Opis protokołu Mbus v2 dla telefonów Nokia 3210, 33xx, 3410, 51xx, 61xx, 62xx, 7110, 82xx, 9110, 9210

Programowanie telefonów komórkowych, część 1

Programowanie telefonów komórkowych jest z jednej strony „sztuką magiczną“, natomiast z drugiej można je przeprowadzić za pomocą dowolnego komputera i odpowiedniego oprogramowania. Podstawą jest znajomość protokołu Mbus, który przedstawiamy w artykule.

Transmisja w standardzie Mbus odbywa się jednoprzewodowo, tzn. przesył danych do i z telefonu odbywa się jedną linią komunikacyjną. Dane przesyłane są w postaci ramek, w których poszczególne bajty mają ściśle określone znaczenie. Transmisja zestawu ramek jest zabezpieczona przed błędami. Ostatnie miejsce w ramce zarezerwowane jest dla sumy kontrolnej, która obliczana jest specjalnym algorytmem.

W protokole Mbus wyróżniamy 2 podstawowe typy ramek:
- ramki danych,
- ramki potwierdzenia.

Komunikacja z telefonem odbywa się według poniższego schematu:
- wysyłamy ramkę danych,
- telefon odpowiada nam ramką potwierdzenia oraz ramką z pakietem informacji,
- wysyłamy ramkę potwierdzającą odbiór danych z telefonu.

Ramka danych

Format ramki danych wysyłanej do telefonu

ID – 00 – Type – Type2 – LenMin – LenMax – Type3 – Block – Seq – CheckSum

Format ramki danych otrzymywanej z telefonu

ID – Type – 00 – Type2 – LenMin – LenMax – Type3 – Block – Seq – CheckSum

Funkcje poszczególnych pól w ramkach wysyłanych i otrzymanych opisano w **tab. 1**.

Tab.1. Funkcje pól w ramkach wysyłanych i otrzymanych

Pozycja w ramce	Znaczenie	Opis
ID	Typ transmisji	0x1C - IR/Fbus 0x1E - Serial Fbus 0x1F - Serial Mbus
Type	Rodzaj transmisji	0x1D - TE Mbus 0x10 - TE Mbus (service soft) -wykorzystując ten rodzaj transmisji, należy wpierw wprowadzić telefon w tryb serwisowy
Type2	Typ ramki	0x40 - Ramka danych 0x7F - Ramka potwierdzająca
LenMin		0x00
LenMax	Długość ramki	Liczba bajtów w przedziale: [Block....Checksum]
Type3	Kierunek danych	0x00, 0x01 - ramka danych do telefonu 0x01, 0x01 - ramka danych z telefonu
Block	Blok danych	Jest to najbardziej znaczący obszar w całej ramce. Znajdują się tu bajty będące rozkazami dla telefonu oraz dane. Chcąc odczytać wartość określonego parametru, w tym bloku należy wstawić jedynie wartość rozkazu odpowiedzialnego za jego pobranie.
Seq	Numer sekwencji	Pole to zawiera numer sekwencji ramki. Numer sekwencji jest zwiększany przy kolejnej ramce wysyłanej do telefonu, pod warunkiem że nie przeprowadzamy retransmisji z powodu błędów.
Checksum	Suma kontrolna	Suma kontrolna niesie informację o poprawności ramki danych. Jeśli nie zostanie ona prawidłowo obliczona, telefon odrzuci ramkę i przerwie komunikację. Suma kontrolna obliczana jest ze wszystkich bajtów wchodzących w skład ramki za pomocą funkcji XOR.

Ramka danych w Mbus

Standardowe parametry transmisji są następujące: prędkość 9600 bd, ramka składa się z 8 bitów danych, 1 bitu stopu, bez parzystości.

Jeśli chcemy zmienić wartości ustawień telefonu, to po określonym rozkazie występują jeszcze bajty danych z nowymi wartościami dla określonego parametru.

W ramkach danych otrzymywanych z telefonu w tym bloku znajduje się kod rozkazu, który był wcześniej wysyłany, oraz wartości parametru, którego dany rozkaz dotyczy.

