

Rafał CUPEK, Piotr GAJ, Andrzej KWIECIEN
Politechnika Śląska, Instytut Informatyki

ZDALNE METODY WIZUALIZACJI PROCESÓW PRZEMYSŁOWYCH

Streszczenie. Praca dotyczy analizy usług komunikacyjnych stosowanych w sieci Internet pod kątem możliwości ich wykorzystania do zdalnej wizualizacji procesów przemysłowych, ze szczególnym uwzględnieniem wpływu doboru wykorzystywanych usług komunikacyjnych oraz przyjętych rozwiązań konstrukcyjnych na parametry systemu wizualizacji. Osobny rozdział poświęcono zagadnieniom związanym z integracją silnie zdeterminowanego w czasie systemu automatyki przemysłowej, z niezdedeterminowaną w czasie siecią Internet. W pracy opisano zarówno rozwiązania bazujące na klasycznej architekturze stacji SCADA, rozwiązania specjalizowane wykorzystujące sieć Internet wyłącznie jako medium komunikacyjne, jak i rozwiązania bazujące na otwartych mechanizmach komunikacyjnych takich jak: serwer WWW, serwer poczty elektronicznej czy serwer FTP.

Słowa kluczowe: TCP/IP, SCADA, WWW, sieci przemysłowe, Internet.

REMOTE METHODS OF INDUSTRY PROCESSES VISUALISATION

Summary. The scope of the article is the analysis of communication services in Internet network to be used in remote visualisation of industrial processes. One of the chapters describes the integration of deterministic and non-deterministic processes. The article also describes some solutions based on the classical SCADA system and on the open communication networks.

Keywords: TCP/IP, SCADA, WWW, industrial networks, Internet.

1. Wprowadzenie

Główną ideą przyświecającą twórcom sieci Internet było stworzenie heterogenicznego systemu komunikacyjnego o globalnym zasięgu. Projektowane z myślą o zastosowaniach militarnych struktury sieciowe bardzo szybko znalazły zastosowanie nieomal we wszystkich

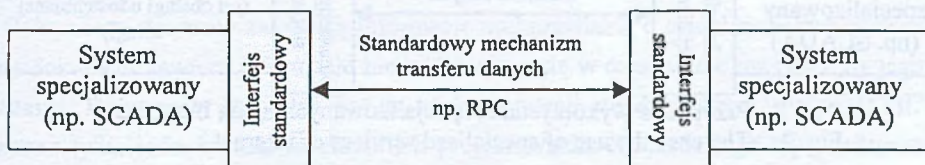
dziedzinach działalności człowieka. Również i w zakresie systemów przemysłowych wymagania związane z szybkim i mobilnym dostępem do hermetycznie zamkniętych dotychczas instalacji informatyki przemysłowej [9] sprawiły, iż w zakresie systemów wizualizacji procesów przemysłowych sieć Internet znajduje coraz to nowe zastosowania, idące w parze tak ze zwiększaniem funkcjonalności oferowanych przez nią usług, jak i ze wzrostem jej dostępności.

Jedną z podstawowych przyczyn dynamicznego rozwoju Internetu jest możliwość porozumiewania się pomiędzy heterogenicznymi systemami informatycznymi za pomocą określonego zbioru standardowych usług sieciowych niezależnych od rozwiązań sprzętowo-programowych poszczególnych elementów składowych Inter sieci [3]. Właściwość ta ma również poważny wpływ na rozwijane obecnie zastosowania sieci Internet dla potrzeb zdalnej wizualizacji przemysłowej. Szeroki wachlarz usług wprowadzanych na poziomie Internetu sprawia, iż poszczególne rozwiązania systemów zdalnej wizualizacji różnią się pomiędzy sobą nie tylko pod względem szczegółów implementacyjnych, ale również w zakresie parametrów jakościowych i funkcjonalnych zależnych od doboru podstawowych usług Internetu, na których oparto budowę konkretnych architektur. Niniejszy artykuł stanowi próbę analizy wpływu doboru usług komunikacyjnych i sposobu ich wykorzystania w zdalnych systemach wizualizacji procesów przemysłowych na parametry użytkowe tych systemów.

