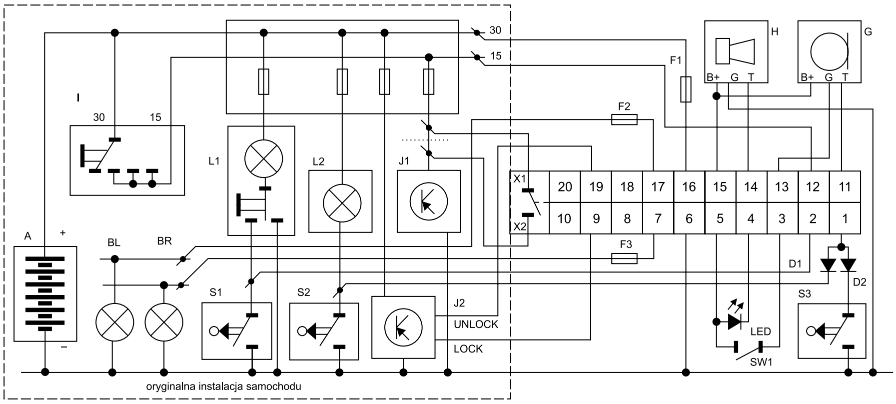
Skoro mamy już wstępnie uruchomioną centralkę oraz piloty możemy przystąpić do zestawienia tych elementów w całość. Normalnie procedura programowania pilotów wymaga autoryzacji wcześniej przypisanym do systemu pilotem. W przypadku nowego urządzenia, gdy w pamięci EEPROM nie ma zapisanych żadnych pilotów obowiązuje odmienna procedura opisana niżej. Wciskamy i trzymamy wciśnięty ukryty przycisk (pin 3 zwarty do masy przez około 10 s), aż do chwili potwierdzenia dźwiękiem syrenki. Dioda LED miga. W przeciągu 10 sekund 10-krotnie zwieramy wyprowadzony wcześniej przewód plusa po stacyjce do plusa zasilania (10 razy przekręcamy stacyjkę). Syrenka potwierdza zakończenie etapu dwukrotnym sygnałem dźwiękowym. Dioda LED miga 10-krotnie pokazując numer aktualnie programowanej opcji. Syrenka modulowanym dźwiękiem sygnalizuje gotowość do programowania. W przeciągu 30 s przypisujemy do centralki nowe piloty. Naciskamy w kilkusekundowych odstępach ten sam przycisk pilota kilkukrotnie. Każde naciśnięcie powinno być sygnalizowane syrenką. Dłuższy, modulowany dźwięk syrenki oznacza, że pilot został zapisany w pamięci. Taką samą procedurę kilkukrotnego naciskania przycisku stosujemy przy kolejnych pilotach do nauczenia. Centralka musi odkodować kolejne transmisje i potwierdzić, że pilot jest uprawniony – transmisja jest kodowana właściwym kluczem i kolejne wartości licznika przyrastają o jeden.

Jeżeli udało się zaprogramować piloty, można kontynuować uruchamianie centralki. Uzbrajamy alarm naciskając przycisk „1" pilota. Fakt ten powinien być zasygnalizowany syrenką.

Podczas oraz po uzbrojeniu syrenka nie powinna już wydawać sygnałów dźwiękowych. Sygnały dźwiękowe podczas uzbrajania oznaczają naruszoną strefę, co może sugerować problem z którymś z układów wejściowych. Należy zwrócić uwagę na rezystory R44 i R45 – nie zostały one ujęte na obwodzie drukowanym i można je dolutować (jeśli obwody drzwi i bagażnika mają lampkę to nie jest to konieczne – żarówki podciągną linie wejściowe do plusa). Dalsze czynności uruchomieniowe sprowadzają sie sprawdzenie pracy układów wejść i wyjść. Mogą się one odbyć po dołączeniu centralki do instalacji samochodu albo poprzez symulowanie tego podłączenia.

Podłączenie do instalacji samochodowej

Do podłączenia centralki z instalacją samochodu służy wiązka przewodów, zawierająca również gniazda bezpieczników samochodowych (jeden główny i dwa bezpieczniki kierunkowskazów). Wiązka jest przyłączana do centralki alarmu za pomocą 20-pinowego złącza. Wyjątkiem są przewody odcięcia zapłonu. Nie zostały one ujęte w złączu głównym ze względu na duży prąd, który może pojawić się w obwodzie. Są one przyłączane do instalacji za pomocą konektorów samochodowych. Na **rysunku 12** przedstawiono numerację doprowadzeń wtyku złącza (widok od strony przewodów).



