STUDIA INFORMATICA 2001
Volume 22 Number 3 (45)

Rafal CUPEK
Politechnika Śląska, Instytut Informatyki

PROTOKÓŁ TCP/IP W SYSTEMACH WIZUALIZACJI PROCESÓW PRZEMYSŁOWYCH

Streszczenie. W pracy poruszono problematykę wykorzystania sieci opartych na protokole TCP/IP w przemysłowych systemach sterowania i wizualizacji. Opisano zastosowanie protokołu TCP/IP w sieciach przemysłowych w kontekście integracji instalacji automatyki przemysłowej z sieciami rozległymi. Omówiono także zagadnienia związane z bezpieczeństwem tych systemów, które powinny zostać uwzględnione w procesie integracji.

THE TCP/IP PROTOCOL IN INDUSTRIAL VISUALISATION SYSTEMS

Summary. This paper describes some problems of using TCP/IP network protocol in industrial control and visualization systems. Industry networks with TCP/IP and methods of their interconnections with Wide Area Networks are described. Problems of security level during interconnection are also showed.

1. Wstęp

Dynamiczny wzrost popularności protokołu TCP/IP dokonuje się niewątpliwie za sprawą rozrastającej się w wykładniczym tempie globalnej sieci Internet. Protokół ten coraz częściej znajduje zastosowanie także w innych obszarach związanych z wymianą informacji. Wzrost zainteresowania możliwościami protokołu TCP/IP nie ominął także dziedziny informatyki przemysłowej. W tym jednym z bardziej zachowawczych obszarów zastosowań informatyki obserwuje się coraz częstsze próby wykorzystywania protokołu TCP/IP. Protokół ten w połączeniu ze znanymi i sprawdzonymi standardami, jak np.: protokołami FIP, PROFIBUS, MAP, czy MODBUS zaczyna być coraz chętniej wykorzystywany w rozwiązaniach sieci przemysłowych.

Zdobywanie przez protokół TCP/IP nowych obszarów zastosowań powodowane jest z jednej strony przez powszechną dostępność tego standardu. Nie bez znaczenia są czynniki ekonomiczne, do jakich należy brak opłat licencyjnych związanych z jego wykorzystywaniem oraz dostępność rozwiązań sprzętowo-programowych dla tego protokołu. Z drugiej strony systemy automatyki przemysłowej zaczynają tracić swoją pierwotną hermetyczność. Początkowo systemy te zamykały się w obrębie jednego bądź kilku segmentów sieci przemysłowych. Na tym poziomie konstruowane były stacje kontrolno-nadzorcze klasy SCADA (ang. Supervisory Control and Data Acquisition). W części zastosowań stacje te współpracowały z równie hermetycznymi systemami typu MES (ang. Manufacturing Execution System) czy systemami ERP (ang. Enterprise Resources Planning). Dominująca dzisiaj - także z pobudek ekonomicznych - potrzeba otwarcia się na świat, stymulowana przez rozwijającą się dynamicznie e-gospodarkę sprawiła, iż również od hermetycznych dotychczas przemysłowych systemów wizualizacji i sterowania wymaga się w mniejszym bądź szerszym zakresie współpracy z globalną siecią Internet.

Wymienione powyżej niewątpliwe zalety protokołu TCP/IP nie przesądzają jednak o możliwości jego bezkrytycznego stosowania jako uniwersalnego środka, zdolnego zaspokoić wymagania każdej instalacji automatyki przemysłowej. Wykorzystywanie w sieciach przemysłowych protokołu TCP/IP, jak również integracja tych systemów z sieciami rozległymi i siecią Internet, pociągają za sobą szereg nowych, nie występujących w rozwiązaniach stosowanych dotychczas zjawisk. Podobnie jak w przypadku każdego innego narzędzia, również w dziedzinie systemów automatyki przemysłowej o powodzeniu wykorzystania protokołu TCP/IP decydować będzie tak sposób jego użycia, jak i świadomość związanych z jego zastosowaniem skutków ubocznych. To od właściwej architektury systemów przemysłowych wykorzystujących mechanizm TCP/IP zależeć będą zarówno ich funkcjonalność i efektywność, jak i bezpieczeństwo obsługiwanych przez nie instalacji. Niniejszy artykuł stanowi próbę spojrzenia na zagadnienie zastosowania stosu protokołów TCP/IP w systemach automatyki przemysłowej dokonaną poprzez pryzmat rozproszonych systemów wizualizacji i sterowania.

2. Hierarchiczna struktura systemów wizualizacji i sterowania

Postęp w zakresie konstrukcji urządzeń mikroprocesorowych umożliwił powszechne wykorzystywanie tych układów w przemysłowych systemach sterowania. Współczesne instalacje automatyki przemysłowej buduje się coraz częściej opierając się na zasadzie rozpraszania funkcji urządzeń automatyki i wiązania ich z poszczególnymi elementami kontrolowanego procesu. Podejście takie wymaga stosowania coraz sprawniejszych sieci

