mgr inż. Marcin Gliński,
dr inż., Roman Szewczyk
mgr inż. Andrzej Bratek
Przemysłowy Instytut Automatyki i Pomiarów

# METODY ZDALNEGO SERWISOWANIA UKŁADÓW POMIAROWYCH I SYSTEMÓW AUTOMATYKI.

*W referacie przedstawiono możliwości i uwarunkowania wykorzystania dostępnych obecnie usług teletransmisji, począwszy od telefonicznych łącz komutowanych, poprzez sieć ethernet i bezprzewodową sieć GSM*

# MEASUREMENT AND CONTROL SYSTEMS REMOTE SERVICE METHODS

*Paper presents possibilities and limitations of teletransmission services utilization discussion in context of remote service operations starting with switched PSTN lines through ethernet and cellular network.*

## 1.WPROWADZENIE

Niezwykle dynamiczny rozwój telekomunikacji w ostatnich latach doprowadził do powszechnego dostępu do różnorodnych metod teletransmisji. W niniejszej pracy skupiono się na wykorzystaniu usług operatorów gotowej infrastruktury teleinformatycznej jako naturalnej metody do prowadzenia operacji zdalnej diagnostyki, rekonfiguracji, oraz rozruchu systemów automatyki i pomiarów. Potrzeba taka wydaje się być truizmem, dlatego dla porządku należy przytoczyć jedynie główne korzyści wynikających ze zdalnego serwisownia urządzeń automatyki. Są to przede wszystkim:

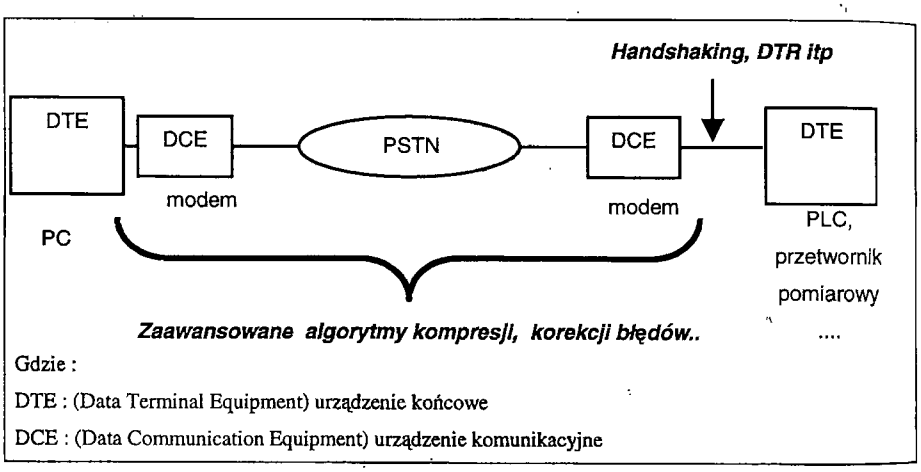
- oszczędność kosztów związanych z bezproduktywnym czasem inżyniera poświęconym na dojazd na obiekt (często czas ten przekracza czas całej operacji wykonywanej na miejscu)
- możliwość natychmiastowego połączenia on-line z systemem na obiekcie w nieregularnie występujących stanach niestabilności instalacji.

Wykorzystanie powszechnie znanych kanałów teletransmisji w przypadku teleserwisowania systemów przemysłowych wymaga szczególnego omówienia ze względu na specyfikę tych urządzeń. Polega ona na implementacji niestandardowych protokołów, przy ograniczonych możliwościach komunikacyjnych w porównaniu ze standardem platformy PC.

# 2.OMÓWIENIE WYBRANYCH KANAŁÓW TELETRANSMISJI

## 2.1. Łącza komutowane publicznej sieci telefonicznej PSTN

Jest to najstarszy z omawianych typów kanałów teletransmisji. Schemat tego typu połączenia przedstawiono na rys. 1. Połączenie jest komutowane (zestawiane) w publicznej sieci telefonicznej (PSTN). Z punktu widzenia użytkownika (czyli urządzeń końcowych DTE) kanał ten wygląda jak połączenie typu „punkt-punkt" za pomocą zwykłego kabla w standardzie łącza szeregowego (przeważnie RS-232). Powszechnie rolę urządzeń końcowych pełnią komputery PC i zestawienie takiego połączenia nie stanowi większego problemu, z uwagi na pełną obsługę sygnałów portów szeregowych oraz na łatwą konfigurację modemów z wykorzystaniem drajwerów dedykowanych dla systemu operacyjnego.




