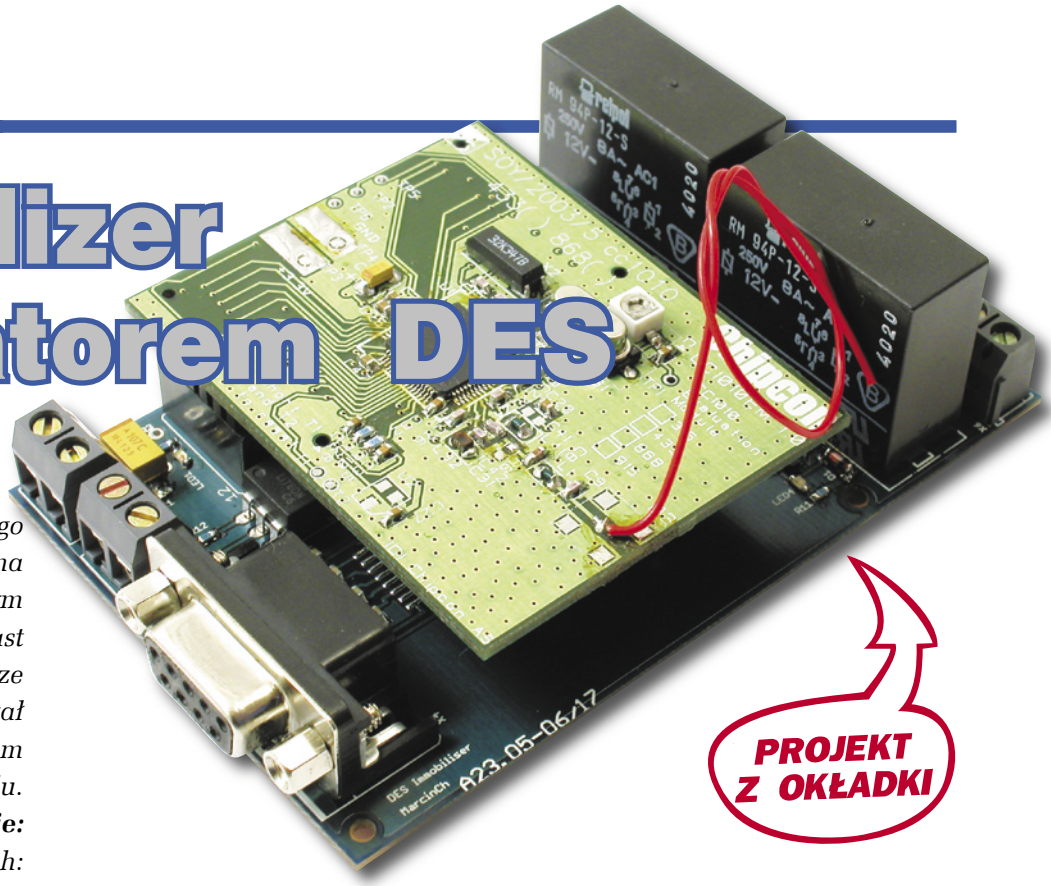
Immobilizer z szyfratorem DES



Założeniem przedstawionego projektu była ochrona samochodu przed niepowołanym uruchomieniem, natomiast inspiracją historia jednego ze znajomych autora, który stał się szczęśliwym posiadaczem niebanalnego pojazdu.

Rekomendacje: *urządzenie o niebanalnych: konstrukcji i pomyśle. Jest to pierwsze prezentowane na łamach EP praktyczne zastosowanie sprzętowego szyfratora DES – warto dowiedzieć się jak działają i gdzie można kupić tak wyrafinowane układy!*

Dodatkowe materiały do artykułu publikujemy na CD-EP oraz www.ep.com.pl

PODSTAWOWE PARAMETRY

- Płytka o wymiarach: 100 x 64 mm
- Zasilanie płytki jednostki centralnej: 12 VDC (instalacja samochodowa)
- Zasilanie karty transponderowej: 3 VDC (bateria CR2477 – 3 V/1000 mAh)
- Czas pracy karty na jednej baterii: ok. 2 miesięcy
- Pasmo pracy: 868 MHz
- Moc sygnału: +4 dBm
- Modulacja: FSK
- Kodowanie: Manchester
- Prędkość transmisji: 2400 bd
- Czułość: –103 dB
- Sposób zabezpieczenia: blokada dopływu paliwa