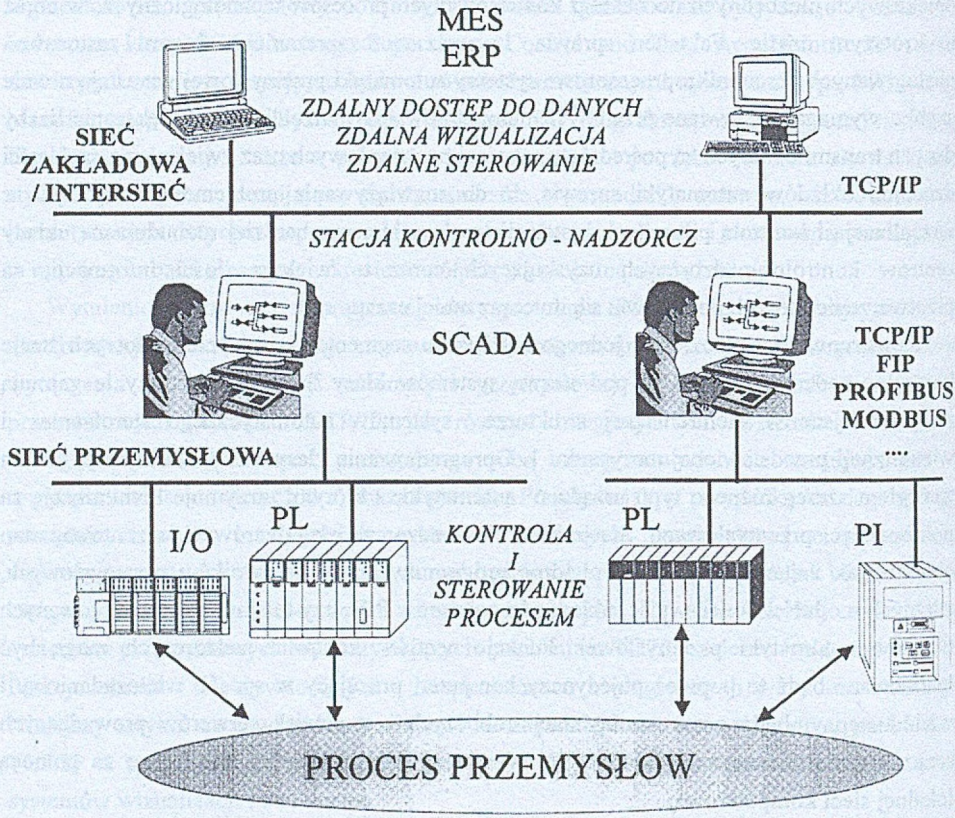
przemysłowych zapewniających wymianę informacji pomiędzy rosnącą liczbą abonentów rozmieszczanych na terenie obsługiwanego obiektu. Rozproszone terytorialnie instalacje automatyki przemysłowej wymagają również sprawnych i skutecznych systemów umożliwiających tak wizualizację, jak i sterowanie pracą kontrolowanych przez nie urządzeń.

Systemy sterowania i wizualizacji muszą przetwarzać coraz to większą liczbę sygnałów obiektowych niezbędnych do obsługi kontrolowanych procesów technologicznych, w coraz to krótszym czasie. Fakt ten sprawia, iż wraz z rozszerzaniem obszaru zastosowań obsługiwanych przez mikroprocesorowe systemy automatyki przemysłowej wzrastają równie szybko wymagania stawiane przed systemami sterowania i wizualizacji. Zwiększanie liczby danych transmitowanych za pośrednictwem sieci przemysłowych oraz zwiększanie szybkości działania układów automatyki sprawia, iż do rozwiązywania problemów związanych z wizualizacją i kontrolą pracy tych instalacji tworzy się coraz bardziej rozbudowane układy centrów kontrolno-nadzorczych uzyskujących coraz to większe ilości informacji, na przetworzenie których pozostawia się im coraz mniej czasu.

Konstruowane na poziomie jednego bądź kilku segmentów sieci przemysłowych stacje kontrolno-nadzorcze znane są pod nazwą systemów klasy SCADA. Systemy te zajmują ważne miejsce w hierarchicznej strukturze systemów automatycznego sterowania i wizualizacji przedstawionej na rysunku 1. Oprogramowanie klasy SCADA obejmuje swoim zasięgiem szereg różnego typu urządzeń automatyki, z którymi utrzymuje komunikację za pomocą sieci przemysłowych. Stacje kontrolno-nadzorcze mogą zarówno prezentować stan obiektu, jak i sterować pracą swobodnie programowalnych sterowników przemysłowych, zdalnych modułów wejść-wyjść, układów regulatorów PID, czy też innych specjalizowanych układów automatyki przemysłowej. Funkcje centrów kontrolno-nadzorczych mogą być realizowane bądź to poprzez pojedynczy komputer, pracujący w sposób wielozadaniowy i wielodostępny, bądź przez szereg stacji roboczych i stanowisk serwerów prowadzących rozproszone przetwarzanie informacji i wymieniających pomiędzy sobą dane za pomocą lokalnej sieci komputerowej.

Stacje kontrolno-nadzorcze pełnią często funkcję urządzeń pośredniczących (ang. Interconnection Device) pozwalając na dostęp do danych opisujących w sposób kompleksowy pracę większej instalacji lub nawet całego zakładu przemysłowego z poziomu sieci zakładowej bądź też sieci rozległej. Poziom ten wymaga uwzględnienia zagadnień związanych ze współpracą różnych układów technologicznych, realizację wymiany informacji pomiędzy poszczególnymi oddziałami czy też filiami przedsiębiorstwa. Na podstawie danych dotyczących bieżącej produkcji, stanu magazynów oraz wpływających zamówień na wyroby istnieje możliwość optymalnego zarządzania zarówno pracą poszczególnych oddziałów, jak i całego zakładu przemysłowego.

Wymienione powyżej zadania są realizowane za pomocą oprogramowania Systemów Zarządzania Produkcją, zwanych także systemami typu MES. Informacje dostarczane na temat procesu mogą być dalej wykorzystywane poprzez oprogramowanie systemów baz danych, programy technicznego przygotowania produkcji TPP, czy też programy zarządzania przedsiębiorstwem ERP.



Rys. 1. Hierarchiczna struktura systemów wizualizacji i sterowania
Fig. 1. Hierarchy structure of visualization and control systems

W tak skonstruowanej hierarchicznej strukturze rozproszonego systemu automatyki przemysłowej stacja kontrolno-nadzorcza zajmuje bardzo ważne miejsce łącząc poziom sieci przemysłowych z poziomem sieci zakładowej oraz z poziomem sieci rozległych. Zarówno na poziomie sieci przemysłowej, jak i na poziomie sieci rozległej coraz powszechniej wykorzystuje się protokół TCP/IP. Szereg funkcji związanych tak z wizualizacją, jak i sterowaniem obiektem udostępnianych jest w sposób zdalny, wliczając w to dostęp poprzez

sieć Internet. W związku z tym, iż zarówno w sieciach przemysłowych, jak i w sieciach rozległych wykorzystuje się standard protokołu TCP/IP, nasuwa się pytanie, czy funkcje urządzenia pośredniczącego realizowane dotychczas przez stację kontrolno-nadzorczą mogą zostać zastąpione prostymi funkcjami rutowania w sieciach TCP/IP bądź też czy funkcje te mogą zostać wyodrębnione ze stacji kontrolno-nadzorczej i przekazane w całości do ruterów IP?