**Rys. 1 Schemat połączenia komutowanego**

W przypadku zastosowania jako urządzeń końcowych, urządzeń stosowanych w rozwiązaniach przemysłowych (np. sterowników PLC) należy liczyć się z możliwością wystąpienia problemów wynikających zarówno z braku zachowania standardu RS-232, jak i nakładania się zaawansowanych protokołów modemowych.

Najprostszym, ale zarazem najczęściej występującym przypadkiem są odstępstwa od specyfikacji łącza szeregowego.

Należy pamiętać że urządzenia automatyki i pomiarów (PLC, konwertery RS232/485 itp.) zgodnie ze specyfikacją EIA/TIA, z reguły należą do kategorii urządzeń komunikacyjnych DCE, choć np. na

Rys. 1 widać, że funkcjonalnie pełnią one rolę terminali końcowych DTE. Paradoks ten wynika stąd, że wg specyfikacji urządzenia kategorii DCE mają na fizycznym złączu tak usytuowane wszystkie złącza sygnałowe, aby połączenie z urządzeniem DTE (najczęściej stacją PC) było wykonywane prostym kablem typu „jeden do jednego". Z uwagi na to, że podstawową konfiguracją pracy omawianych elementów systemów przemysło-

wych jest bezpośrednia współpraca z komputerem PC, ich porty wykonywane są właśnie w konwencji DCE.

Najczęściej obsługiwane są tylko sygnały nadawania i odbioru danych. Prowadzi to do konieczności mozolnego konfigurowania modemu za pomocą komend AT lub wprowadzania odpowiednich „sztucznych" sygnałów elektrycznych na port – np. DTR (gotowości do pracy urządzenia DTE).

W pewnych okolicznościach problemem może się okazać również sterowanie przepływem. Nie są znane autorom przemysłowe aplikacje sterowania programowego (xon, xof), natomiast sterownie sprzętowe wymaga obsługi odpowiednich sygnałów (RTS, CTS) od strony serwisowanego urządzenia i przeważnie konfiguracji modemu z poziomu komend AT. Należy zauważyć, że sterownie przepływem jest potrzebne wtedy, kiedy prędkość transmisji między modemami telefonicznymi jest niższa niż prędkość na łączu serwisowanego urządzenia. Problem ten można ewentualnie rozwiązać poprzez konfigurację komunikacji z poziomu oprogramowania serwisowego, parametryzując bloki zapytań tak, aby odpowiedzi mieściły się w buforze modemu, oraz ustawiając odpowiednio duże czasy okresów zapytań i oczekiwania na odpowiedź.

Problem nakładania zaawansowanych protokołów modemowych na protokoły przemysłowe polega na tym, że z punktu widzenia urządzeń DTE połączenie modemowe tylko pozornie jest równoważne połączeniu kablowemu. W rzeczywistości modemy przed przesłaniem danych na linię telefoniczną dokonują obróbki przesyłanych danych poprzez ich kompresję, przy odbiorze zaś stosują algorytmy do korekcji błędów. Może to powodować deformację danych pierwotnego protokołu przemysłowego do takiego stopnia, że przestanie on być czytelny dla urządzenia odbiorczego. Dotyczy to głównie starszych protokołów, w których wykorzystywane były przerwy czasowe (np. protokół używany przez starsze jednostki centralne sterowników GE-Fanuc rodziny 90-30, wykorzystujący tzw. Long Brakes). W takim przypadku należy wyłączyć algorytmy własne modemu. Może to być proces żmudny, ponieważ każdy z producentów modemowych scalonych układów mikroprocesorowych używa własnych komend AT.

Znacznie łatwiejsze jest wykorzystanie łącza komutowanego do serwisowania stacji PC będącej węzłem systemu SCADA. Wykorzystuje się tu szeroko dostępne oprogramowanie typu zdalny terminal, które przesyła poprzez dostępny kanał komunikacyjny (np. połączenie modemowe lub Ethernet) jedynie obraz ze stacji serwisowanej oraz rozkazy klawiatury i myszy ze stacji serwisowej. Dzięki temu nawet przy połączeniu z prędkością rzędu 33 kb/s istnieje możliwość efektywnej pracy na komputerze zdalnym.