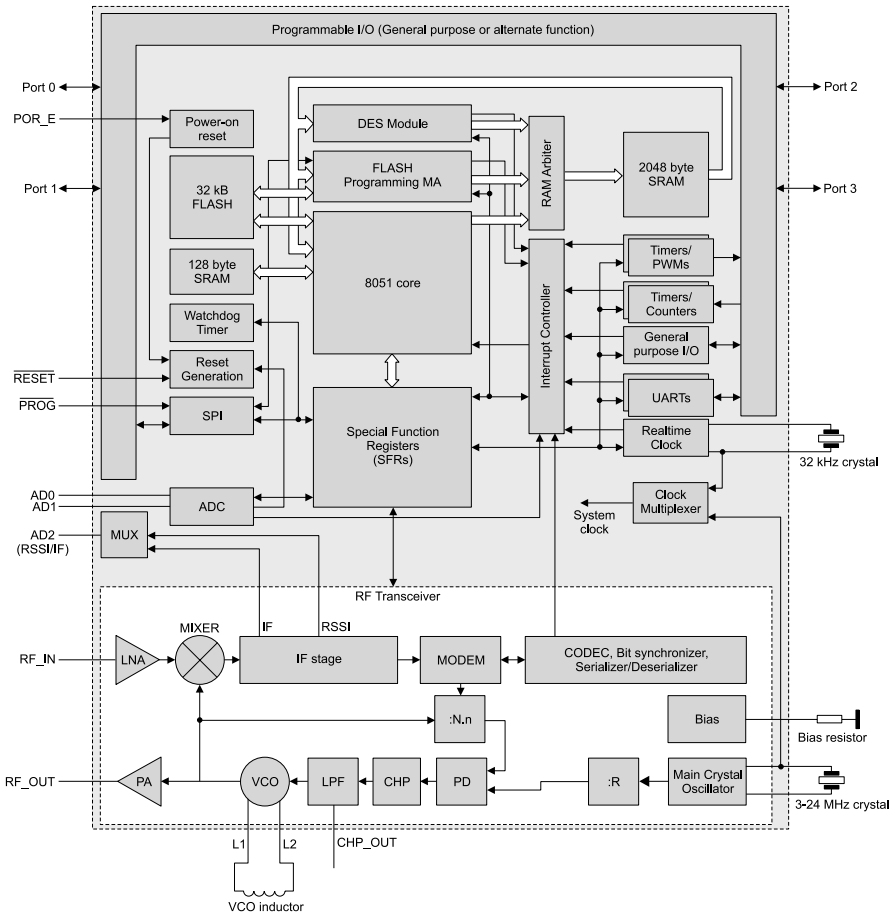
Niebanalność polegała na tym, iż towarzystwo ubezpieczeniowe nie chciało wydać polisy na ów pojazd bez zamontowania w nim dodatkowo (oprócz standardowego alarmu) systemu trackingowego. Jako dodatek do owego systemu dołączona została karta transponderowa, która przez cały czas użytkowania samochodu musi pozostać w jego wnętrzu, stanowiąc jednoczenie zabezpieczenie przed ucieczką samochodem po uprzednim, fizycznym usunięciu właściciela z jego wnętrza. Po zgrubnych oględzinach karty okazało się, że jest ona zasilana bateryjnie i posiada nadajnik radiowy. Usunięcie karty z wnętrza pojazdu powoduje zerwanie komunikacji karty z jednostką w samochodzie i tym samym powiadomienie (GPRS) patrolu interwencyjnego firmy zapewniającej obsługę całego systemu. Skomplikowane i kosztowne...

W artykule przedstawiono projekt immobilizera samochodowego z aktywną kartą transponderową. Funkcja układu sprowadza się do blokady dopływu paliwa do silnika samochodu w przypadku, gdy niepowołana osoba nie dysponuje kartą transponderową. Urządzenie działa niejako w tle, nie absorbując uwagi użytkownika. Duży nacisk położono na realizację bateryjnego zasilania karty transponderowej (tak aby wymiana baterii nie stała się głównym zajęciem kierowcy). Od pewnego czasu na rynku krajowym dostępny jest dość interesujący i niedrogi układ, idealnie nadający się do celów prezentowanego projektu. Jest to CC1010 produkowany przez firmę Chipcon.

Opis układu

CC1010 jest scalonym transceiverem pracującym w paśmie ISM, zintegrowanym z mikrokontrolerem 8051. Hierarchia (transceiver z mikrokontrolerem) nie jest tu przypadkowa, ponieważ bloki układu w nim zawarte zostały dobrane wyłącznie z myślą o transmisjach radiowych. Na **rys. 1** przedstawiono schemat blokowy układu CC1010, natomiast w **tab. 1** zestawiono jego najważniejsze parametry. Oprócz standardowych elementów jak pamięć programu typu Flash czy przetwornik A/C, układ CC1010 ma wbudowane dwa interfejsy UART, zegar czasu rzeczywistego (po dołączeniu zewnętrznego rezonatora 32,768 kHz), interfejs SPI. Prawdziwym rarytasem w prezentowanym układzie jest programowo konfigurowalny transceiver pozwalający na pracę w jednym z wybranych pasm ISM (315 MHz, 433 MHz, 868 MHz i 915 MHz). W każdym z pasm mamy do wyboru kilka kanałów pracy transceivera oraz możliwość programowej kontroli poziomu mocy emitowanego sygnału. Całości dopełnia sprzętowy blok kryptograficzny (DES – *data encryption standard*) pozwalający na szyfrowanie i deszyfrowanie bloków po 256 bajtów danych za pomocą 56 bitowego klucza. Dodatkowo blok ten może pracować w tzw. trybie Triple – DES (dedykowanym do