W niniejszym artykule zaprezentowane zostaną argumenty wykazujące, iż zastosowanie rozwiązania opartego wyłącznie na mechanizmach protokołu TCP/IP, pomimo iż jest ono z technicznego punktu widzenia możliwe do zrealizowania, to w przypadku instalacji automatyki przemysłowej stanowić może poważne zagrożenie dla bezpieczeństwa całej instalacji. Wymagania niezawodnościowe, wymagania związane z determinizmem czasowym, jak i konieczność ścisłej kontroli dostępu do instalacji przemysłowych w sposób zdecydowany dyskwalifikuje takie podejście. Z drugiej strony wymagania stawiane przed współcześnie realizowanymi systemami wizualizacji i sterowania sprawiają, iż nie da się uniknąć ich integracji z sieciami rozległymi, w tym również z siecią Internet. Autor postara się pokazać, iż odpowiednio skonstruowane oprogramowanie stacji kontrolno-nadzorczej jest w stanie zapewnić bezpieczną wymianę informacji pomiędzy poziomem sieci przemysłowych i poziomem sieci rozległych. Ponadto postara się on zaprezentować korzyści wynikające z takiej właśnie architektury, które wpływają na podniesienie właściwości funkcjonalnych tworzonych na jej bazie systemów wizualizacji i sterowania.

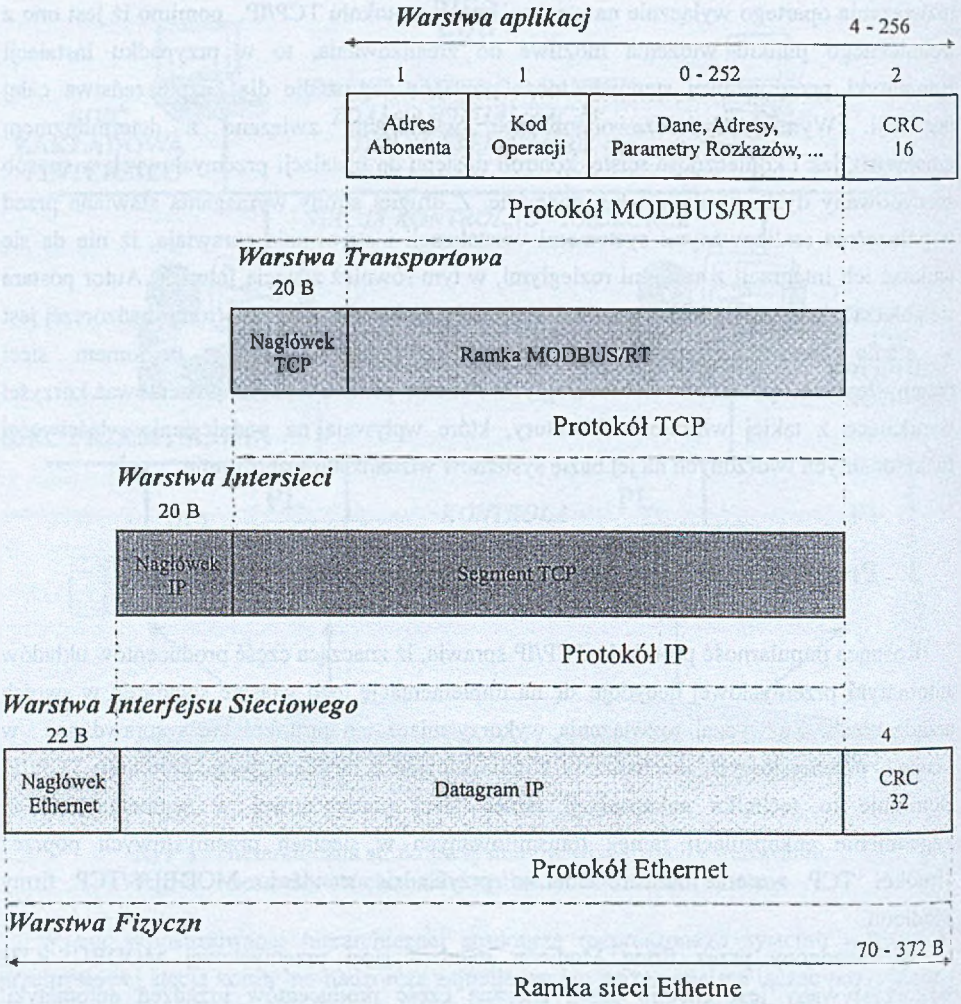
3. Protokół TCP/IP w sieciach przemysłowych

Rosnąca popularność protokołu TCP/IP sprawia, iż znacząca część producentów układów automatyki przemysłowej decyduje się na implementację tego właśnie standardu w swoich urządzeniach. Zazwyczaj rozwiązania wykorzystujące ten protokół łączą sprawdzone w sieciach przemysłowych mechanizmy komunikacyjne z mechanizmami protokołu TCP/IP. Dominuje tu technika enkapsulacji ramek sieci przemysłowej w segmentach TCP. Zagadnienie enkapsulacji ramek transmitowanych w sieciach przemysłowych poprzez protokół TCP zostanie zilustrowane na przykładzie standardu MODBUS/TCP firmy Modicon.