Omawiany sposób komunikacji nie wymaga żadnej dodatkowej konfiguracji ze strony operatora sieci transmisyjnej. Jedynym wymaganiem jest doprowadzenie przez użytkownika końcowego linii telefonicznej do miejsca pracy serwisowanego zdalnie modułu systemu. Nie jest wymagany bezpośredni dostęp do numeru końcowego z sieci publicznej, jeśli użytkownik końcowy posiada automatyczną centralę wewnętrzną. Jedyną przeszkodę może stanowić ręczne zestawianie połączenia, ale w praktyce rozwiązanie to nie jest już spotykane.

Należy podkreślić że przy takim sposobie zdalnego serwisowania urządzeń automatyki, koszty naliczane są w zależności od czasu połączenia.

## 2.2. Sieć ethernet

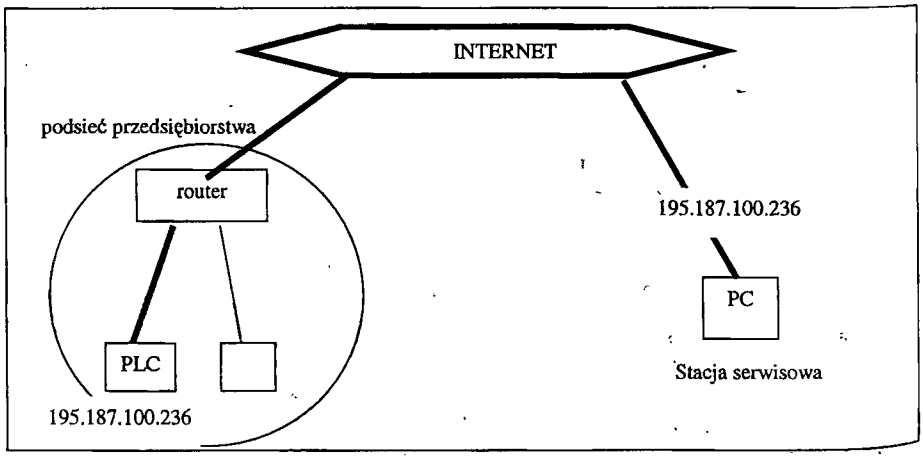
Jest to sieć, której powszechność, przepustowość i globalna infrastruktura (jako składowa sieci Internet) czynią ją standardem, który również będzie wykorzystywany w automatyce przemysłowej.

Rozwój komunikacyjnych standardów przemysłowych postępuje krok za teleinformatyką. Chociaż obecnie jesteśmy „w przeddzień" praktycznej implementacji standardu ethernet w większości urządzeń przemysłowych (gdzie nie jest wymagany formalny determinizm sieci przesyłowej) to należy liczyć się z tym, że jeszcze przez kilka lat porty szeregowe będą na wyposażeniu nowych urządzeń, a w przypadku integracji systemów pracujących na obiekcie, stan ten będzie się utrzymywał znacznie dłużej.

Podstawowym warunkiem wykorzystania łącza ethernet w aplikacjach serwisowych jest wyposażenie serwisowanego urządzenia w odpowiedni port i obsługę protokołów. W przypadku braku takiego rozwiązania można skorzystać z zewnętrznych konwerterów portów szeregowych na zestaw protokołów TCP/IP.