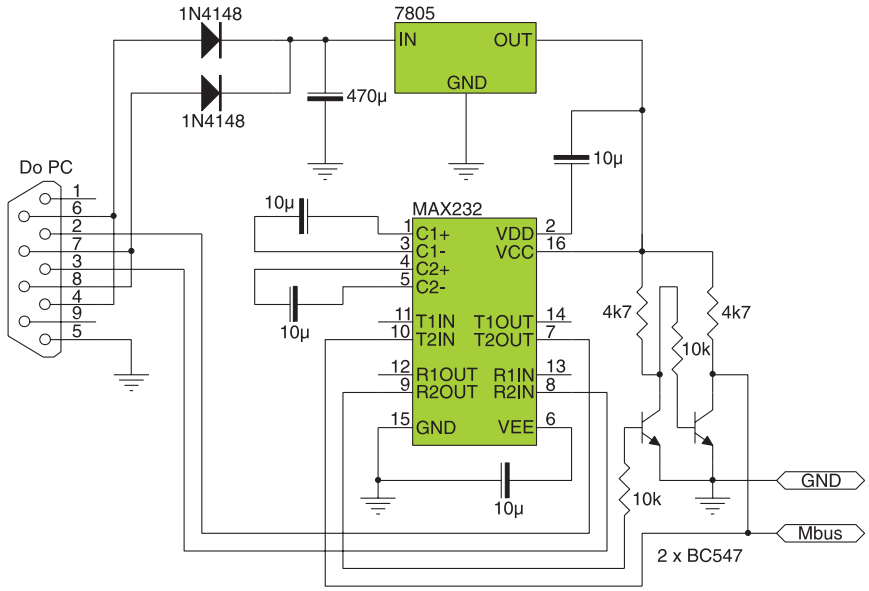
Ramki potwierdzenia

Po wysłaniu odpowiednio zbudowanej ramki danych, telefon odpowiada ramką potwierdzenia, oznaczającą poprawne odebranie danych, a następnie prześle nam w odpowiedzi ramkę danych. Odbiór danych musimy potwierdzić, wysyłając ramkę potwierdzenia o określonym formacie.

Format ramki potwierdzenia otrzymywanej z telefonu:

ID – Type – 00 – 7F – Seq2 – Checksum

W ramce potwierdzającej, którą otrzymujemy z telefonu, komorka Seq2 przyj-



Rys. 1. Schemat elektryczny standardowego interfejsu Mbus

muje wartość pola Seq z ramki, którą wcześniej wysyłaliśmy (ramka danych).

Format ramki potwierdzenia wysyłanej do telefonu

ID – 00 – Type – 7F – Seq2 – Checksum

Tryb testowy

Czynności opisane poniżej można wykonać wyłącznie po wcześniejszym wprowadzeniu telefonu w tryb testowy, tzw. *TEST MODE*. W tym trybie telefon jest przygotowany jedynie do wykonywania operacji testowych. Odbieranie połączeń przychodzących, a także wykonywanie połączeń nie jest możliwe. Telefon powróci do normalnego trybu pracy po wyzerowaniu lub wyłączeniu i ponownym włączeniu. Aby wprowadzić telefon w tryb testowy, należy wysłać ramkę z rozkazem przełączenia w *TEST MODE* (kod 0x64, 0x02).

Przełączenie w tryb testowy wymaga wysłania ramki danych pokazanej poniżej:

1F – 00 – 10 – 40 – 00 – 04 – 00 – 01 – 64 – 02 – 31 – 1D

Telefon potwierdza przyjęcie ramki poprzez wysłanie ramki:

1F – 10 – 00 – 7F – 31 – 41

Następnie telefon przesyła odpowiedź:

1F – 10 – 00 – 40 – 00 – 0C – 01 – 01 – 64 – 02 – 01 – 45 – 0D – 01 – 01 – 01 – 1B – 58 – 02 – 2C

Odebranie danych należy potwierdzić za pomocą ramki:

1F – 00 – 10 – 7F – 09 – 79

Najlepiej przeprowadzić retransmisję w celu uzyskania pewności, że telefon przełączył się w tryb testowy!

Prezentację budowy ramek komunikacyjnych mamy już za sobą, możemy więc przystąpić do „zabawy“ z telefonem.