Wprowadzony przez firmę Modicon standard sieci przemysłowej MODBUS/RTU wykorzystywany jest chętnie przez znaczną część producentów urządzeń automatyki. Standard ten zakłada realizację sieci o architekturze Master – Slave. W każdym segmencie sieci przemysłowej MODBUS wyróżnia się jednego abonenta nadrzędnego – urządzenie Master i od jednego do 255 abonentów podrzędnych - urządzenia Slave. O czasie i rodzaju

transmisji realizowanych w sieci decyduje w sposób arbitralny urządzenie Master, które wysyła do poszczególnych abonentów Slave ramki zawierające dane lub zapytania. Rola abonentów Slave ogranicza się do udzielania odpowiedzi na żądania wysyłane poprzez Mastera sieci. Długość ramki w sieci MODBUS została ograniczona do 256 bajtów.

Proponowane przez firmę Modicon rozwiązanie MODBUS/TCP zakłada kapsułkowanie ramek zgodnych ze standardem MODBUS/RTU w segmencie TCP. Schemat, według którego realizowana jest wielostopniowa enkapsulacja, został przedstawiony na rysunku 2.



Rys. 2. Mechanizm enkapsulacji stosowany w sieci MODBUS/TCP
Fig. 2. Encapsulation in MODBUS/RTU network

Na poziomie warstwy aplikacji oprogramowanie odpowiedzialne za obsługę protokołu MODBUS generuje ramki zgodne ze standardem MODBUS/RTU. Po usunięciu z ramki sumy kontrolnej CRC 16 pozostała część kapsułkowana jest w segmencie TCP. Segmenty TCP, zgodnie z warstwową budową stosu protokołów TCP/IP, kapsułkowane są na poziomie Intersieci w datagramy IP. Datagramy IP na poziomie interfejsu sieciowego kapsułkowane są w ramki sieci Ethernet. Warstwa sprzętu zapewnia dostarczenie ramki do adresata. Oprogramowanie komunikacyjne po stronie odbiorcy realizuje odwrotną procedurę. Ramka sieci Ethernet poprzez datagram IP i segment TCP doprowadzana jest do postaci zgodnej ze standardem MODBUS/RTU.

Opisane powyżej rozwiązanie techniczne podyktowane zostało względami natury ekonomicznej. Z jednej strony istnieje możliwość wykorzystania istniejącego sprzętu i oprogramowania stosowanego przez systemy automatyki przemysłowej, które często wyposażone były w interfejs MODBUS/RTU, uzupełnieniu podlegają jedynie elementy sprzętowe i moduły programowe zajmujące się kapsułkowaniem ramek sieci MODBUS transmisją w sieci Ethernet. Z drugiej strony oparcie się na dwóch dobrze sprawdzonych i powszechnie znanych protokołach pozwoliło na uniknięcie czasochłonnych i kosztownych badań nad nowym protokołem sieci przemysłowej.

Do wad powyższego rozwiązania należy zaliczyć narzut czasowy związany z konwersją ramki sieci MODBUS, której struktura oraz realizowane funkcje odpowiadają drugiej warstwie w modelu OSI/ISO – warstwie łącza danych. Ramka ta przenoszona jest w górę na poziom warstwy aplikacji i stamtąd poprzez warstwą transportową i warstwę intersieci przekazywana jest do warstwy interfejsu sieciowego. Związany z operacją enkapsulacji narzut staje się widoczny jeszcze bardziej w przypadku analizy długości danych wymienianych pomiędzy poszczególnymi warstwami. O ile długość ramki definiowanej przez standard MODBUS/RTU wynosi w zależności od przesyłanej treści od 4 (np. odczyt pojedynczego bajtu) do 256 bajtów, to wartości te po przejściu poprzez kolejne poziomy kapsułkowania wynosić będą odpowiednio 22 – 274 bajty dla segmentu TCP, 42 – 294 bajty dla datagramu IP i 70 – 372 bajty dla ramki Ethernet.

Pomimo tak znacznych narzutów, wynoszących w przypadku krótkich ramek ponad 1000% ich pierwotnej długości, opisane rozwiązanie cieszy się ciągle wzrastająca popularnością, a wymienione wady kompensowane są znaczną różnicą w szybkości transmisji informacji przez warstwę fizyczną występującą pomiędzy standardem RS485/422/232C a standardem Ethernet 10/100.

Nie we wszystkich rozwiązaniach wykorzystanie protokołu TCP/IP wymaga cofnięcia się z poziomu ramki sieci przemysłowej na poziom aplikacji zlecającej usługi warstwie transportowej protokołu TCP. Przykładem innej architektury może być standard sieci MAP. Sieć zaprojektowano opierając się na siedmiowarstwowym modelu OSI/ISO. Rozwiązanie to

zakładało połączenie warstwy sesji z niższymi warstwami oprogramowania komunikacyjnego za pomocą mechanizmów zdalnego wywołania procedur RPC (ang. Remote Procedure Call). W przypadku realizacji sieci MAP/TCP mechanizm RPC został wykorzystany do komunikacji pomiędzy warstwą sesji protokołu MAP a warstwą transportową protokołu TCP. Rozwiązanie takie pozwoliło na uniknięcie konieczności enkapsulacji ramek na najniższym poziomie.

Osobnym zagadnieniem jest problem determinizmu czasowego stającego u podstaw konstrukcji wszystkich sieci przemysłowych. Zapewniający usługę przesyłania niezawodnymi strumieniami protokół TCP opiera się na pracującym zgodnie z zasadą przenoszenia w ramach dostępnych możliwości protokole IP. Kolejna warstwa bazuje na nie dającym żadnych gwarancji co do czasu realizacji usługi, rywalizacyjnym algorytmie CSMA/CD, będącym podstawą funkcjonowania sieci Ethernet. Zagadnienia związane z determinizmem czasowym w sieciach przemysłowych wykorzystujących protokół TCP/IP są więc dosyć złożone. Odmiennie niż występuje to w przypadku klasycznych rozwiązań sieci przemysłowych, w rozwiązaniach opartych na protokole TCP/IP bezpieczeństwo sieci zależy od wyższych warstw oprogramowania komunikacyjnego. Niniejszy artykuł nie stawia sobie za cel przeprowadzenie pełnej analizy czasowej stosowanych w przemyśle sieci TCP/IP, lecz ma on za zadanie dyskusję zjawisk zachodzących podczas integracji systemów automatyki przemysłowej z sieciami rozległymi. Próba odniesienia się do opisanych powyżej problemów przeprowadzona poprzez pryzmat stacji kontrolno-nadzorczej została zawarta w rozdziale czwartym.

