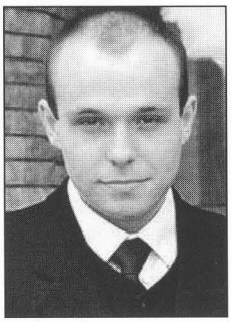
Lucjan BRYNDZA, Dariusz RZOŃCA
POLITECHNIKA RZESZOWSKA, KATEDRA INFORMATYKI I AUTOMATYKI

Zdalna obsługa sterowników przemysłowych przy użyciu sieci Internet lub telefonii GSM

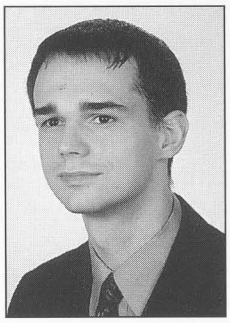
mgr inż. Lucjan BRYNDZA



Jest absolwentem Wydziału Elektrotechniki i Informatyki Politechniki Rzeszowskiej na kierunku Elektrotechnika, specjalność Automatyka i Informatyka. Główne zainteresowania skupiają się na automatyce, informatyce, zagadnieniach dotyczących komunikacji sieciowej, oraz projektowaniu sterowników mikroprocesorowych opartych na mikrokomputerach jednoukładowych.

e-mail: lucck@loken.pl

mgr inż. Dariusz RZOŃCA



Jest absolwentem Wydziału Elektrotechniki i Informatyki Politechniki Rzeszowskiej na kierunku Informatyka. Obecnie asystent w Katedrze Informatyki i Automatyki Politechniki Rzeszowskiej. Zajmuje się zagadnieniami związanymi z komunikacją w systemach mikroprocesorowych.

e-mail: drzonca@prz-rzeszow.pl

Streszczenie

W artykule opisano dwa urządzenia umożliwiające zdalną obsługę sterownika przemysłowego, opracowane w Katedrze Informatyki i Automatyki Politechniki Rzeszowskiej. Jedno z urządzeń wykorzystuje do tego celu sieć Internet, drugie zaś sieć telefonii komórkowej GSM.

Abstract

This article presents two devices enabling programmable controllers remote control, built in Computer and Control Engineering Chair of Rzeszow University of Technology. One of them uses Internet, the other one uses GSM cellular phone network.

Słowa kluczowe: protokół Modbus, sterowniki przemysłowe, zdalna obsługa.

Keywords: Modbus protocol, programmable controllers, remote control.

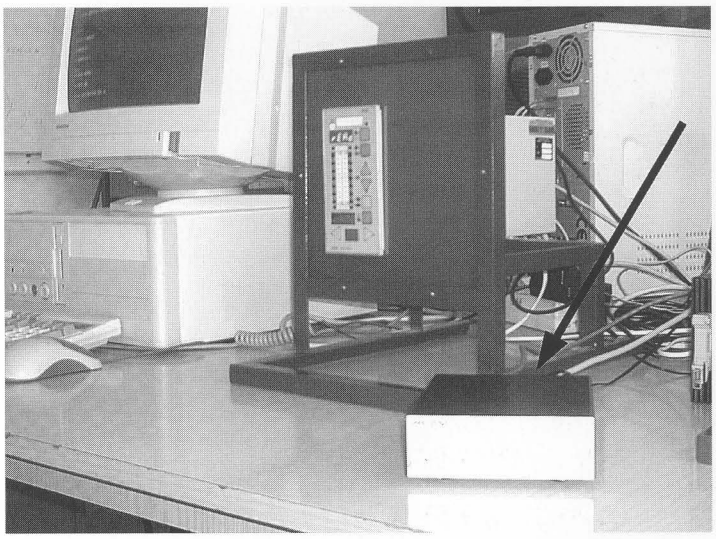
1. Wstęp

Sterowniki przemysłowe są obecnie powszechnie wykorzystywane w przemyśle. Zazwyczaj umożliwiają one komunikację przy wykorzystaniu protokołu Modbus [1], który stał się niejako standardem. Często jednak pojawia się problem zdalnej obsługi sterownika - zaistniała więc potrzeba skonstruowania odpowiedniego konwertera. W niniejszym artykule opisane są dwa takie urządzenia, których prototypy autorzy opracowali na Politechnice Rzeszowskiej w ramach prac dyplomowych. Jedno z nich wykorzystuje w tym celu sieć Internet, natomiast drugie sieć telefonii komórkowej GSM.