A - akumulator
I - wyłącznik zapłonu
BL - lewy kierunkowskaz
BR - prawy kierunkowskaz
L1 - lampka oświetlenia wnętrza
L2 - lampka bagażnika
S1 - wyłącznik dzwiowy
S2 - wyłącznik lampki bagażnika
J1 - sterownik silnika
J2 - sterownik centralnego zamka
F1 - bezpicznik główny alarmu 15A
F2 - bezpiecznik kierunkowskazu 7,5A
F3 - bezpiecznik kierunkowskazu 7,5A
H - syrena alarmowa
G - ultradzwiękowy czujnik ruchu
S3 - wyłącznik maski silnika
D1 - dioda 1N4148
D2 - dioda 1N4148
LED - dioda LED sygnalizująca stan alarmu
SW1 - ukryty przycisk

Rysunek 13. Schemat dołączenia centralki

Tabela 1. Opis funkcji sterowania centralką

Funkcja	Przycisk	Opis
Pełne uzbrajanie alarmu	1	Pełne uzbrojenie alarmu – wszystkie strefy ochrony są aktywne po 40 sek. Jeśli podczas uzbrajania, któraś ze stref ochrony jest naruszona zostaje ona trwale odłączona (czujniki są sprawdzane przez ostatnie 5 sek. uzbrajania). Kod odłączonej strefy jest sygnalizowany syreną.
Niepełne uzbrajanie alarmu	2	Uzbrajanie niepełne (z odłączoną strefą „4" - czujnik ruchu) . Przy uzbrajaniu sprawdzane są pozostałe strefy podobnie jak przy pełnym uzbrajaniu.
Rozbrajanie alarmu	1	Rozbrojenie alarmu w przypadku gdy nie jest aktualnie wyzwolony. Jeśli wcześniej, podczas czuwania była naruszona któraś ze stref ochrony jest to sygnalizowane diodą LED (kod strefy/5 sek przerwy). W przypadku naruszenia kilku stref ich kody są przedstawiane po kolei. Pamięć alarmów jest kasowana po przekręceniu stacyjki.
Wyłączenie trwającego alarmu	1	Ma miejsce gdy wyzwolony został alarm. Powoduje wyłączenie trwającego alarmu. Centralka pozostaje w stanie uzbrojonym.
Szukanie auta na parkingu	2	Powoduje zapalenie świateł kierunkowskazów na 5sek. Funkcja jest aktywna tylko w przypadku gdy alarm jest uzbrojony

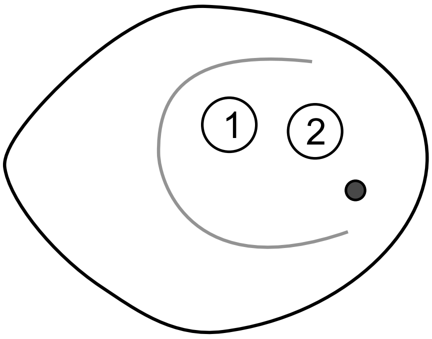
Tabela 2. Wykaz funkcji dodatkowych

Nr funkcji	Nazwa funkcji dodatkowej	Opis działania
1	Ciche uzbrajanie i rozbrajanie	Alarm nie potwierdza komend uzbrajania i rozbrajania syreną.
2	Autouzbrajanie	Alarm samoczynnie się uzbraja w przypadku gdy została wydana komenda rozbrojenia, a nie zostały otwarte dzwi (przez 30 sek.)
3	Domykanie szyb	W niektórych pojazdach poprzez wydłużenie (do 12 sek.) impulsu „zamknij" można sterować zamykaniem szyb.
4*	Immobilizer	Odcięcie zapłonu zwalnia się po naciśnięciu ukrytego wyłącznika
5	Funkcja antynapadowa	Włącza funkcje antynapadową opisaną dalej.
6	Zamykanie w trakcie jazdy	Włączenie i wyłączenie zapłonu powoduje odpowiednie wygenerowanie sygnałów dla centralnego zamka: „zamknij" i „otwórz".
7	Autouzbrojenie po wyłączeniu zapłonu	Po wyłączeniu zapłonu następuje samoczynne uzbrojenie.