Informacje o telefonie

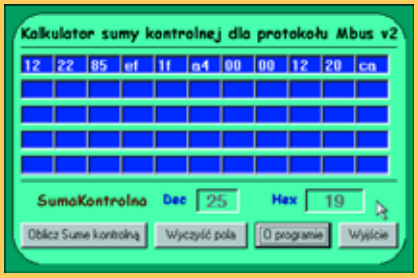
Aby uzyskać jakiekolwiek informacje od telefonu na temat jego parametrów, należy wysłać ramkę z rozkazem ich podania. W zależności od parametru, na temat którego chcemy uzyskać informacje, należy posłużyć się rozkazem odpowiedzialnym za ich pobranie. Każdemu rozkazowi przyporządkowany jest inny parametr.

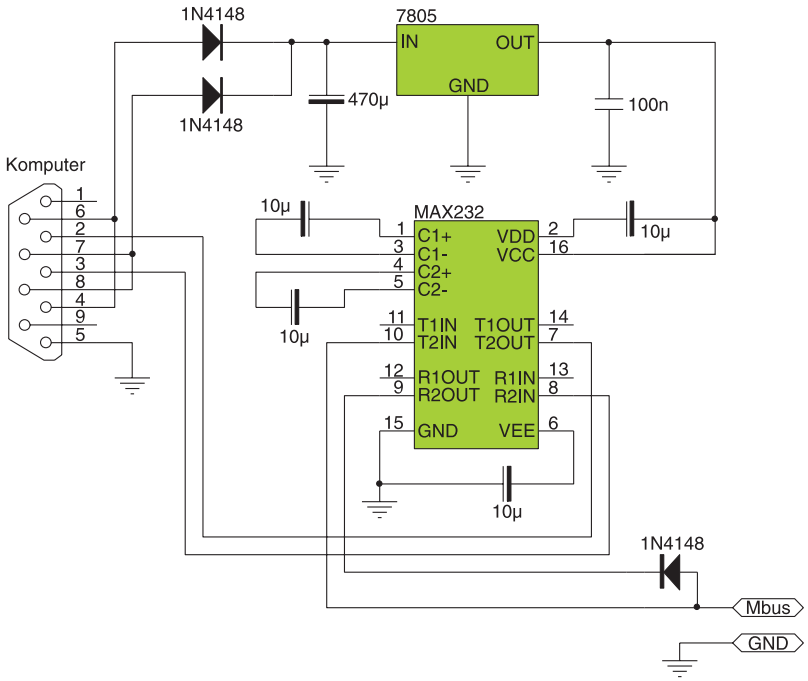
Tab. 2. Parametry możliwe do odczytania z telefonu oraz odpowiadające im kody rozkazów

Parametr do pobrania	Rozkaz binarny
MSID	0xB4, 0x45, 0xF9
MCU SW Checksum	0xC8, 0x02
COBBA	0xC8, 0x0D
DSP internal (ROM)	0xC8, 0x09
HW	0xC8, 0x05
ASIC Sys	0xC8, 0x0C
Locks info	0x8A, 0x00
Product serial number	0xCA, 0x03
Product code	0xCA, 0x04
Manufacter Month	0xCC, 0x02
Ustawienia profilu	0x6A

Sumy kontrolne

Liczenie sum kontrolnych ramek przesyłanych przez magistralę Mbus ułatwi program udostępniony przez autora artykułu, który publikujemy na płycie CD-EP5/2003B.





Rys. 2. Schemat uproszczonego interfejsu Mbus (dla modeli Nokia 8210 i 8850)

Przykłady

Wysyłamy ramkę z rozkazem podania wersji, daty powstania oraz wersji modelu

1F – 00 – 10 – 40 – 00 – 04 – 00 – 01 – C8 – 01 – 01 – 82

Telefon potwierdza przyjęcie ramki z poleceniem

1F – 10 – 00 – 7F – 01 – 71

Następnie przesyła odpowiedź:

1F – 10 – 00 – 40 – 00 – 25 – 01 – 01 – C8 – 01 – 00 – 56 – 20 – 30 – 36 – 2E – 30 – 30 – 0A – 30 – 33 – 2D – 31 – 30 – 2D – 30 – 30 – 0A – 4E – 53 – 45 – 2D – 38 – 0A – 28 – 63 – 29 – 20 – 4E – 4D – 50 – 2E – 00 – 03 – 84

Transmisję kończy potwierdzenie odebrania danych z telefonu

1F – 00 – 10 – 7F – 0A – 7A

Odebrane dane są zapisane są w kodzie szesnastkowym. Po konwersji kodu na znaki ASCII otrzymamy np.:

```
_V 06.00_03-10-00_NSE-8_
©|NMP.
```