4. Metody wymiany informacji w rozproszonych systemach sterowania i wizualizacji

Prezentowana w rozdziale drugim hierarchiczna struktura systemu automatyki przemysłowej rozdziela na poziomie stacji kontrolno-nadzorczej funkcje związane z przekazywaniem informacji związanych bezpośrednio z wymianą danych pomiędzy poszczególnymi urządzeniami automatyki przemysłowej od informacji wymienianych poprzez sieć zakładową i sieć rozległą służących do zdalnej wizualizacji i kontroli obsługiwanego procesu. Pierwsze z tych zadań realizowane jest poprzez poziome wymiany danych, drugie zadanie realizują wymiany pionowe. Wydawać by się mogło, iż implementacja w sieciach rozległych i w sieciach przemysłowych tych samych protokołów komunikacyjnych, ba, nawet tych samych rozwiązań sprzętowych, umożliwi bezpośrednie połączenie urządzeń automatyki z poziomem sieci rozległej. W takim przypadku poszczególne urządzenia stawałyby się wprost abonentami Internetu, pozwalając tym samym

na zdalny dostęp do danych z dowolnego punktu na świecie. Chociaż przedstawiona powyżej optymistyczna wizja wydaje się bardzo kusząca, a bezpośrednie połączenie poszczególnych urządzeń do Intersieci jest z technicznego punktu widzenia dosyć proste do zrealizowania, to jednak rozwiązanie powyższe w zdecydowanej większości przypadków nie nadaje się do zastosowania.

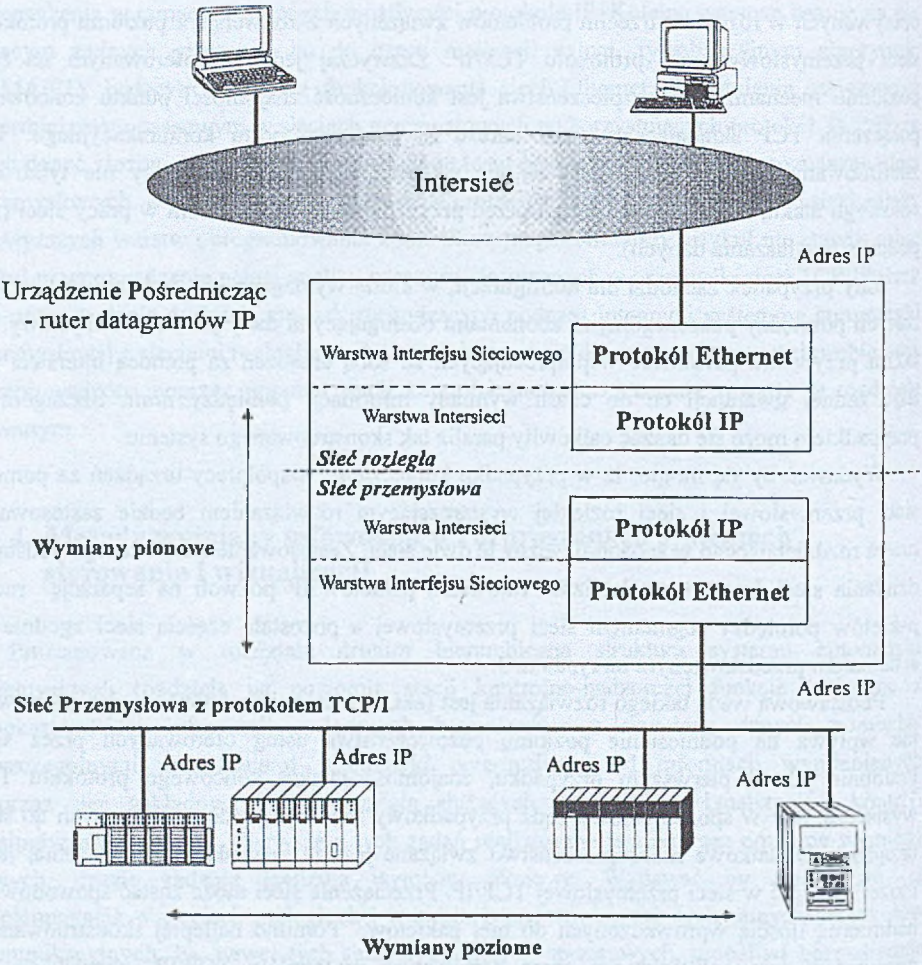
Podstawową przyczyną dyskredytującą powyższy schemat jest brak mechanizmów zapewniających bezpieczeństwo na poziomie właściwym dla urządzeń automatyki przemysłowej. Stan taki powodowany jest nie tylko niedoskonałością algorytmów warstwy aplikacyjnej stosowanych w konstruowanych urządzeniach, ale wynika on wprost z opisywanych w rozdziale trzecim problemów związanych z konwersją z poziomu protokołu sieci przemysłowych do protokołu TCP/IP. Zazwyczaj jedynym oferowanym na tym poziomie mechanizmem bezpieczeństwa jest konieczność znajomości punktu końcowego połączenia TCP składającego się z adresu IP i numeru portu komunikacyjnego. Tak zdefiniowany poziom bezpieczeństwa nie stanowi wystarczającej bariery nie tylko dla celowego ataku, ale nawet nie chroni przed przypadkowym zaburzeniem w pracy sieci (np. podczas rozgłaszania danych).

Inny przypadek zachodzi dla konfiguracji, w której wymagana jest dodatkowa wymiana danych pomiędzy poszczególnymi abonentami obsługującymi dany proces przemysłowy. W takim przypadku połączenie współpracujących ze sobą urządzeń za pomocą Intersieci nie daje żadnej gwarancji co do czasu wymiany informacji pomiędzy nimi. Szczególnym przypadkiem może się okazać całkowity paraliż tak skonstruowanego systemu.