2. Ewolucja przemysłowych systemów wizualizacji

Przejście od zamkniętych systemów sterowania i wizualizacji do systemów otwartych wykorzystujących usługi Internetu przebiega w sposób ewolucyjny. Wśród poszczególnych rozwiązań firmowych daje się zauważyć przesuwanie środka ciężkości od zamkniętych rozwiązań stacji kontrolno – nadzorczych w stronę rozwiązań bardziej otwartych, w których dostęp do informacji staje się możliwy z wykorzystaniem zasady serwer informacji – „cienki klient” czy też serwer – przeglądarka internetowa. Pierwszą grupę stanowią rozwiązania zdalnych systemów wizualizacji i sterowania zachowujące dotychczasową hermetyczność i skupiające się jedynie na wykorzystaniu Internetu jako medium do transferu danych użytecznych z jednego specjalizowanego systemu do drugiego (rys. **Błąd! Nie można odnaleźć źródła odsyłacza.**). Każdy z biorących udział w wymianie informacji systemów wymaga wyposażenia go w specjalistyczne oprogramowanie, a nierzadko w specjalistyczne rozwiązania sprzętowe. Ta klasa rozwiązań zakłada stopniową asymilację usług oferowanych przez sieć Internet poprzez klasyczną wielowarstwową strukturę systemów kontrolno – nadzorczych. Przykładem takiego rozwiązania może być stacja kontrolno – nadzorcza umożliwiająca podłączenie zdalnego stanowiska kontroli i nadzoru poprzez Internet z wykorzystaniem mecha-

nizmu RPC (*ang. Remote Procedure Call*) [4, 6, 8]. Powstały system wizualizacji jest wielostanowiskową stacją typu SCADA, wykorzystującą standardową usługę RPC definiowaną niezależnie od protokołu sieci Internet, w której poszczególne stanowiska operatorskie komunikują się ze sobą poprzez heterogeniczne środowiska sieciowe.



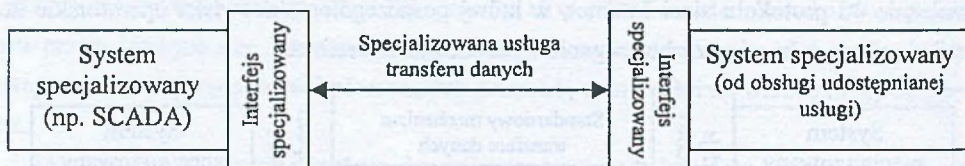
Rys. 1. Klasyczny przypadek wykorzystania standardowych usług Internetu
Fig. 1. The classical case the use of standard services of internet

Podstawową wadą takiego rozwiązania jest konieczność stosowania specjalistycznego oprogramowania umieszczanego po obu stronach połączenia sieciowego. Oprogramowanie to z jednej strony obniża mobilność systemu, z drugiej podnosi znacząco jego koszt.

Zupełnie odmienną filozofię reprezentują rozwiązania zakładające pełne wykorzystanie zestawu protokołów sieci Internet i standardowych usług definiowanych w ramach opisu standardu tychże protokołów w celu uzyskania dostępu do informacji pochodzącej z różnych elementów systemu przemysłowego. Systemy prezentujące powyższe podejście można, bazując na analogii do mechanizmów biologicznych, określić mianem konwergentnych systemów informatyki przemysłowej. Systemy konwergentne łączą dostęp do informacji pochodzącej z różnych źródeł za pomocą jednorodnego interfejsu. W dotychczasowych klasycznych rozwiązaniach systemy informatyki przemysłowej oferowały dostęp do często wysoce specjalistycznych usług za pomocą odmiennych interfejsów użytkownika, wymagając wielokrotnie zbierania danych pochodzących z różnych podsystemów i konstruowania kosztownych i często zawodnych mechanizmów umożliwiających wymianę informacji pomiędzy nimi. Konwergentne systemy informatyki przemysłowej bazują na wykorzystaniu powszechnych w sieci Internet usług, przez co sprzyjają wykształceniu takich cech oprogramowania, które umożliwiają spójny dostęp do informacji opisującej funkcjonowanie przedsiębiorstwa niezależnie od tego czy prezentowane informacje pochodzą bezpośrednio z linii produkcyjnej, systemów baz danych, czy też systemów przygotowania i planowania produkcji. Pochodząca z różnych źródeł informacja prezentowana jest w spójny sposób za pomocą przemysłowych portali internetowych, do których dostęp możliwy jest za pomocą przeglądarki internetowej czy też poczty elektronicznej.