Tab. 1. Najważniejsze parametry układu CC1010	
Parametry transceivera	**Parametry rdzenia 8051**
Programowana częstotliwość pracy (300 do 1000 MHz)	Zoptymalizowany rdzeń 8051. 2,5 raza wydajniejszy niż standardowy 8051
Duża czułość odbiornika (typ. –107 dBm przy 2,4 kbd)	Tryb bezczynności (idle) i czuwania (sleep)
Programowalny poziom mocy wyjściowej (–20 do +10 dBm)	32 kB nieulotnej pamięci Flash
Niski pobór mocy (9,1 mA w trybie odbioru)	2 k + 128 bajtów wewnętrznej pamięci SRAM
Modulacja FSK (max. 76,8 kbd)	Zasilanie 2,7…3,6 V
Wyjście RSSI (poziom sygnały wejściowego)	Częstotliwość taktowania 3…24 MHz

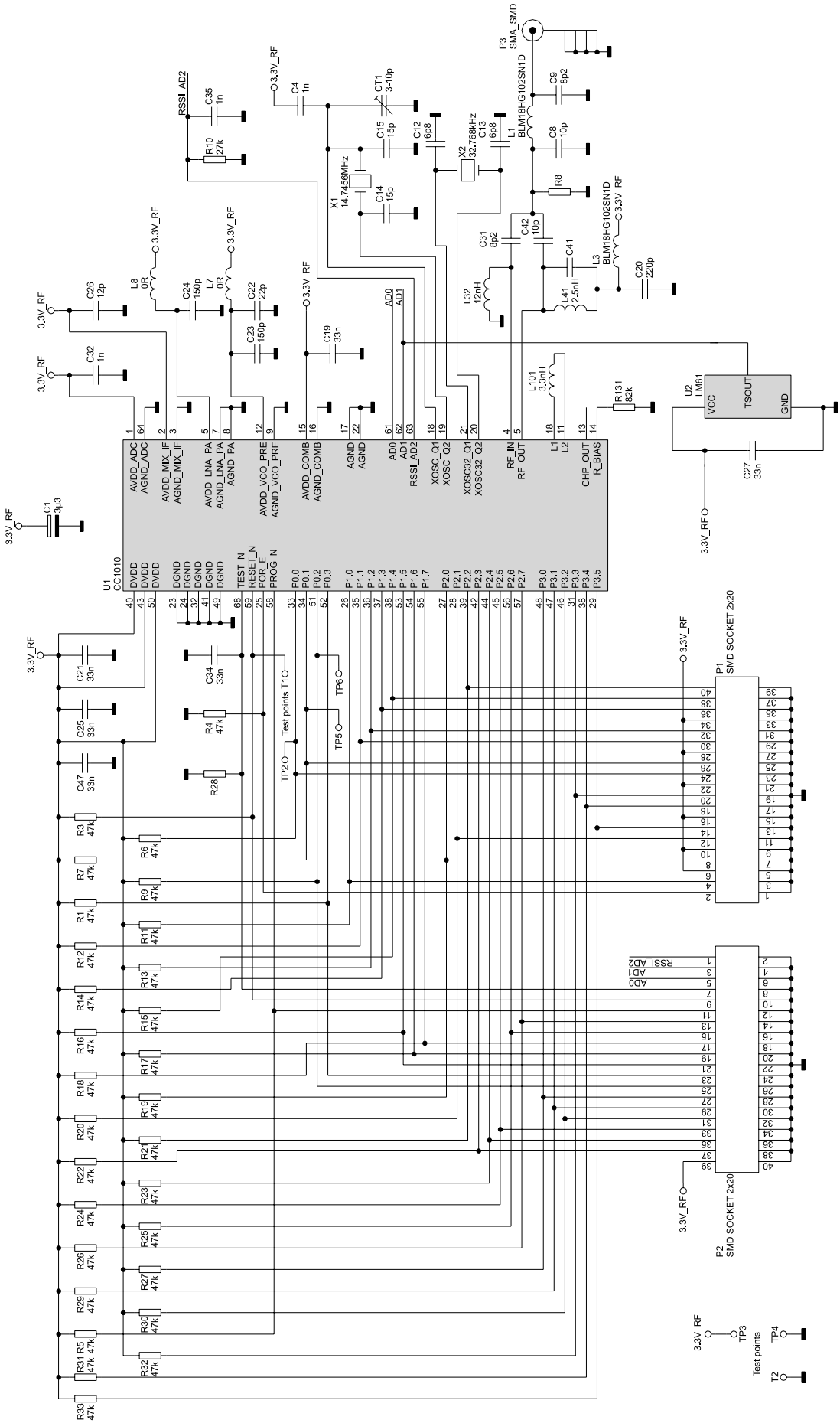


Rys. 1. Schemat blokowy układu CC1010

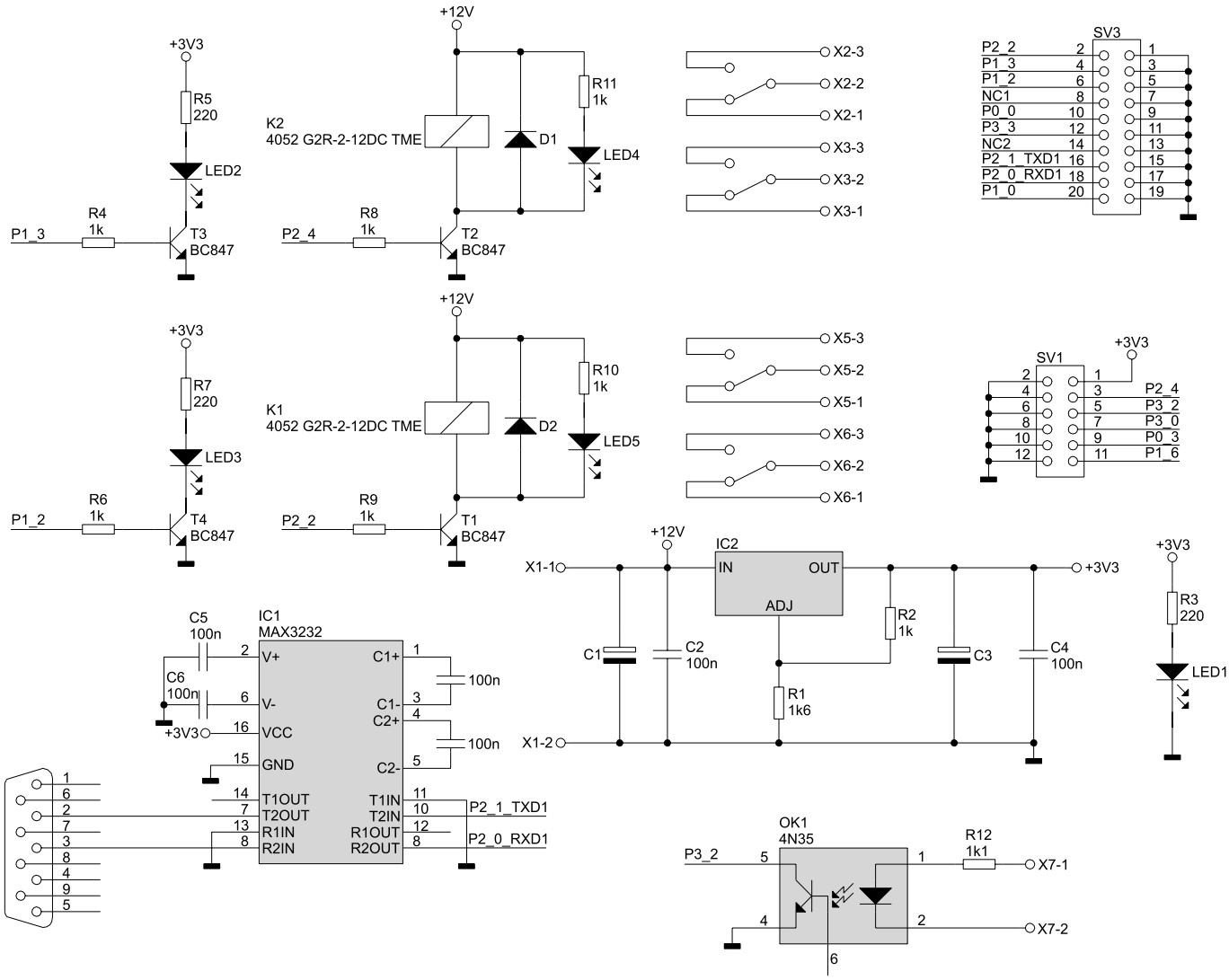
systemów o szczególnych wymogach bezpieczeństwa). Transceiver jest wyposażony w wyjście napięciowe poziomu odebranego sygnału (RSSI – *received signal strength indication*), które może być bezpośrednio podane na wejście wewnętrznego przetwornika A/C. Ciekawostką jest wyposażenie układu w generator losowego bitu, przy czym nie jest to blok pseudolosowy. Wartość bitu uzyskiwana jest poprzez wzmocnienie poziomu szumu w torze odbiorczym transceivera, a następnie podawanie takiego sygnału na blok decyzyjny. Sam CC1010 do poprawnej pracy wymaga niewielu elementów zewnętrznych. Większość z nich jest niezbędna do poprawnej pracy części radiowej układu. Pozornie, jak przekonał się autor, sprawa projektu płytki drukowanej pod opisywany układ wygląda prosto. Jednak po dokładnym przestudiowaniu dokumentacji