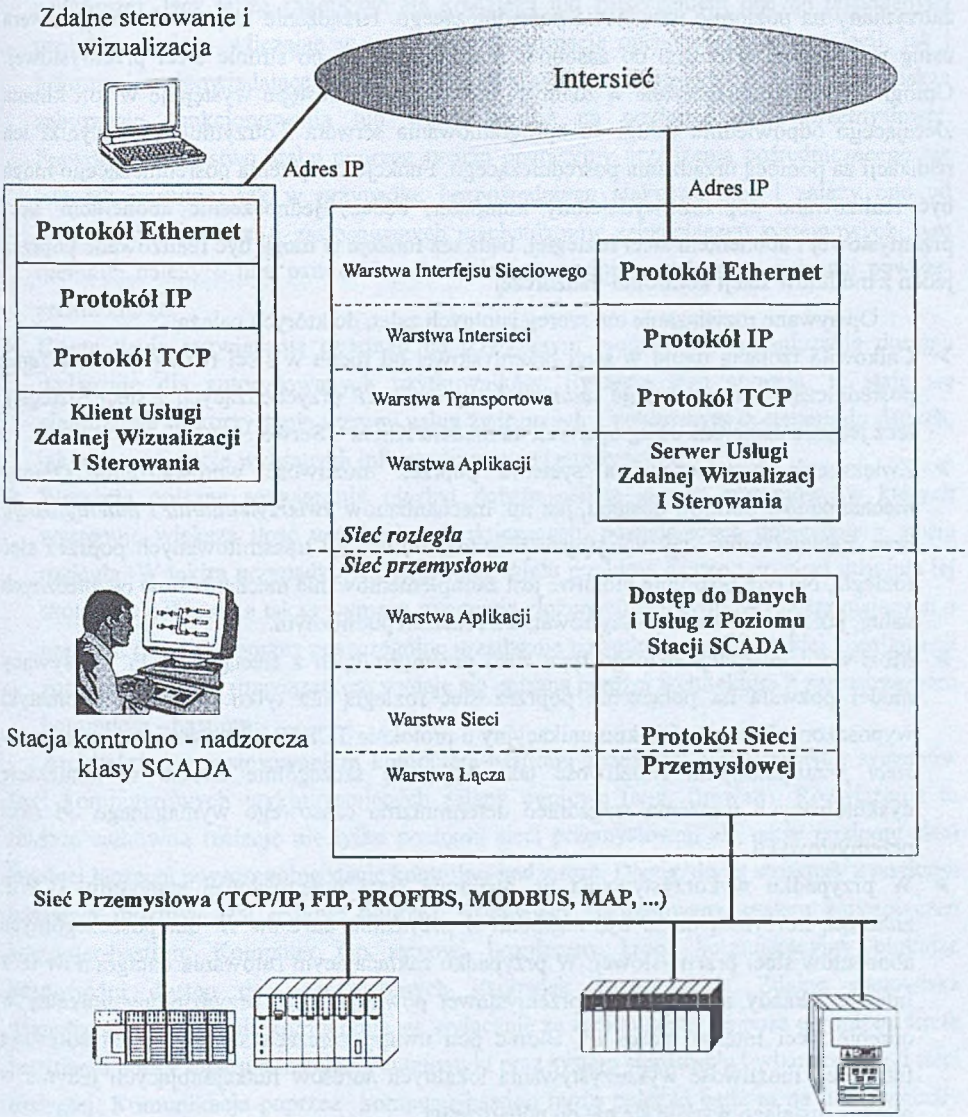
Wydawać by się mogło, iż w przypadku konieczności współpracy urządzeń za pomocą sieci przemysłowej i sieci rozległej wystarczającym rozwiązaniem będzie zastosowanie rutera rozdzielającego w sposób fizyczny te dwie sieci. Zastosowanie stanowiącego podstawę działania sieci Internet mechanizmu rutowania pakietów IP pozwoli na separację ruchu pakietów pomiędzy segmentem sieci przemysłowej a pozostałą częścią sieci zgodnie ze schematem przedstawionym na rysunku 3.

Podstawową wadą takiego rozwiązania jest fakt, iż mechanizm rutowania datagramów IP nie wpływa na podniesienie poziomu bezpieczeństwa usług oferowanych przez sieć. Podobnie jak w pierwszym przypadku, znajomość punktu końcowego protokołu TCP wystarcza, aby w sposób celowy bądź przypadkowy zaburzyć pracę podłączonych do sieci urządzeń. Dodatkowe niebezpieczeństwo związane jest ze zjawiskiem przeciążenia, jakie może wystąpić w sieci przemysłowej TCP/IP. Przeciążenie sieci może zostać spowodowane nadmierną ilością wprowadzonych do niej pakietów. Pomimo najlepiej skonstruowanego oprogramowania aplikacyjnego sama architektura protokołów TCP/IP, pozwalająca na kolejkowanie, powielanie i transport różnymi trasami datagramów IP, nie pozwala na wykluczenie sytuacji (co więcej, jest ona w przypadku przeciążenia sieci rozległej wysoce

prawdopodobna), w której ruter łączący tą sieć z siecią przemysłową stanie przed zadaniem wprowadzenia w krótkim czasie znacznej ilości datagramów IP do sieci przemysłowej, zwiększając tym samym liczbę kolizji w sieci Ethernet. Sytuacja ta spowoduje wzrost obciążenia sieci przemysłowej. Wzrost ten, zgodnie z teorią kolejkowania, spowoduje zmianę wariacji czasu podróży pakietu q=1/(1-L), gdzie L oznacza współczynnik aktualnego obciążenia sieci (0 □ L □ 1), czyniąc tym samym niemożliwym do wyznaczenia maksymalny czas dostępu do łącza dla abonentów sieci przemysłowej. Stan taki leży w oczywistej sprzeczności z zasadą determinizmu czasowego, stawianą u podstaw konstrukcji sieci przemysłowych.