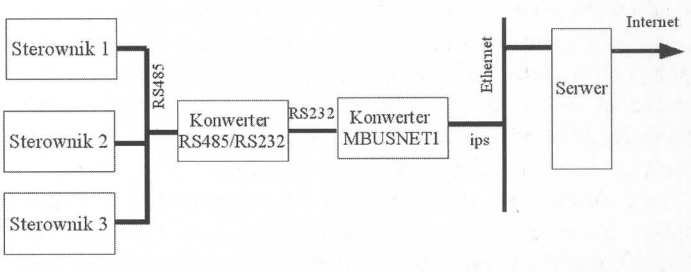
2. Wykorzystanie sieci LAN

Obecnie często w budynkach dostępna jest sieć lokalna LAN, łącząca ze sobą komputery i umożliwiająca dostęp do Internetu. Idealne w takim przypadku wydaje się podłączenie sterownika przemysłowego wprost do gniazdka sieciowego, przez co uzyskujemy możliwość tworzenia rozległej sieci sterowników niewielkim nakładem finansowym. Najprostszą możliwością podłączenia sterownika do sieci jest wykorzystanie specjalnie napisanej aplikacji dla komputera PC i podłączenie go do portu RS232. Jednak jest to rozwiązanie dość drogie i niezbyt bezpieczne. Znacznie lepszym rozwiązaniem jest zbudowanie dedykowanego urządzenia.

Opracowane urządzenie [2] realizuje funkcję serwera, który umożliwia przesyłanie komunikatów Modbus, wykorzystując protokół TCP/IP. Jako medium transmisyjne zastosowano sieć 10Mbit Ethernet. Komunikacja od strony sieciowej odbywa się za pomocą specjalnie opracowanego protokołu transmisyjnego, służącego do przekazywania ramek Modbus za pośrednictwem protokołu TCP/IP. Szczególny nacisk położono na zapewnienie bezpieczeństwa poprzez szyfrowanie przesyłanych ramek [3]. Cała sesja jest szyfrowana za pomocą algorytmu ze 128 bitowym kluczem, więc bez obawy o bezpieczeństwo przesyłanych danych możemy urządzeniu przypisać zewnętrzny adres IP. Przesyłanie danych wymaga wcześniejszego uwierzytelnienia oraz zgodności kluczy szyfrujących w urządzeniu i programie sterującym. Możliwa jest także jednoczesna obsługa wielu połączeń. Urządzenie wyposażono w prosty serwer protokołu Telnet, który umożliwia zdalną zmianę parametrów konfiguracji sieci, ustawień portu szeregowego, oraz klucza szyfrującego. Dostęp do serwera Telnet został ograniczony tylko do sieci lokalnej, ponieważ dane w tym protokole nie są szyfrowane i stanowią potencjalne zagrożenie dla bezpieczeństwa. Na rysunku 2 przedstawiono sposób podłączenia grupy sterowników do Internetu z wykorzystaniem jednego konwertera MODBUS<->TCP/IP.

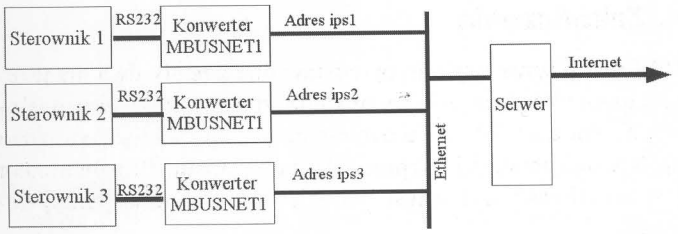


Rys. 1. Konwerter MODBUS<->TCP/IP wraz ze sterownikiem PSW-84
Fig. 1. MODBUS<->TCP/IP converter and PSW-84 programmable controller.



Rys. 2. Wykorzystanie pojedynczego konwertera MODBUS<->TCP/IP do podłączenia grupy sterowników.
Fig. 2. Single MODBUS<->TCP/IP converter applied to connect group of controllers.

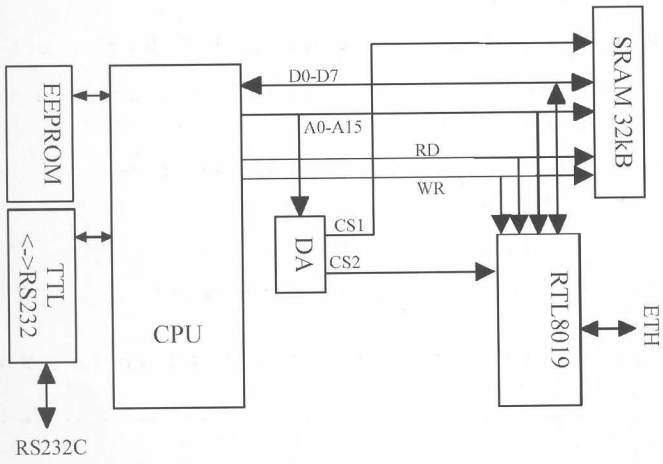
Sterowniki połączone są ze sobą w sieć RS485, a następnie podłączone do urządzenia za pośrednictwem konwertera RS232/RS485. Program nadrzędny w celu skomunikowania się ze sterownikami łączy z konwerterem, a wybór sterownika odbywa się poprzez pole adresowe ramki Modbus. Lepszym rozwiązaniem ze względu na wydajność jest sposób podłączenia sterowników przedstawiony na rysunku 3.