Pomiędzy systemami bazującymi na klasycznej architekturze oprogramowania SCADA [5] i systemami konwergentnymi znajduje się całe spektrum oprogramowania aplikacyjnego wykorzystywanego do zdalnej wizualizacji procesów przemysłowych. Systemy te bazują w mniejszym lub większym stopniu na tych usługach, które spełniają wymagania specjalo-

wanego użytkownika, jakim jest użytkownik przemysłowych systemów kontrolno-nadzorczych (rys. Błąd! Nie można odnaleźć źródła odsyłacza.).



Rys. 2. Przypadek wykorzystania specjalizowanych usług Internetu
Fig. 2. The case the use of specialised services of internet

2.1. Wykorzystanie usługi WWW

Usługa WWW jest najbardziej popularną usługą Internetu dającą najlepiej rozwinięty interfejs użytkownika [3]. Wynika to ze znacznego spopularyzowania komputerów personalnych wykorzystujących systemy operacyjne z graficznym interfejsem użytkownika, takich jak Windows czy X-Windows, które dają duże możliwości dla prezentacji dokumentów hipertekstowych. Ze względu na fakt, iż przemysłowe stacje kontrolne stanowią interfejs pomiędzy systemem automatyki obsługującym proces a człowiekiem, wydaje się, że najistotniejsze zastosowanie w dziedzinie pośrednictwa z człowiekiem będzie miała ta właśnie usługa.

Usługa WWW jest popularna, a jej obsługa jest powszechnie znana, co kwalifikuje ją do zastosowań na płaszczyznach wymian pionowych [5]. WWW jest usługą udostępniającą użytkownikowi interaktywny dokument w postaci tzw. strony WWW. To samo w gruncie rzeczy wykonuje stacja SCADA, udostępniając tzw. ekrany. Zarówno usługa WWW, jak i stacja SCADA, przekazują użytkownikowi informacje graficzno-tekstowe umożliwiając jednocześnie interakcję przy użyciu standardowych urządzeń wejścia jak klawiatura czy mysz. Różnice, jakie tutaj zaistnieją, grupują się wokół następujących zagadnień:

- sposoby dostarczania danych,
- sposoby prezentacji danych,
- mechanizmy kontroli dostępu do danych.

Abstrahując od różnic w udostępnianiu informacji można stwierdzić, iż korzystając ze standardowego interfejsu usługi WWW jesteśmy w stanie wyeliminować specjalistyczne oprogramowanie po stronie stacji zdalnej. Jest to na tyle istotna pokusa, choćby ze względów ekonomicznych czy nawet samej wygody, że należy ten aspekt rozważyć dokładniej.

2.1.1. Rodzaje prezentacji

Ponieważ podstawowymi zadaniami stojącymi przed przemysłowymi systemami wizualizacji jest prezentacja informacji oraz interakcja z użytkownikiem, należy przyjrzeć się, co

obecnie usługa WWW ma w tej kwestii do zaoferowania. Istnieją trzy podstawowe typy dokumentów WWW [3]. Są to dokumenty:

- statyczne,
- dynamiczne,
- aktywne.

Dokumenty statyczne zawierają informację multimedialną o charakterze stałym. Raz pobrany dokument zawiera informacje nie zmieniające się w czasie i nie ma potrzeby jego odświeżania. Dokumenty statyczne bazują na interpretacji standardowego języka HTML i są tworzone tylko jednokrotnie na etapie ich projektowania. Na bazie tego typu dokumentów przy wizualizacji systemów przemysłowych można oprzeć prezentację wszystkich elementów statycznych, czyli takich, które stanowią graficzne i tekstowe tło danego ekranu.