Rys. 3. Separacja sieci przemysłowej poprzez ruting IP
Fig. 3. Separation using IP routing



Rys. 4. Separacja sieci przemysłowej na poziomie stacji SCADA
Fig. 4. Industrial network separation on SCADA level

Alternatywą dla rozwiązania z rutingiem IP może być zastosowanie separacji sieci przemysłowej od sieci rozległej na poziomie warstwy aplikacji. Przedstawiona na rysunku 4 konfiguracja zakłada całkowitą izolację tych dwóch rodzajów sieci na poziomie aplikacji urządzenia pośredniczącego. Jakikolwiek ruch przychodzący z sieci rozległej zostaje

zatrzymany na poziomie urządzenia pośredniczącego. Urządzenie to pełni funkcję serwera usług pozwalając na dostęp do zasobów znajdujących się po stronie sieci przemysłowej. Oprogramowanie umieszczone w zdalnych stanowiskach dostępu występuje w roli klienta zlecającego odpowiednie usługi do oprogramowania serwera i otrzymującego wyniki ich realizacji za pomocą urządzenia pośredniczącego. Funkcje urządzenia pośredniczącego mogą być realizowane poprzez wydzielony komputer, będący jednocześnie abonentem sieci przemysłowej i abonentem sieci rozległej, bądź też funkcje te mogą być realizowane poprzez jeden z modułów stacji kontrolno-nadzorczej.

Opisywane rozwiązanie ma szereg istotnych zalet, do których należą:

- Całkowita izolacja ruchu w sieci przemysłowej od ruchu w sieci rozległej. Urządzenie pośredniczące nie przekazuje *żadnych datagramów IP* przychodzących z sieci rozległej, lecz jedynie dostarcza usług opartych na modelu Klient – Serwer.
- Zwiększenie bezpieczeństwa systemu poprzez możliwość wprowadzenia szeregu mechanizmów kontroli dostępu, jak np. mechanizmów *uwierzytelniania i autentyfikacji*, oraz mechanizmów zapewniających *poufność informacji* transmitowanych poprzez sieć rozległą. Na tym poziomie możliwe jest zaimplementowanie mechanizmów bezpiecznych usług, jak np. mechanizmu szyfrowania z kluczem publicznym.
- Możliwość integracji różnego typu sieci przemysłowych z siecią rozległą. Opisywany model pozwala na połączenie poprzez sieć rozległą nie tylko urządzeń automatyki wyposażonych w interfejs komunikacyjny o protokole TCP/IP, ale również *innych* typów *sieci przemysłowych*. Możliwość taka staje się szczególnie istotna w kontekście dyskutowanych wcześniej zagadnień determinizmu czasowego wymaganego od sieci przemysłowych.
- W przypadku wykorzystywania na poziomie sieci przemysłowej standardu TCP/IP znaczącą korzyścią może być *swoboda w przydziale adresów IP* dla poszczególnych abonentów sieci przemysłowej. W przypadku zakładającym rutowanie datagramów IP z Intersieci każdy abonent sieci przemysłowej powinien mieć przydzielony unikalny w obrębie sieci Internet adres IP. Biorąc pod uwagę kurczącą się przestrzeń adresową Intersieci, możliwość wykorzystywania lokalnych adresów funkcjonujących jedynie w obrębie instalacji wydaje się nie do pogardzenia.

Powyższe rozwiązanie ma również swoje wady:

- Najpoważniejszą z punktu widzenia bezpieczeństwa wadą jest możliwość ataku na sieć wewnętrzną poprzez wykorzystanie błędów systemu operacyjnego kontrolującego pracę urządzenia pośredniczącego. Możliwość ta staje się szczególnie groźna w przypadku konfiguracji przedstawionej na rysunku 4, w której funkcję urządzenia pośredniczącego pełni jeden z modułów stacji kontrolno-nadzorczej. W takim przypadku atak na system operacyjny może spowodować nie tylko zaburzenie funkcjonowania stacji kontrolno-

nadzorczej, lecz także zakończyć się kradzieżą lub zniszczeniem danych posiadanych przez tą stację – wliczając w to zarówno informacje opisujące pracę instalacji, jak i informacje odpowiadające za bezpieczeństwo systemu. Przypadek ten obejmuje także zaburzenie funkcjonowania lub wręcz paraliż na poziomie sieci przemysłowej. Prawdopodobieństwo ataku poprzez system operacyjny urządzenia pośredniczącego nie jest tak wysokie, jak w przypadku bezpośredniego ataku na sieć i zależy ono od wybranych rozwiązań i zastosowanych mechanizmów zabezpieczeń systemowych, tym niemniej należy o nim pamiętać podczas konstruowania systemów o opisanej powyżej architekturze.

- Drugą wadą rozwiązania opartego na powyższym modelu jest ograniczanie dostępu wyłącznie dla autoryzowanych użytkowników. Sytuacja taka sprawia, iż staje się niemożliwe wykorzystanie szeregu usług związanych z publicznym dostępem do danych, jak np. prezentacja wybranych informacji poprzez strony www.
- Wreszcie opisane rozwiązanie niezbyt dobrze nadaje się do systemów, w których występuje większa ilość urządzeń pośredniczących, posiadających połączenie z siecią rozległą. W takim przypadku występowanie wielu punktów dostępu do sieci utrudnia jej skuteczną ochronę, a także wymaga tworzenia złożonych algorytmów rozstrzygających o prawach dostępu poprzez poszczególne urządzenia pośredniczące. Dla takiej konfiguracji znacznie lepszym rozwiązaniem wydaje się opisana poniżej architektura z zastosowaniem komputera - bastionu.