Rys. 3. Wykorzystanie kilku konwerterów do podłączenia grupy sterowników.
Fig. 3. Multiple MODBUS<->TCP/IP converters applied to connect group of controllers.

Każdy sterownik połączony jest za pośrednictwem portu RS232 z osobnym konwerterem, podłączonym do sieci LAN. Program nadrzędny w celu skomunikowania się z wybranym sterownikiem musi połączyć się z konwerterem o określonym adresie IP do którego jest podłączony sterownik, a następnie przesłać dane dla sterownika.

Poniżej przedstawiono schemat blokowy urządzenia.



Rys. 4. Schemat blokowy konwertera MODBUS<->TCP/IP.
Fig. 4. MODBUS<->TCP/IP converter block diagram.

Urządzenie zostało zbudowane w oparciu o mikrokontroler P89C664 [4] (zgodny z 8051). Program zapisany jest w wewnętrznej pamięci flash. Do przestrzeni adresowej mikrokontrolera za pośrednictwem dekodera adresowego (DA) podłączono kontroler sieci Ethernet RTL8019AS oraz pamięć SRAM 32kB służącą do przechowywania zmiennych. Do portów wejścia-wyjścia mikrokontrolera podłączono pamięć EEPROM z magistralą I2C, która przechowuje dane konfiguracyjne sterownika. Linie łącza szeregowego procesora za pośrednictwem konwertera poziomów napięć z TTL/RS232 podłączone są do zewnętrznego gniazda portu RS232.

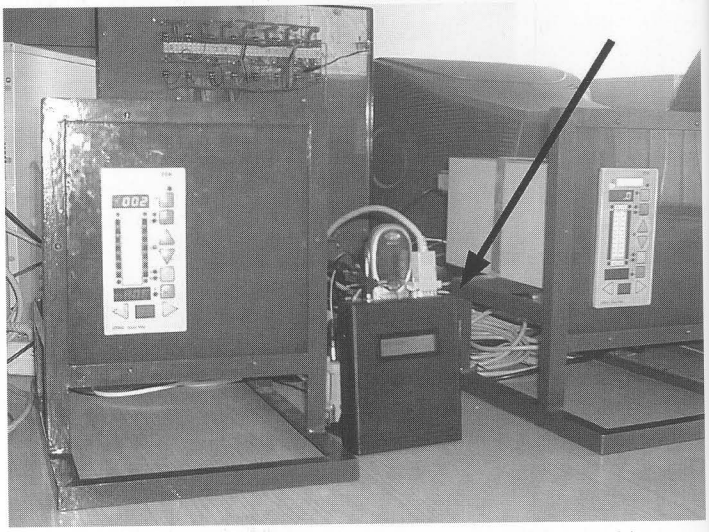
Została opracowana również specjalna biblioteka na komputer nadrzędny, oparta na technologii COM, udostępniająca zestaw funkcji służących do komunikacji z konwerterem. Zawarty w bibliotece zestaw funkcji sprawia, że dla aplikacji transmisja jest „przeźroczysta", ponieważ dane otrzymane z urządzenia są dekodowane i kodowane przez bibliotekę zwalniając programistę od obowiązku tworzenia ramek dla urządzenia.

Program sterujący działający na komputerze PC nawiązuje połączenie ze sterownikiem, wysyłając w postaci zaszyfrowanej login i hasło. Konwerter po przeprowadzeniu identyfikacji umożliwia przeprowadzenie transmisji ze sterownikiem. Aplikacja, gdy chce wysłać zapytanie do sterownika tworzy ramkę Modbus i wywołuje odpowiednią funkcję biblioteki, która formuje ramkę transmisyjną, szyfruje ją i przesyła za pomocą protokołu TCP/IP. Konwerter po odebraniu ramki deszyfruje ją i sprawdza integralność pakietu. Jeżeli pakiet jest poprawny i poprzez port szeregowy nie są właśnie wysyłane inne dane (mogące pochodzić od innej sesji), wówczas przesyłany jest on do sterownika. Sterownik w odpowiedzi przesyła ramkę, na podstawie której tworzony jest pakiet transmisyjny, szyfrowany, oraz za pomocą protokołu TCP/IP przesyła go do komputera. Gdy odpowiedź dotrze do biblioteki, wówczas jest ona deszyfrowana, sprawdzana jest jej poprawność, a następnie jest ona przesyłana do programu nadrzędnego.