Uzyskanie numeru IMEI wymaga wysłania ramki z danymi pokazanymi poniżej:

1F – 00 – 10 – 40 – 00 – 04 – 00 – 01 – CC – 01 – 02 – 85

Telefon potwierdza jej poprawne przyjęcie:

1F – 10 – 00 – 7F – 02 – 72

Następnie przesyła odpowiedź:

1F – 10 – 00 – 40 – 00 – 15 – 01 – 01 – CC – 01 – 00 – 35 – 35 – 35 – 35 – 35 – 35 – 35 – 35 – 35 – 35 – 35 – 35 – 35 – 35 – 38 – 00 – 03 – AC

Transmisję kończy potwierdzenie odebrania danych z telefonu:

1F – 00 – 10 – 7F – 0B – 7B

Po konwersji odebranego kodu na znaki ASCII otrzymamy numer IMEI:

```
555555555555558
```

Zmiana IMEI i innych parametrów telefonu

Modyfikację IMEI oraz szeregu innych parametrów umożliwia program Nokia Tester, który publikujemy na CD-EP7/2003B.

Przedstawiony powyżej IMEI został celowo zmieniony w telefonie na potrzeby artykułu. W rzeczywistości taka wartości nie jest prawidłowa. Każdy telefon ma swój niepowtarzalny IMEI, który nie powinien być nikomu udostępniany. W niektórych krajach zmiana IMEI w telefonach jest prawnie zabroniona.

Odczytanie kodu zabezpieczającego wymaga wysłania ramki pokazanej poniżej:

1F – 00 – 10 – 40 – 00 – 04 – 00 – 01 – 6E – 01 – 03 – 26

Telefon potwierdza jej poprawny odbiór za pomocą ramki:

1F – 10 – 00 – 7F – 03 – 73

Następnie telefon przesyła odpowiedź zawierającą kod zabezpieczający (w zapisie szesnastkowym):

1F – 10 – 00 – 40 – 00 – 0B – 01 – 01 – 6E – 01 – 01 – 31 – 32 – 33 – 34 – 35 – 00 – 05 – 1E

Transmisję kończy potwierdzenie odbioru danych:

1F – 00 – 10 – 7F – 0C – 7C

Po konwersji odebranego kodu na znaki ASCII otrzymujemy:

```
12345
```

Uzyskanie informacji o zainstalowanym w telefonie pakiecie językowym wymaga przesłania do telefonu następującej ramki danych:

1F – 00 – 10 – 40 – 00 – 04 – 00 – 01 – C8 – 12 – 04 – 94

Telefon potwierdza jej przyjęcie za pomocą ramki pokazanej poniżej:

1F – 10 – 00 – 7F – 04 – 74

Następnie przesyła odpowiedź:

1F – 10 – 00 – 40 – 00 – 07 – 01 – 01 – C8 – 12 – 00 – 42 – 00 – 09 – D9

Transmisję kończy potwierdzenie odbioru danych:

1F – 00 – 10 – 7F – 0D – 7D

Po konwersji odebranego kodu na znak ASCII otrzymamy: B - litera ta oznacza w przypadku Nokii 3210 następujące dostępne języki: angielski, niemiecki, francuski, grecki, bułgarski, węgierski, rumuński, polski, czeski, słowacki, chorwacki, serbski, słoweński, rosyjski, estoński, litewski, łotewski, arabski, hebrajski.

W **tab. 2** zestawiono niektóre parametry, które można odczytać z telefonu oraz odpowiadające im kody rozkazów.

Do odczytywania i modyfikacji parametrów telefonów jest niezbędne specjalne oprogramowanie oraz łatwy w wykonaniu interfejs, którego dwa warianty przedstawiono na **rys. 1** i **2**. Oprogramowanie sterujące, w tym edytor podstawowych parametrów telefonów, publikujemy na CD-EP7/2003B.

Marcin Czerniawski
SimKom@wp.pl

Pragnę gorąco podziękować mojej dziewczynie Agnieszce za duchowe wsparcie podczas zdobywanie informacji na temat protokołu oraz podczas pisania artykułu. Bez jej pomocy artykuł nigdy by nie powstał.