Na języku HTML bazują również dokumenty dynamiczne. Jednak celem istnienia takich dokumentów jest przekazywanie informacji zmieniających się w czasie. Istnieje zatem potrzeba istnienia mechanizmu tworzenia dokumentu na żądanie. Serwer powinien mieć możliwość tworzenia dokumentu w momencie każdorazowego dotarcia żądania od klienta. Aby zapewnić taką dynamikę często używa się mechanizmu o nazwie CGI. Jest to wywołanie zdalnej aplikacji w celu uzyskania danych. Program CGI uruchamiany jest na żądanie klienta na serwerze WWW generując każdorazowo nowy kod strony. Dzięki temu uzyskujemy stronę WWW, zawierającą najnowsze informacje. Przy wizualizacji przemysłowej program CGI może pobierać dane od systemu i modyfikować zawartość przekazywanej klientowi informacji przy każdorazowym odświeżeniu strony. Połączenie elementów statycznych z elementami generowanymi przez CGI daje już skuteczny sposób prezentacji stanu procesu. Uzyskujemy możliwość obsługi zarówno elementów statycznych, jak i animacyjnych i kontrolnych. Elementy kontrolne mogą być realizowane przez wykorzystanie mechanizmu formularzy w połączeniu z mechanizmem krótkoterminowego przekazywania informacji o stanie. Daje to możliwość budowania stron WWW jako dialogów parametryzacyjnych dla procesu.

Najbardziej zaawansowaną techniką prezentacji są dokumenty aktywne. Dokument aktywny samoczynnie, bez konieczności odświeżania strony przez użytkownika, aktualizuje swój stan. Może to się odbywać na dwa sposoby. Najprostszym, a zarazem dość skutecznym sposobem jest „wpychanie” przez serwer (ang. *server push*). Polega to na cyklicznym wymuszaniu wysyłki zmodyfikowanej strony do klienta. Drugi sposób jest bardziej złożony, ale też zasadniczo lepszy. Jest to technika Javy. W tej metodzie postać dokumentów aktywnych nie jest w pełni określona przez serwer. Serwer wysyła do klienta jedynie „przepis” na to, jak ma klient zadziałać. Tym „przepisem” jest specjalny program, który jest wykonywany lokalnie u klienta, lokalnie generując strony WWW i mogąc przy tym korzystać z połączeń TCP/IP. Program klienta WWW może wówczas stać się klientem zupełnie nowych usług definiowanych na potrzeby aplikacji. Zawartość dokumentu aktywnego może się zmieniać w sposób ciągły bez konieczności retransmisji jego opisu. Dla prostych stacji monitorujących wystar-

czający jest mechanizm cyklicznego wypychania. Jednak gdy strona zawiera dużo informacji i do tego w formie graficznej, metoda ta powoduje nieprzyjemne miganie ekranu, a w przypadkach zwiększonych opóźnień transmisji staje się uciążliwa. Wówczas najbardziej korzystnym rozwiązaniem okazuje się technologia Java. Dzięki lokalnemu sterowaniu strona może niczym nie różnić się od dedykowanej aplikacji uruchomionej lokalnie. Jedyne działanie elementów animacyjnych zależy od połączenia TCP/IP. Podobną w idei działania do technologii Javy jest technologia ActiveX.

Bazując na powyższych charakterystykach można zauważyć duże podobieństwo pomiędzy typami dokumentów WWW i rodzajami elementów stosowanych przy wizualizacji przemysłowej. Można również stwierdzić, iż technika Javy lub ActiveX w połączeniu z dokumentami statycznymi opartymi na HTML jest najskuteczniejszą metodą prezentacji danych w systemach wizualizacji przemysłowej opartej na usługach WWW. Jednak technika ta, dając szerokie pole do implementacji specyficznych usług, stwarza również zagrożenia z punktu widzenia bezpieczeństwa.