dostarczonej przez Chipcona okazuje się, że do poprawnej pracy w paśmie 868 MHz (taką częstotliwość pracy wybrano do projektu) niezbędne jest wykonanie 4–warstwowej płytki drukowanej, co okazało się zbyt kosztownym zadaniem. Z pomocą przybył krajowy dystrybutor firmy Chipcon, oferujący w swoim asortymencie 4–warstwowe płytki drukowane wykonane według *reference design* dostarczonego wraz z dokumentacją układu. Płytki dostarczane są bez elementów, które należy skompletować we własnym zakresie na podstawie dołączonego do dokumentacji wykazu elementów. Opisywana płytka ma wymiar 5x6 cm i mieści na sobie pola lutownicze do montażu samego CC1010, elementów toru radiowego, dwóch oscylatorów kwarcowych oraz specjalnych konektorów SMD lutowanych od spodu. Kompletny schemat modułu przedstawiono na **rys. 2**. W celu realizacji karty transponderowej użyta została jedna taka płytka, którą wyposażono w gniazdo płaskiej baterii litowej 3 V. Jedynym poważnym mankamentem CC1010 jest to, że narzędzia oficjalnie wspierane przez Chipcona nie są dostępne bezpłatnie. Dostarczone do układu biblioteki HAL (*Hardware Abstraction Library*) i CUL (*Chipcon Utility Library*) zostały stworzone z myślą o środowisku Keil uVision, którego ewaluacyjna wersja posiada ograniczenie rozmiaru kodu wynikowego do 2 kB (co uniemożliwia swobodne korzystanie z układu). Z pomocą jednak przyszedł kompilator SDCC, który nie jest oficjalnie wspierany przez Chipcon, to jednak bezproblemowo radzi sobie z kompilacją programów pisanych z użyciem obu wymienionych bibliotek.