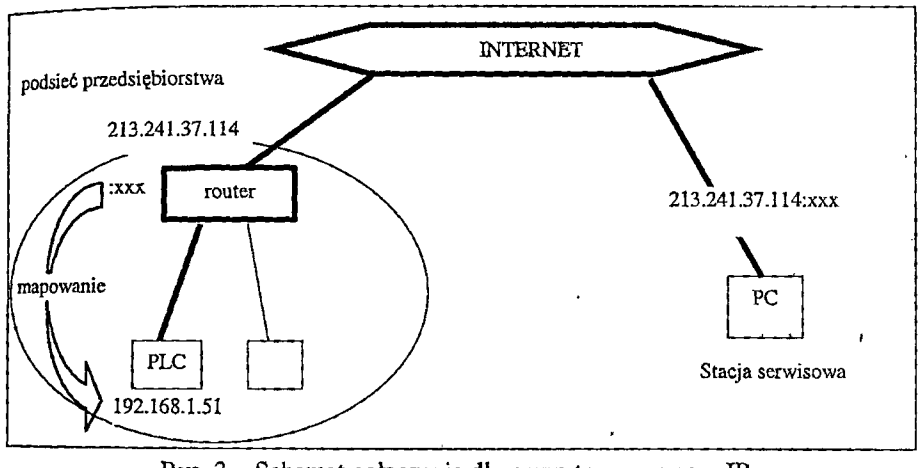
Następnym warunkiem jest, podobnie jak w bezprzewodowej transmisji GPRS, przydzielenie stałego (tzw. publicznego) adresu IP, widzianego w całej sieci Internet. Realizacja tego warunku leży, w zasadzie, po stronie użytkownika końcowego i jego służb IT. W niniejszej pracy zostaną opisane dwie typowe konfiguracje połączenia TCP/IP stosowanego do celów serwisu urządzeń automatyki.

Pierwsza konfiguracja (mniej powszechna) dotyczy przedsiębiorstw, które wcześnie integrowały swoje sieci prywatne z siecią Internet i otrzymały z organizacji IANA (Internet Assigned Numbers Authority) przydział dostatecznie dużej liczby publicznych adresów IP, tzn takich, które są niepowtarzalne w całej sieci Internet. W takim przypadku nawiązanie połączenia z serwisowanym urządzeniem realizowana jest przez podanie jego adresu IP. Schemat takiego połączenia przedstawiono na rys. 2.




Rys. 2 Schemat połączenia dla numeru IP publicznego

Znacznie powszechniejszym jest model, w którym tylko ruter ma przydzielony adres publiczny (np. 213.241.37.114), natomiast pozostałe węzły podsieci przedsiębiorstwa mają adresy prywatne (np. 192.168.1.51), które są widziane tylko w podsieci (Rys. 3). W takim przypadku użytkownik końcowy musi skonfigurować przekierowanie połączenia z wykorzystaniem jednego z portów rutera na adres przydzielony w podsieci serwisowanemu urządzeniu. Format adresu urządzenia serwisowanego w tym przypadku jest postaci 213.241.37.114:xxx, gdzie xxx oznacza numer portu rutera, z którego następuje przekierownie bezpośrednio na adres urządzenia serwisowanego (192.168.1.51) funkcjonujący w podsieci użytkownika końcowego




Rys. 3. Schemat połączenia dla prywatnego numeru IP

W obu przypadkach należy zwrócić szczególną uwagę na konfigurację systemów bezpieczeństwa sieciowego u użytkownika końcowego, jak np. ścian ogniowych „firewall", aby pozwalały one na dostęp do serwisowanego urządzenia z komputera zewnętrznego.

### 2.3. Łącze komutowane GSM

Z punktu widzenia użytkownika jest to analogiczny sposób transmisji, jak w przypadku łącza komutowanego PSTN.

Różnica polega na tym, że urządzenia DCE są bezprzewodowe. Nie są one modemami, określa się je mianem modułów transmisji danych, lub terminali GSM. Wynika to stąd, że w przypadku terminali GSM nie zachodzi proces modulacji i demodulacji sygnału analogowego, ponieważ transmisja odbywa się cyfrowo.

Transmisja w infrastrukturze operatora sieci przesyłowej odbywa się poprzez łącza bezprzewodowe między modułami GSM użytkownika, a stacjami bazowymi BTS oraz w sieci szkieletowej między stacjami BTS. Występują tu znaczące opóźnienia transmisyjne (głównie składające się z opóźnień przełączania, w znacznie mniejszym stopniu z

opóźnień propagacyjnych), co wymaga odpowiedniej konfiguracji protokołu w oprogramowaniu serwisowym.

Zestawienie tego typu połączenia wymaga aktywacji dodatkowej usługi transmisji danych u operatora sieci komórkowej. Dostępne są dwa tryby: zwykła transmisja danych CSD z prędkością 9600 bit/s oraz szybka HSCD, gdzie przydzielane jest do transmisji kilka kanałów (szczelin czasowych) jednocześnie i obecnie prędkość transmisji wynosi już 56 000 bit/s.