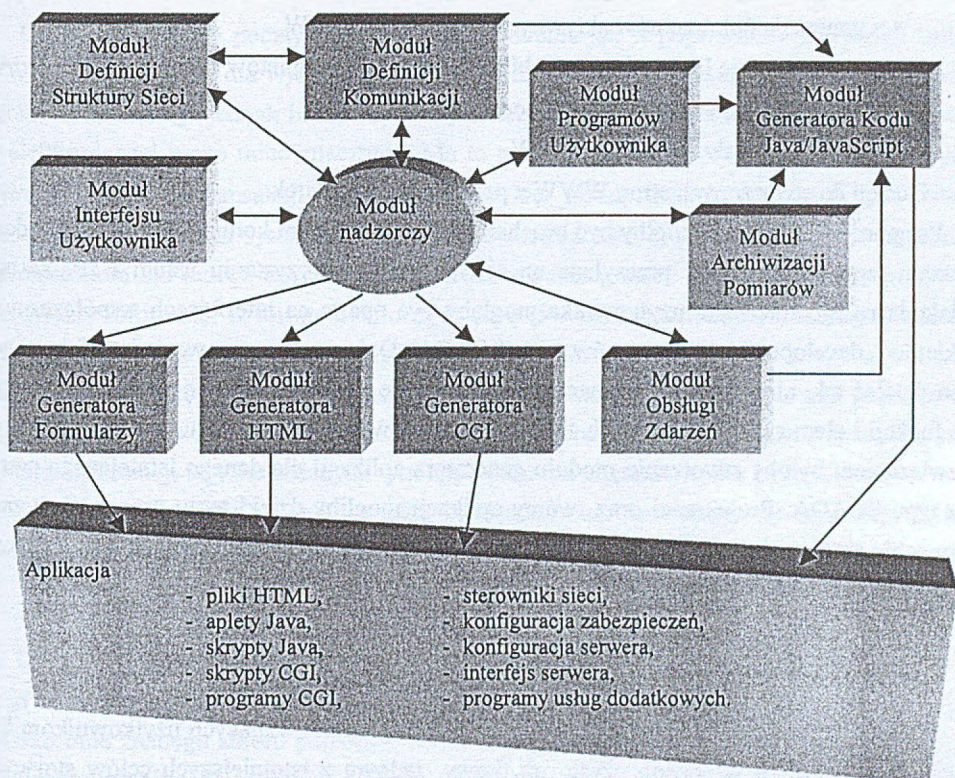
2.1.2. Struktura komunikacji

Usługa WWW działa w sieci Internet, a więc korzysta z protokołów TCP/IP, a w szczególności w warstwie aplikacji z protokołu HTTP. W warstwie niższej transfer danych zachodzi z wykorzystaniem protokołu TCP. Protokół HTTP, tak jak wiele innych usług internetowych, działa na bazie modelu klient-serwer. Serwerem jest zawsze specjalizowany abonent udostępniający i uaktualniający dokumenty, natomiast klientem jest oprogramowanie przeglądarki (ang. *browser*). Model ten doskonale pasuje do realizacji zdalnego dostępu do lokalnego systemu kontrolnego. Serwer, serwery lub hybrydy serwerów WWW z lokalnymi stacjami typu SCADA mogą być bez większych przeszkód instalowane wraz z systemem informatycznym kontrolującym proces. Aplikacje klienckie – przeglądarki mogą pracować gdziekolwiek w sieci Internet.

Praca serwera w klasycznych rozwiązaniach jest niezwykle prosta. Czeka on w pętli na zgłoszenie żądania transferu dokumentu od klienta. Gdy takie żądanie nadejdzie, serwer przesyła dany dokument, zamyka połączenie i czeka na kolejne żądania. Znacznie bardziej złożona jest konstrukcja aplikacji klienta. Ponieważ na transfer dokumentu hipertekstowego może składać się wiele żądań transferu jego elementów składowych, przeglądarka musi składać się z całego zestawu klientów, interpreterów, a także modułów zarządzania i interakcji z użytkownikiem. Dzieje się tak, gdyż dokument hipertekstowy jest dokumentem multimedialnym. Może się on składać z szeregu elementów typu: tekst, obraz, dźwięk oraz elementów dynamicznych typu: skrypty, odnośniki czy programy wykonywalne. Protokół HTTP definiuje transfer takiego dokumentu jako szereg transmisji jego elementów składowych. Po

odebraniu elementu połączenie z serwerem zostaje zamknięte i, o ile istnieje potrzeba pobrania następnego elementu, znowu otwarte jako kolejna transakcja.

Upraszczając, protokół HTTP działa podobnie do protokołu FTP, lecz oprócz standardowego przesłania pliku na żądanie klienta protokół umożliwia przesyłanie danych generowanych dynamicznie przez aplikacje pracujące na serwerze oraz przetwarzanie w tych aplikacjach danych pobranych z aplikacji klienta. Cecha ta doskonale się nadaje do realizacji interakcji pomiędzy lokalnym systemem nadzorczym a stacją zdalną.