Karta transponderowa

Jak wspomniano wcześniej, budowa karty transponderowej opiera się jedynie na module z układem CC1010 z dołączoną baterią. Nieco więcej wysiłku wymagała część programowa. Problemem był pobór prądu podczas pracy układu. Ponieważ z założenia karta po zbliżeniu do samochodu powinna odebrać ramkę danych nadawaną przez część immobilizera umieszczoną w samochodzie, a następnie po jej odszyfrowaniu, modyfikacji i ponownym zaszyfrowaniu odesłać odpowiedź, to jej odbiornik powinien być gotowy na przyjęcie transmisji w każdej chwili. Oznaczałoby to, że pobór prądu przez kartę wynosiłby około 20 mA, co powodowałby bardzo szybkie zużycie baterii. Aby rozwiązać ten problem, zastosowano tzw. *polling* odbiornika radiowego. Na początku pracy transponder (przypomnijmy wyposażony w dwa generatory kwarcowe) uruchamia drugi generator o częstotliwości pracy 32,768 kHz, po czym przełącza



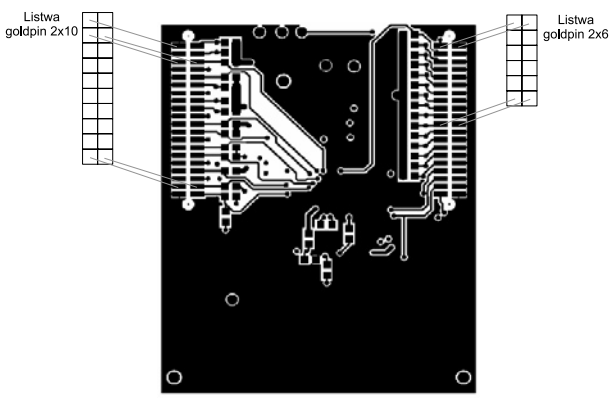
Rys. 2. Schemat elektryczny modułu z *reference design* dostarczonego przez Chipcon



Rys. 3. Schemat elektryczny jednostki umieszczonej w samochodzie

układ taktowania rdzenia na ten właśnie wolny oscylator uprzednio uaktywniając zegar czasu rzeczywistego, tak aby generował przerwanie co 2 s. Pobór prądu w tym momencie wynosi 1,3 mA i niemożliwe jest korzystanie z transceivera. Kolejnym krokiem jest przejście rdzenia mikrokontrolera w tryb bezczynności (*idle*), co powoduje kolejny spadek poboru prądu do 29,4 µA. Mikrokontroler pozostanie w trybie *idle* do momentu, kiedy zegar RT nie wygeneruje sygnału przerwania, czyli przez dwie sekundy. Po tej czynności układ przechodzi ponownie do trybu aktywnego i przełącza źródło zegara na szybki oscylator (14,7456 MHz). Następuje uruchomienie toru odbiorczego transpondera i rozpoczyna się oczekiwanie na nadejście ramki. Czas oczekiwania wynosi 20 ms. Kod odpowiedzialny za tę część programu przedstawiono na **list. 1**.