Pojecie szczelin czasowych dotyczy łącz z czasową multipleksacją kanałów (TDMA) i polega na transmisji kilku kanałów informacyjnych jednym łączem, gdzie każdy z kanałów jest transmitowany w przypisanej mu przerwie czasowej (time slot) w sposób sekwencyjny.

Ten sposób transmisji danych serwisowych nie wymaga żadnej dodatkowej infrastruktury ze strony użytkownika końcowego, za wyjątkiem sytuacji, kiedy nie ma zasięgu sieci telefonii komórkowej w miejscu pracy instalacji. W takim przypadku może zajść potrzeba instalacji anten o większej sprawności i lepszej lokalizacji.

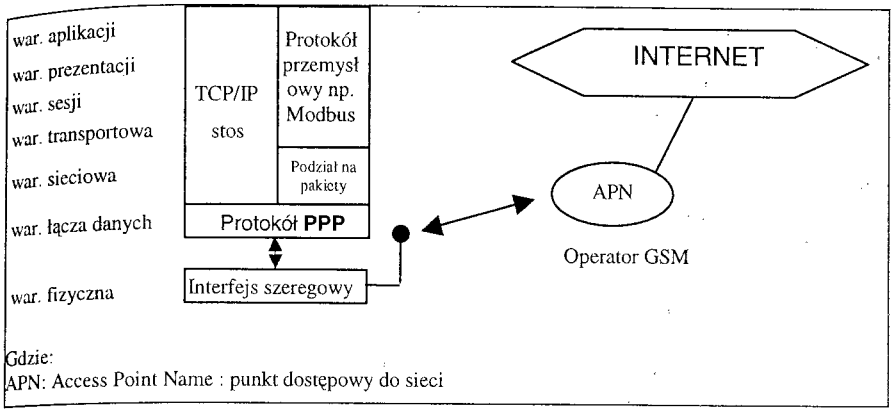
Problem sterowania przepływem danych na łączu RS jest identyczny jak dla transmisji komutowanym łączem PSTN. Także koszt połączenia naliczany jest w funkcji czasu.

## 2.4. Transmisja GPRS

To najnowszy tryb transmisji dostępny w sieciach telefonii komórkowej, polegający na tym, że dane użytkownika są dzielone na pakiety i przesyłane w kanale transmisyjnym (w rzeczywistości składającym się z 8 szczelin czasowych), do którego użytkownik ma stały, lecz nie wyłączny dostęp. Pozwala to na efektywniejsze wykorzystanie łącza i naliczanie przez operatora opłat w funkcji ilość przesłanych danych.

Usługa ta jest zoptymalizowana dla użytkowników mobilnych korzystających głównie z zasobów stacjonarnych sieci Internet. Powoduje to, że poza wymienionymi powyżej zaletami ma niestety dość poważne wady w przypadku stosowania jej do aplikacji serwisowych.

Pierwsze z tych ograniczeń spowodowane jest przez protokół wymagany na wejściu do modułu GSM. W odróżnieniu od transmisji komutowanych, gdzie łącze jest teoretycznie „przezroczyste" dla protokołów łącza szeregowego, w tym przypadku na wejściu do modułu dane muszą być dostarczane w formacie zgodnym z protokołem PPP (Point to Point Protocol). Zilustrowano to na rys. 4. W związku z tym, że nie jest znane autorom żadne urządzenie przemysłowe dysponujące w chwili obecnej tą opcją wymagane jest zastosowanie dodatkowego, zewnętrznego konwertera protokołu szeregowego na protokół pakietowy . Konwerter ten dokonuje enkapsulacji ramek protokołu łącza szeregowego w pakietach protokołu PPP.




Rys. 4. Protokół PPP w transmisji GPRS

Następną przeszkodą jest problem związany z odpowiednim przydzieleniem adresu IP. Jak już wspomniano, standardowa usługa GPRS służy głównie do łączenia się z zasobami stacjonarnymi sieci Internet przez użytkowników mobilnych. Konsekwencją tego jest dynamiczne przydzielanie adresów IP dla abonamentów tej usługi. W przypadku aplikacji serwisowych nie ma zatem możliwości wywołania urządzenia oddalonego ponieważ, nie wiadomo jaki adres IP jest mu przydzielony w danej chwili.