Architektura z zastosowaniem komputera-bastionu znana jest z klasycznych systemów sieci komputerowych wykorzystujących ściany ogniowe (ang. firewall). Rozwiązanie to zakłada całkowitą izolację nie tylko poziomu sieci przemysłowej, ale także poziomu sieci lokalnej łączącej poszczególne stacje kontrolno-nadzorcze. Dostęp do tej struktury z poziomu Intersieci możliwy jest jedynie poprzez posiadający rozbudowany system zabezpieczeń komputer-bastion. Komputer ten stanowi bezpieczny kanał komunikacyjny blokując bezpośredni dostęp do poszczególnych stanowisk operatorskich. Zdalne stanowiska wizualizacji i sterowania komunikują się wyłącznie ze znajdującym się poza chronioną strefą bastionem, który separuje instalację automatyki oraz system sterowania i wizualizacji od sieci rozległej. Komunikacja poprzez komputer-bastion może polegać bądź to na udostępnianiu przygotowanych na nim do prezentacji danych, np. poprzez strony www, bądź też poprzez realizację usług opartych na modelu Klient-Serwer, podobnie jak to występowało w przypadku opisanej wcześniej architektury wykorzystującej urządzenie pośredniczące.

5. Podsumowanie

Dynamiczny rozwój sieci opartych na protokole TCP/IP stymulowany wykładniczym tempem rozrastania się Internetu znalazł odzwierciedlenie również w rozwiązaniach wykorzystywanych w sieciach przemysłowych. Patrząc na instalację automatyki przemysłowej poprzez pryzmat systemów klasy SCADA współpracujących zarówno z poziomem sieci przemysłowej, jak i rozpraszających dostęp do informacji i usług za pomocą sieci rozległej (w tym też poprzez sieć Internet) należy stwierdzić, iż zastosowanie nowych rozwiązań niesie za sobą zarówno szereg korzyści, jak i nowe, nie występujące do tej pory w tych systemach automatyki przemysłowej, zagrożenia. Od właściwego zaprojektowania ogniwa łączącego poziom sieci przemysłowych z poziomem Intersieci zależy zarówno bezpieczeństwo całego systemu sterowania, jak i jego elastyczność, przejawiająca się w łatwości implementacji dostępnych dziś i pojawiających się w przyszłości nowych usług. Trwające prace nad szóstą wersją protokołu IP budzą nadzieje również w dziedzinie przemysłowych systemów wizualizacji i sterowania. Wprowadzane przez protokół IP wersja szósta wsparcie dla rezerwacji zasobów może być kluczem do tworzenia bezpiecznych kanałów komunikacyjnych zapewniających wymaganą w systemach przemysłowych gwarantowaną przepustowość i stałe opóźnienie.

Bez względu na siłę wprowadzanych nowych rozwiązań sprzętowych i możliwości wnoszonych przez nowe protokoły komunikacyjne bezpośrednia odpowiedzialność za bezpieczeństwo obsługiwanych instalacji spoczywać będzie w dalszym ciągu na oprogramowaniu aplikacyjnym kontrolującym dostęp do przemysłowych systemów wizualizacji i sterowania. Oprogramowanie stacji kontrolno-nadzorczych klasy SCADA wymaga rozwoju takich mechanizmów, które pozwolą na efektywne i bezpieczne wykorzystywanie nowych technik wprowadzanych przez protokół TCP/IP i bazującą na nim sieć Internet. Jednym z głównych zadań tego oprogramowania powinno stać się udostępnianie zasobów urządzeń automatyki w sieci rozległej z zachowaniem właściwego dla systemów informatyki przemysłowej poziomu bezpieczeństwa.

LITERATURA

1. Arvind A. i in.: A local area network architecture for communication in distributed real time systems, Real Time Systems Journal, May 1991.
2. Bernstein P.: Middleware : A model for Distributed System Services. Communication of the ACM: Computer Science in Manufacturing. V39.N2. February 1996.

3. Comer D.: Sieci komputerowe TCP/IP. WNT, Warszawa 1998.
4. Cupek R., Fojcik M.: Budowa modułów komunikacyjnych stacji nadzorczej z sieciami przemysłowymi. ZN Pol. Śl. s. Informatyka z. 32, Gliwice 1997.
5. Cupek R.: Metody hierarchizacji wizualizacji rozproszonych procesów przemysłowych. ZN Pol. Śl. s. Informatyka z. 28, Gliwice 1995.
6. FIP NETWORK General Introduction, DPS 50249 aA, Clamart 1990.
7. Gressier E.: TCP/IP Manufacturing Applications : an experiment with MMS over RPC. Materiały konferencyjne
8. Grzywak A. i in.: Rozproszone systemy komputerowe, Pronet, Gliwice 1994.
9. Grzywak A. i in.: Rozwiązania sprzętowe i programowe sieci przemysłowej FIP. ZN Pol. Śl. s. Informatyka z.30, Gliwice 1996.
10. Grzywak A.: Problemy integracji sieci komputerowych. ZN Pol. Śl. s. Informatyka z. 23, Gliwice 1993.
11. Ham A., Kumara E.: Global Collaborative Manufacturing and the World-Wide Web Integrated Design and Manufacturing in Mechanical Engineering. IDMME'96. Avril 1996. Nantes. France.
12. Klubowe materiały szkoleniowe: WorldFip, Clamart 1995, 1996, 1997, 1998.
13. Kwiecień A.: Analiza przepływu komunikatów w komputerowych sieciach przemysłowych, praca habilitacyjna, Politechnika Śląska, Gliwice 1998.
14. Torngren M.: Fundamentals of Implementing Real –Time Control Applications in Distributed Computer Systems, Journal of Real Time Systems 1996.

Recenzent: Dr inż. Włodzimierz Boroń

Wpłynęło do Redakcji 2 kwietnia 2001 r.

Abstract

The great popularity of TCP/IP protocol in computer networks has big influence on the industrial network area. Many vendors purpose TCP/IP protocol in their industrial equipment. Visualization and Control systems produce data witch may bee accessible with using Wild Area Networks and especially Internet. The SCADA systems are important part of distributing data from industrial installation add taking control commands in distributed control systems.

The security of industrial installations depends in big part on construction of visualization and control systems. Good architecture of SCADA systems may provide security distribution of new services witch can bee accessible from Wild Area Network. A few propositions of interconnection architecture for industrial control systems are showed in this paper.