Jeśli nie było transmisji, układ po 20 ms oczekiwania przechodzi ponownie w tryb bezczynności i jest taktowany sygnałem zegarowym o małej częstotliwości. Jeżeli ramka danych została poprawnie odebrana, następuje analiza nagłówka ramki. Są dwa możliwe przypadki: ramka konfiguracyjna i ramka kontrolna. Ramka konfiguracyjna jest to ramka niosąca informację o 7–bajtowym kluczu, jaki ma być używany do dekodowania ramek standardowych. Klucz wyłuskany z ramki zostaje zapisany w obszarze pamięci flash pod stosownym adresem tak, aby po wyjęciu baterii wartość klucza została zachowana. Służy do tego



Rys. 4. Sposób montażu goldpinów na module CC1010 (widok modułu od strony złącza)

Pasma ISM

ISM – *Industrial, Scientific, Medical* – są to nielicencjonowane pasma radiowe, przeznaczone do transmisji z małymi mocami na niewielkie odległości. Najpopularniejszym pasmem ISM jest 2,4 GHz, wykorzystywane m.in. przez urządzenia Bluetooth oraz WiFi. Równie popularnym pasmem dopuszczonym do użytkowania w Polsce jest 868 MHz, w którym pracuje immobilizer opisany w artykule.

Rys. 5. Widok informacji powitalnej immobilizera z bieżącą wartością klucza DES

funkcja z biblioteki HAL o nazwie *halFlashWritePage()*. Po sprawdzeniu sumy kontrolnej (dokonuje tego funkcja *halRFReceivePacket()*) następuje zapis nowej wartości klucza do pamięci Flash.

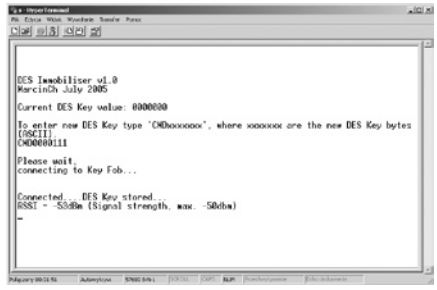
W drugim przypadku, gdy odebrana została ramka kontrolna (domyślna ramka wysyłana przez jednostkę w samochodzie), następuje jej deszyfracja za pomocą zapisanego klucza. Deszyfrowane dane zostają następnie zmodyfikowane (zwiększenie wartości bajtów o 1), po czym ponownie zostają poddane szyfrowaniu tym samym kluczem. Następuje włączenie toru nadawczego transpondera i odesłanie tak zmodyfikowanej paczki danych do jednostki w samochodzie (**list. 2**).

Jest to kompletna sekwencja pracy transpondera. Średni pobór prądu tak pracującego układu wynosi 0,77 mA, co pozwoli na pracę na pojedynczym ogniwie CR2477 (3 V/1000 mAh) około 2 miesięcy bez konieczności wymiany, co nie jest może wynikiem rewelacyjnym, ale zdaniem autora akceptowalnym.

Jednostka centralna

Jednostka umieszczona w samochodzie została zbudowana w oparciu o identyczny moduł jak karta transponderowa, jednak osadzona została na płytce drukowanej zawierającej blok zasilania, dwa przekaźniki (odcięcie dopływu paliwa oraz sygnalizacja obecności transpondera) oraz wejście sygnału włączenia zapłonu. Dodatkowo na płytce znajduje się konwerter poziomów MAX3232, pozwalający na podłączenie komputera przy nadawaniu klucza przez użytkownika do jednostki centralnej i karty transponderowej. Schemat elektryczny jednostki centralnej przedstawiono na **rys. 3**.

Algorytm jej działania jest dość prosty. Po prawidłowej konfiguracji, a więc po nadaniu klucza jednostce centralnej oraz karcie transponderowej (odbywa się to za pośrednictwem terminala), jednostka wysyła w pętli zaszyfrowaną sekwencję 10 bajtów do karty transponderowej. Ramka zostaje nadana z bardzo długą preambułą (255 bajtów), co zwiększa szansę odbioru ramki przez kartę. Jeśli nie uzyskuje odpowiedzi (karta poza zasięgiem sygnału), jednostka nie podejmuje żadnej akcji (przekaźnik K1 załączony, przekaźnik K2 wyłączony). W przypadku, gdy do jednostki centralnej dociera odpowiedź, następuje deszyfracja informacji i porównanie jej z wiadomością nadaną. Jeśli porównanie wypadło pomyślnie, przekaźnik K2 zostaje załączony na 20 s, natomiast jednostka centralna sprawdza, czy załączony jest zapłon w samochodzie (co oznacza chęć uruchomienia silnika) i jeśli jest tak faktycznie, wówczas wyłączony zostaje przekaźnik K1 (odpowiedzialny



Rys. 6. Nowa wartość klucza (0000111) zapisana do transpondera (Key Fob)

WYKAZ ELEMENTÓW

Rezystory

R1: 1,6 kΩ 0603
R2, R4, R6, R8...R11: 1 kΩ 0603
R3, R5: 220 Ω 0603
R12: 1,1 kΩ

Kondensatory

C1, C3: 100 µF/16 V SMD D
C2, C4...C8: 100 nF 0603

Półprzewodniki

LED1...LED5: SMD 0603
OK1: (transoptor) 4N35 DIP6
D1, D2: BAS81 SOD80
IC1: MAX3232 SO16
IC2: LM317L
T1...T4: BC847