* funkcja nie jest realizowana (ale jest w kodzie źródłowym)

Tabela 3. Opis stref i przypisane do nich kody

Kod strefy	Obszar ochrony
1	Załączenie zapłonu (zacisk 15 instalacji samochodu)
2	Czujniki dzwiowe
3	Czujniki maski i bagażnika
4	Czujnik ruchu (ultradzwiękowy)



Rysunek 14. Przyciski na pilocie

Schemat podłączenia centralki do instalacji samochodu przedstawiony na **rysunku 13**. Na schemacie użyto oznaczeń obwodów powszechnie stosowane w instalacjach samochodowych:

- Zacisk 30 – plus akumulatora.
- Zacisk 15 – plus po przekręceniu stacyjki. Ważne aby napięcie na tym zacisku nie zanikało w trakcie pracy rozrusznika..
- Zacisk 31 – masa.

Jako syrenkę **H** można użyć sygnalizatora dowolnego typu dostępnego w sprzedaży, przeznaczonego dla instalacji 12 V i załączanego masą. Najlepiej aby była to syrena z własnym zasilaniem (odłączenia zasilania powoduje, że syrenka nadal działa zasilana z wewnętrznego akumulatorka). Podobnie wygląda sytuacja odnośnie czujnika ruchu **G** (dowolny 12 V, reagujący na naruszenie zwieraniem obwodu do masy).

Obsługa i programowanie funkcji

Podstawowe funkcje alarmu realizowane są za pomocą pilota. Rozmieszczenie przycisków na pilocie przedstawione zostało na **rysunku 14**. W **tabeli 1** zamieszczono opis funkcji służących do sterowania centralką.

Funkcje dodatkowe

Standardowe zachowanie się systemu można modyfikować poprzez włączenie funkcji dodatkowych. Funkcje te są domyślnie wyłączone i wymagają ustawienia. Programowanie opisanych ustawień odbywa się w zamontowanym urządzeniu bez konieczności dostępu do centralki. W **tabeli 2** zestawione zostały funkcje dodatkowe. Programowanie funkcji dodatkowych możliwe jest dopiero po przejściu do trybu serwisowego.

Tryb serwisowy

Jest to specjalny tryb pracy alarmu, w którym wyłączone są funkcje alarmowe i antynapadowe centralki. Realizowane jest jedynie sterowanie centralnym zamkiem. Ten tryb pracy jest przydatny w przypadku konieczności oddania samochodu do naprawy. Auto nie stwarza wtedy niepotrzebnych problemów, związanych ze znajomością działania alarmu i antynapadu, pracownikom warsztatu. Ponadto nie musimy zdradzać osobom trzecim umiejscowienia ukrytego przycisku. Programowanie funkcji dodatkowych oraz pilotów możliwe jest wyłącznie z poziomu trybu serwisowego. Stan serwisowy jest sygnalizowany świecącą diodą LED przy włączonym zapłonie.

Włączenie trybu serwisowego

Należy zwrócić uwagę na fakt, że przejście do trybu programowania oraz wyjście z trybu serwisowego jest możliwe tylku przy użyciu tego samego pilota, który został użyty do aktywacji opisywanego trybu. Aby przełączyć alarm w tryb serwisowy należy włączyć zapłon i trzymać wciśnięty ukryty przycisk do chwili potwierdzenia sygnałem akustycznym (około 10 s). Następnie należy wcisnąć przycisk „1" pilota, co zostanie potwierdzone kolejnym sygnałem akustycznym. Alarm znajduje się w trybie serwisowym (dioda LED jest zapalona)