Urządzenie zostało przetestowane w konfiguracji z rysunku 2. Testy zostały wykonane z wykorzystaniem sterowników PSW-84 oraz PSW-166.

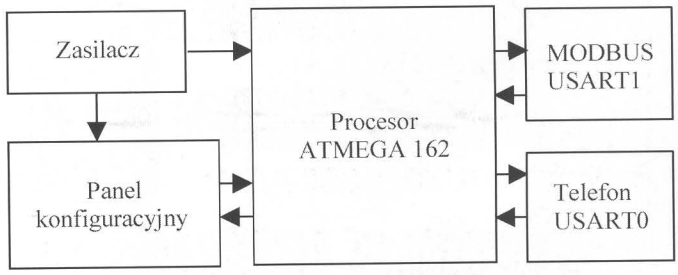
3. Wykorzystanie sieci GSM

Aby maksymalnie zwiększyć mobilność i dyspozycyjność operatora sterownika przemysłowego korzystne wydaje się wykorzystanie telefonu komórkowego - urządzenia, które umożliwia działanie w niemal dowolnym miejscu na całym świecie. Zagadnienie to jest stosunkowo nowe, gdyż dopiero gwałtowny rozwój telefonii komórkowej w ciągu ostatnich kilku lat umożliwił jego praktyczną realizację. Podobne urządzenia wykorzystuje się już wprawdzie w przemyśle, lecz wciąż znajdują się w fazie intensywnego rozwoju.



Rys. 5. Konwerter MODBUS<->GSM wraz ze sterownikiem PSW-84.
Fig. 5. MODBUS<->GSM converter and PSW-84 programmable controller.

Opracowane urządzenie [5] bazuje na mikrokontrolerze typu Atmel AVR [6]. Schemat blokowy konwertera pokazany jest na rysunku 6.



Rys. 6. Schemat blokowy konwertera MODBUS<->GSM.
Fig. 6. MODBUS<->GSM converter block diagram.

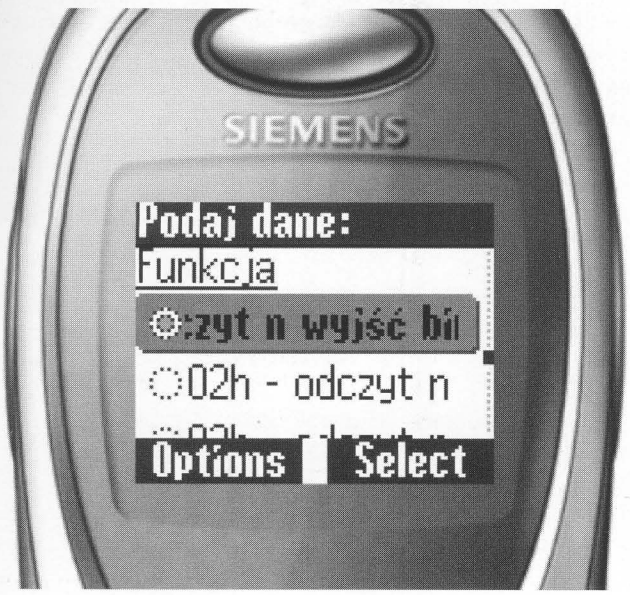
Konwerter ten pozwala na podłączenie dowolnego sterownika przemysłowego obsługującego standardowy protokół Modbus poprzez port szeregowy RS232 lub grupy takich sterowników przy wykorzystaniu interfejsu RS485. Jako urządzenie nadawczo-odbiorcze zastosowano zwykły telefon komórkowy, ale oczywiście istnieje możliwość podłączenia przemysłowego modemu GSM.

Komunikacja odbywa się za pomocą krótkich wiadomości tekstowych SMS. Identyfikacja operatora i weryfikacja uprawnień następuje na podstawie numeru telefonu nadawcy. Po stronie operatora zazwyczaj znajduje się analogiczne urządzenie podłączone do komputera PC z odpowiednim oprogramowaniem. Możliwa jest także obsługa bezpośrednio z poziomu telefonu komórkowego, z pominięciem dodatkowego urządzenia i kompute-

ra. Współczesne telefony komórkowe często umożliwiają uruchamianie specjalnych aplikacji (tzw. midletów) napisanych w języku Java [7]. Korzystając z tego opracowaliśmy specjalny program na telefon komórkowy, pozwalający operatorowi na obsługę sterownika. Alternatywą, w przypadku starszych telefonów komórkowych nie wspierających technologii J2ME (tj. nie pozwalających na uruchamianie midletów) jest bezpośrednie wpisanie przez operatora odpowiedniego komunikatu i wysłanie go jako wiadomość SMS - niestety pogarsza to wygodę obsługi.