Inne

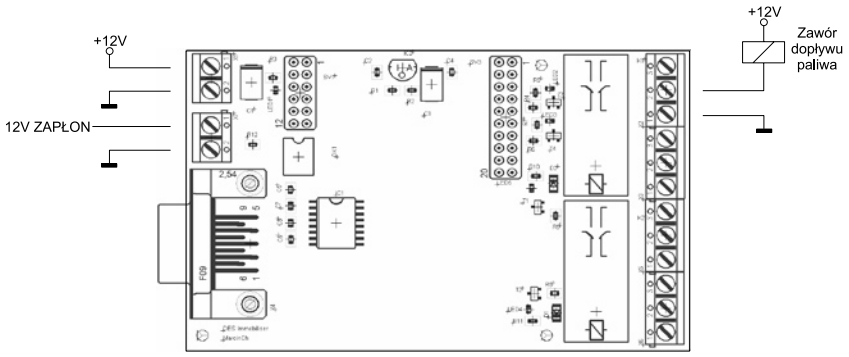
K1, K2: Przekaźnik, G2R-2-12DC /12 V
SV1: Gniazdo goldpin – 2x6
SV2: Gniazdo goldpin – 2x10
X1, X7: AK500/2
X2, X3, X5, X6: AK500/3
X4: DB9 żeńskie

List. 1. Sekwencja przełączania pomiędzy dwoma rodzajami sygnału taktującego

```
//Wyłączenie transceivera
RFMAIN=0xF8;

//Przełączenie źródła sygnału taktującego na oscylator 32kHz
MAIN_CLOCK_SET_SOURCE(CLOCK_X32);
//Wyłączenie oscylatora 14MHz
XOSC_ENABLE(FALSE);
//Wejście w tryb bezczynności
ENTER_IDLE_MODE();
//Od tej chwili CC1010 może być przywrócony do
//normalnej pracy przez reset bądź przerwanie
//RTC generuje przerwanie po 2 sek.
//.....................................................
//Włączenie oscylatora 14MHz
XOSC_ENABLE(TRUE);
//moment oczekiwania na stabilizacje pracy oscylatora
//CC1010 ciągle pracuje na wolnym sygnale zaegarowym zatem opóźnienie
//w postaci jednej iteracji pętli jest wystarczające
for(i = 1; i > 0; i--);

//Przełączenie rdzenia na szybki sygnał zegarowy
MAIN_CLOCK_SET_SOURCE(CLOCK_XOSC);
//Kalibracja toru RX
halRFCalib(&RF_SETTINGS, &RF_CALDATA);
//włączenie odbiornika i oczekiwanie przez 20ms na nadejście ramki
halRFSetRxTxOff(RF_RX, &RF_SETTINGS, &RF_CALDATA);
status=halRFReceivePacket(200, rfdata, 10, 0, CC1010EB_CLKFREQ);
```

List. 2. Sekwencja obsługi ramki wysłanej z samochodu

```
//Przygotowanie buforów z danymi do deszyfracji
memcpy(ramBuf, rfdata, DATA_LENGTH);
//deszyfracja kluczem pojedynczym
halDES(DES_SINGLE_DES | DES_DECRYPT | DES_OFB_MODE, ramBuf, keyBuf, DATA_LENGTH);
//modyfikacja zawartości ramki
for(i=0; i<10; i++)
++ramBuf[i];
//ponowne szyfrowanie tym samym kluczem
halDES(DES_SINGLE_DES | DES_ENCRYPT | DES_OFB_MODE, ramBuf, keyBuf, DATA_LENGTH);
memcpy(rfdata, ramBuf, DATA_LENGTH);

//Kalibracja
halRFCalib(&RF_SETTINGS, &RF_CALDATA);
//Włączenie nadajniki I odesłanie ramki do jednostki w samochodzie
halRFSetRxTxOff(RF_TX, &RF_SETTINGS, &RF_CALDATA);
halRFSendPacket(preamble_length, rfdata, 10);
```



Rys. 7. Przykładowy sposób dołączenia układu do instalacji elektrycznej samochodu

za dopływ paliwa). W tym momencie układ znajduje się w stanie rozbrojenia (sygnalizowanym miganiem diody LED3) i pozostaje w nim do momentu wyłączenia zapłonu.

Częstotliwość pracy nadajników i odbiorników obu układów wynosi 868,277 MHz. Sygnały nadawane są z mocą +4 dBm, z modulacją FSK oraz kodowaniem Manchester. Czułość odbiorników przy zastosowanej prędkości transmisji (2,4 kbd) wynosi –103 dBm.

Montaż i uruchomienie

Przede wszystkim należy dysponować dwoma zmontowanymi modułami CC1010. Pomimo, iż układ produkowany jest w obudowie TQFP, da się go wlutować w warunkach domowych (przy odrobinie praktyki w montażu SMD). Pozostałe elementy modułu są w większości w rozmiarze 0603, co wymaga nieco zręczności i dobrego wzroku. W miejsce przeznaczone na montaż złącza antenowego SMA należy przylutować odcinek przewodu o długości kilkunastu centymetrów. Gniazdo baterii można zamontować w sposób przedstawiony na zdjęciu modelu. Przed dalszym montażem należy zapisać odpowiednie programy do pamięci flash obu modułów. W tym celu należy posłużyć się programatorem, którego schemat umieszczony jest w dokumentacji znajdującej się pod adresem: *http://www.chipcon.com/files/CC1010EB_Reference_Design_3_0.zip*.