Rozwiązaniem jest uzyskanie od operatora stałego adresu IP, lecz obecnie procedura ta jest dość skomplikowana, ponieważ polityka operatorów sieci komórkowych nie przewiduje tego typu rozwiązań dla użytkowników indywidualnych.

Wyżej wymienione cechy czynią to rozwiązanie komunikacyjne mało przydatnym do aplikacji serwisowych, gdzie przeważnie sesje transmisji prowadzone są okazjonalnie i krótkotrwale.

## 3.WNIOSKI

Z przedstawionych w pracy rozważań wynika, że aplikacje serwisowe mają szczególne wymagania odnośnie kanału teletransmisji, które nie zawsze wpisują się w ogólne kierunki rozwoju teleinformatyki. Chodzi tutaj głównie o zapewnienie „przezroczystości" łącza, zminimalizowaną zależność od użytkownika końcowego (w sensie wykorzystywania jego infrastruktury), oraz wymaganie łatwości integracji z istniejącymi na rynku komponentami systemów pomiarowych i automatyki.

Doskonałym przykładem tego jest bezprzewodowa transmisja GPRS w sieci GSM – przełomowy krok w technologii tego typu usług, lecz niestety trudno integrowalna z urządzeniami przemysłowymi.

Należy pamiętać o tym, że systemy przemysłowe ewoluują także pod względem możliwości komunikacyjnych. W porównaniu z teleinformatyką jest to jednak proces znacznie wolniejszy, lecz naturalny dla branży, gdzie czas życia sprzętu jest kilkukrotnie

dłuższy niż w dziedzinie IT. Dlatego wymagane przepustowości kanałów transmisji danych również pozostają na relatywnie stabilnym poziomie, co wynika z typu transmitowanych informacji.

W zakresie kierunków tej ewolucji pewność można mieć co do standardu dostępu do łącza danych ethernet i protokołu IP, które niewątpliwie zastąpią dominujące jeszcze dziś łącza szeregowe.

Zaskakujący jest wniosek, że w chwili obecnej najlepsze do celów serwisowych są łącza komutowane (GSM i PSTN).

Wynik przeprowadzonej dyskusji można sprowadzić do następujących, praktycznych wytycznych:

Gdy potrzebny zdalny serwis niezależny od użytkownika końcowego (lub dodatkowa infrastruktura niemożliwa) należy zastosować transmisje bezprzewodową GSM:

– Komutowaną : gdy wymagane jest zapewnienie możliwości modyfikacji oprogramowania systemu, pobrania danych archiwalnych lub monitoringu systemu „w danej chwili"

– GPRS: wyłącznie gdy niezbędne jest zbieranie danych w czasie rzeczywistym.

Warunkiem dodatkowym (w większości przypadków trudny do osiągnięcia) są odpowiednie możliwości komunikacyjne komponentów systemu ( np. PLC)– zaimplementowany protokół PPP oraz „publiczne" adresy IP dla terminali .

Gdy użytkownik dysponuje jedynie podstawową infrastrukturą (sieć telefoniczna) należy zastosować telefoniczną linię komutowaną – zwłaszcza gdy wymagany jest dostęp do pojedynczego urządzenia.

Gdy użytkownik dysponuje odpowiednią infrastrukturą i jest możliwa jej dodatkowa konfiguracja można pozwolić sobie na nieograniczony dostęp poprzez sieć Internet do wszystkich komponentów systemu posiadających interfejs ethernet i zaimplementowany protokół IP. Należy jednak pamiętać o zapewnieniu stałego IP dla urządzenia serwisowanego.

Dla każdego z omawianych metod teletransmisji można zastosować oprogramowanie typu zdalny terminal. Warunkiem jest skonfigurowanie nadrzędnej stacji PC w roli bramy pomiędzy podsiecią serwisowanego układu, a stacja serwisową.

## 4. LITERATURA


[1] T. Parker, M. Sportack „TCP/IP Księga eksperta", Helion 2000

[2] R. Szewczyk, W. Winiarski „Nadzór sieci rurociągowej przy pomocy telefonii komórkowej GSM" Rurociągi 4/2001, str. 35-36

[3] Materiały techniczne firmy Cisco : www.cisco.com

[4] W. Mielczarek „Szeregowe interjejsy cyfrowe", Helion 1993