Programowanie funkcji dodatkowych

Jest możliwe wyłącznie z trybu serwisowego. Procedura wygląda następująco: przy wyłączonym zapłonie trzymamy wciśnięty ukryty przycisk do czasu potwierdzenia sygnałem akustycznym (około 10 sek.). Następnie naciskamy przycisk „1" pilota (tego samego, który został użyty do aktywacji stanu serwisowego). Dioda LED miga – można wprowadzić kod funkcji poprzez włączanie zapłonu (mamy na to 10 s). Koniec wprowadzania kodu sygnalizowany jest dwukrotnym sygnałem akustycznym. Modulowany dźwięk syrenki sygnalizuje, że możemy ustawić stan aktualnej funkcji. Ukrytym przyciskiem zmieniamy stan opcji. Dioda LED pokazuje czy funkcja będzie włączona (LED świeci – włączona/nie świeci – wyłączona). Gdy ustawimy oczekiwany stan możemy przejść do programowania kolejnej opcji poprzez chwilowe włączenie zapłonu (potwierdzone sygnałem akustycznym). Gdy zakończymy programowanie wszystkich interesujących nas opcji nie przekręcamy stacyjki (kod 0 – wyjście z trybu programowania).

Przykładowo, chcemy włączyć funkcje nr 1 i 3:

- Włączamy zapłon, trzymamy ukryty przycisk, 1 dźwięk syrenki, puszczamy przycisk, wciskamy przycisk pilota, 2 dźwięki syrenki, dioda LED świeci się.
- Wyłączamy zapłon, dioda LED gaśnie, trzymamy ukryty przycisk, 1 dźwięk syrenki, puszczamy przycisk, wciskamy przycisk pilota.
- 1 dzwięk syrenki, LED miga, 1 raz włączamy na chwilę zapłon, 2 dzwięki syrenki, LED zapala sie 1 raz, modulowany dzwięk syrenki.
- Dioda LED zgaszona, wciskamy przycisk – LED zapala się, 1 raz włączamy zapłon.
- 1 dźwięk syrenki, LED miga, 3 razy włączamy na chwilę zapłon, 2 dzwięki syrenki, LED zapala sie 3 razy, modulowany dźwięk syrenki.
- LED zgaszony, wciskamy przycisk – LED zapala się, 1 raz włączamy zapłon.
- 1 dźwięk syrenki, LED miga, nie włączamy zapłonu, 2 dźwięki syrenki, LED nie zapala sie 3, modulowany dźwięk syrenki.
- Włączamy zapłon, LED pali się, trzymamy ukryty przycisk, 1 dźwięk syrenki, puszczamy przycisk, wciskamy przycisk pilota, 2 dźwięki syrenki, LED gaśnie.

Funkcja antynapadowa

Funkcja ma na celu zabezpieczenie pojazdu, w przypadku przejęcia przez inną, niż właściciel, osobę. Działanie funkcji polega na konieczności potwierdzenia ukrytym przyciskiem zdarzeń: włączenia zapłonu i otwarcia drzwi. W przypadku braku potwierdzenia system realizuje program antynapadowy. Przez 30 s od uruchomienia samochodu lub otwarcia drzwi system nie ujawnia w żaden sposób faktu wyzwolenia funkcji antynapadowej (jeśli pojazd został przejęty siłą, to jest czas potrzebny do bezpiecznego oddalenia się kierowcy od napastników). Po tym czasie następują kolejne krótkie, emitowane przez syrenę, sygnały ostrzegawcze. Ostatecznie zostaje włączona na stałe sygnalizacja dźwiękowa i świetlna.

Strefy ochrony

Ochrona została podzielona na niezależne strefy. Podział taki pozwala na identyfikację źródła alarmu oraz na odrębne traktowanie obszarów ochrony. Opisane rozwiązanie jest praktyczne bowiem pozwala na:

- Poinformowanie użytkownika z której strefy został wyzwolony alarm.
- Odłączenie strefy, na przykład w sytuacji gdy w samochodzie zostały uchylone szyby i/lub pozostawiliśmy w samochodzie psa lub inne zwierzę.
- W przypadku awarii czujnika jednej ze stref, odłączenie wyłącznie wadliwej strefy.
- Informacja o wyzwoleniu alarmu w danej strefie podczas uzbrajania alarmu.

W **tabeli 3** zamieszczono opis stref oraz przypisane do nich kody.

Jakub Kietliński
jakub.kietlinski@gmail.com

Bibliografia:
Nota katalogowa HCS200 (http://ww1.microchip.com/downloads/en/devicedoc/40138c.pdf)
Nota AN744 (http://ww1.microchip.com/downloads/en/AppNotes/00744a.pdf)