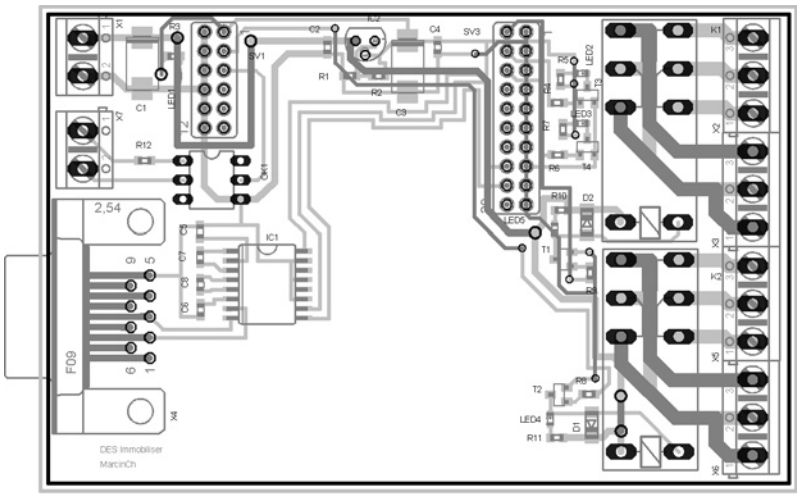
Natomiast program do obsługi programatora można pobrać z *http://www.chipcon.com/files/CC1010_Incircuit_FLASH_programmer_1_3.zip*. Obydwa programy udostępnimy także na naszej stronie WWW w dziale *Download* oraz na CD–EP11/2005B (za miesiąc!).

Odpowiednie wyprowadzenia programatora należy tymczasowo połączyć odcinkami przewodów z odpowiednimi polami lutowniczymi modułu CC1010. Moduł, który zastosowany zostanie w samochodzie należy wyposażyć w goldpiny tak, aby można go było włożyć na bazową płytkę drukowaną. Ponieważ zastosowane przez firmę Chipcon złącze ma raster wyprowadzeń równy 1,27 mm, a na płytce bazowej zastosowano gniazda o rastrze 2,54 mm, to do dyspozycji pozostaje co drugie wyprowadzenie modułu. Płytka bazowa została zaprojektowana pod tym właśnie kątem. Sposób montażu goldpinów przedstawiono na **rys. 4**.

Po zmontowaniu płytki jednostki centralnej należy w pierwszej kolejności sprawdzić wartość napięcia panującego na styku 1 gniazda goldpinów SV1. Powinna ona wynosić +3,3 V (napięcie to sygnalizuje LED1). W tym celu do złącza X1 dołączamy źródło napięcia stałego +12 V. Jeśli wartość napięcia jest prawidłowa, odłączamy zasilanie od układu, następnie umieszczamy płytkę modułu CC1010 (z programem jednostki centralnej i z goldpinami) w miejsce gniazd goldpinów. Łączymy za pomocą prostego kabla RS232 płytkę modułu z portem szeregowym komputera i uruchamiamy dowolny program terminalowy (np. HyperTerminal) z następującymi parametrami transmisji: 57600 b/s, 8N1. Po podaniu zasilania powinna ukazać się informacja powitalna z aktualną wartością klucza DES (**rys. 5**)

Kartę transponderową wyposażamy w baterię 3 V i po zaprogramowaniu umieszczamy blisko jednostki centralnej. Przy pierwszym uruchomieniu należy wprowadzić nową wartość klucza DES. W tym celu wpisujemy z klawiatury sekwencję znaków CMDXXXXXXX, gdzie X to wartość (ASCII) kolejnego bajtu klucza. Po tej czynności jednostka zapisuje nową wartość klucza do pamięci Flash i próbuje nawiązać komunikację z transponderem. Po udanym połączeniu klucz zostaje zapisany również w pamięci Flash transpondera (**rys. 6**) i zostaje wyświetlony poziom sygnału odebranego z karty transpoderowej. Po tych czynnościach układ jest gotowy do pracy. Na **rys. 7** przedstawiono przykładowy sposób dołączenia Immobilisera do instalacji elektrycznej samochodu.

Marcin Chruściel
chrusciel2@wp.pl



Rys. 8. Schemat montażowy płytki bazowej

CC1010 i PCB

Dystybutorem firmy Chipcon jest Soyter Components. Firma ta oferuje zarówno układy CC1010 jak i 4–warstwowe płytki drukowane do modułów radiowych. Kontakt: tel.: (22) 7220685 (6 linii), fax: (22) 7220550, handlowy@soyter.com.pl, www.soyter.com.pl.