W przypadku typowej konfiguracji (z opisywanym urządzeniem i komputerem PC po stronie operatora) konwersja i transmisja dokonywana przez urządzenie jest z punktu widzenia użytkownika „przezroczysta". Oznacza to, że możliwe jest wykorzystanie dotychczas stosowanego oprogramowania operatorskiego, podłączenia zamiast sterownika opisywanego konwertera, podłączenia identycznego urządzenia do sterownika i po krótkiej konfiguracji operator pracuje tak jak dotychczas, przy bezpośrednim połączeniu komputera ze sterownikiem. Dzięki temu nie jest konieczne kosztowne powtórne szkolenie pracowników. Program operatorski tworzy odpowiednie komunikaty Modbus i wysyła je przez port szeregowy. Konwerter po odebraniu komunikatu weryfikuje jego integralność (suma kontrolna), „pakuje" w odpowiednią ramkę transportową i przesyła w postaci wiadomości SMS do odbiornika podłączonego do zaadresowanego sterownika. Odbiornik weryfikuje poprawność transmisji, „rozpakowuje" właściwą ramkę Modbus, kontroluje uprawnienia danego użytkownika do wydania polecenia i jeżeli wszystko się zgadza to przesyła ramkę do sterownika. Odpowiedź do komputera nadrzędnego przesyłana jest analogicznie.

W przypadku wykorzystania po stronie operatora jedynie telefonu komórkowego i aplikacji mobilnej obsługa jest inna, aczkolwiek równie prosta i intuicyjna. Operator, odpowiadając na szereg pytań w programie, wybiera żądaną funkcję Modbus i odpowiednie parametry (patrz rysunek 7).



Rys. 7. Ekran telefonu podczas pracy z aplikacją mobilną.
Fig. 7. Mobile application on phone screen.

Na tej podstawie jest generowana i wysyłana odpowiednia wiadomość tekstowa SMS. Niestety interpretacja wiadomości zwrotnej należy już bezpośrednio do operatora. Midlety ze względów bezpieczeństwa działają w specjalnym środowisku (sandbox) na maszynie wirtualnej i w związku z czym występuje brak dostępu aplikacji mobilnej do odebranych wiadomości.

Urządzenie zostało pomyślnie przetestowane ze sterownikami przemysłowymi PSW-84 i PSW-166, oraz z telefonami komórkowymi Siemens S35 i SL45.

4. Zakończenie

W niniejszym artykule przedstawione zostały dwa urządzenia umożliwiające zdalną obsługę sterowników przemysłowych. Podczas ich opracowywania główny nacisk położono na łatwość obsługi i bezpieczeństwo systemu. Dużym atutem jest możliwość wykorzystania ich w już istniejących systemach.

Praca naukowa częściowo finansowana z grantu badawczego Ministerstwa Nauki i Informatyzacji nr 4 T11A 017 24.

5. Literatura

[1] Modicon MODBUS Protocol Reference Guide. Massachusetts 1996.

[2] L. Bryndza, G. Kowal: Konwerter MODBUS <-> TCP/IP. Politechnika Rzeszowska 2004.

[3] B. Schneier: Kryptografia dla praktyków. WNT, Warszawa 2002.

[4] DataSheet P89C664 80C51 8-bit Flash microcontroller family. Philips 2002.

[5] D. Rzońca, A. Pudelski: Interfejs MODBUS-GSM. Politechnika Rzeszowska 2004.

[6] ATmega 162 Datasheet. Atmel 2003.

[7] K. Topley: J2ME Almanach. Helion, Gliwice 2003.

Title: Programmable controllers remote control using Internet or GSM cellular phones

Artykuł recenzowany

Agenda Wydawnicza Redakcja
Pomiary Automatyka Kontrola

ZATRUDNI

do pracy w redakcji
w niepełnym wymiarze czasu pracy
(etat lub umowa-zlecenie)
osoby
na stanowisku
- specjalisty do spraw marketingu
- sekretarza redakcji

kontakt:
00-050 Warszawa,
ul. Świętokrzyska 14A pok. 535
tel. (022) 827 25 40, 827 31 22
tel. kom 0607 457 328