Rys. 3. Proponowana struktura narzędzia do tworzenia rozproszonej aplikacji wizualizacji przemysłowej

Fig. 3. The proposition of a tool's structure using to creation of distributed application of industrial visualisation

Na rysunku 3 przedstawiono przykładową strukturę systemu do tworzenia rozproszonej aplikacji wizualizacyjnej. Działanie takiego narzędzia obejmuje następujące etapy:

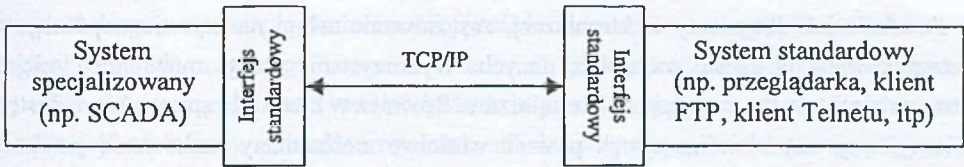
- Przygotowywanie wizualizacji przy użyciu klasycznego interfejsu użytkownika
 - definicja zmiennych, grafiki ekranów i ich elementów składowych,
 - definicja komunikacji,
 - definicja programów użytkownika itp.;

- Generacja dokumentów dla serwera WWW
 - generacja dokumentów statycznych dla serwera WWW,
 - pliki HTML,
 - dołączanie grafiki,
 - generacja dokumentów dynamicznych dla serwera WWW,
 - tworzenie lub dołączanie z bibliotek skryptów i programów CGI,
 - generacja formularzy i dołączanie grafiki,
 - generacja dokumentów aktywnych dla serwera WWW,
 - tworzenie lub dołączanie z bibliotek skryptów i apletów Java,
 - dołączanie aplikacji usług dodatkowych;
- Przesłanie plików do serwerów WWW
- Dostęp do stworzonych stron WWW z poziomu przeglądark.

Program narzędziowy mógłby być uruchamiany na dowolnym komputerze, a pliki będące efektem jego pracy byłyby przesyłane na serwer przy wykorzystaniu usługi FTP. Zasada działania całego interfejsu użytkownika mogłaby być oparta na interfejsach współczesnych pakietów „developerskich” systemów typu SCADA. Dobrze skonstruowany interfejs powinien działać tak, aby ukrywać mechanizmy WWW, nie pozwalając jednocześnie na tworzenie funkcji i elementów nie dających się zaimplementować w technologiach WWW. Dobrym rozwiązaniem byłoby stworzenie modułu generatora aplikacji dla danego istniejącego systemu typu SCADA. Projektanci oraz twórcy aplikacji mogliby dzięki temu pracować w znanym sobie środowisku mając jednocześnie możliwość wygenerowania aplikacji standardowej lub opartej na technologii WWW.

2.2. Wykorzystanie innych usług

W sieci Internet istnieje cały szereg istotnych usług umożliwiających użytkownikom korzystanie z Internetu w sposób czysto użytkowy. Jednym z istotniejszych celów stojących przed mechanizmami standaryzacji sieci Internet jest taki podział zadań funkcjonalnych sieci, aby stworzone grupy najbardziej pasowały do potrzeb jej użytkowników. Jeżeli zdefiniujemy usługę obsługującą daną grupę funkcjonalną w sposób standardowy, wówczas użytkownik jest niezależny od rodzaju sprzętu i systemu operacyjnego. Główne wytyczne do obsługi interfejsu użytkownika stają się standardowe, zatem użytkownik nie musi posiadać zaawansowanej wiedzy z zakresu intersieci i lokalnego systemu stacji roboczej. Na bazie stosu protokołów aplikacyjnych TCP/IP można wprowadzać standardowe usługi Internetu przeznaczone dla użytkowników tej sieci.



Rys. 4. Alternatywny przypadek wykorzystania standardowych usług Internetu
 Fig. 4. The alternate case the use of standard services of internet

2.2.1. Poczta elektroniczna

Usługa przesyłania poczty elektronicznej, podobnie jak w poprzednim przypadku usługi WWW, nie nadaje się dla wymian poziomych. Dziedzina zastosowania tej usługi jest bardzo ograniczona. Istnieje jednak bardzo istotna płaszczyzna wymian, dla której przesyłanie poczty elektronicznej może mieć znaczenie. Ma to miejsce w transmisjach na płaszczyźnie pionowej [5] tylko dla transakcji typu abonent→serwer_poczty. Przesłanie komunikatu bezpośrednio przez abonenta systemu (czyli niejako automatycznie) adresowanego do nadzorca, administratora lub innego użytkownika systemu ma szereg zalet. Mechanizm taki umożliwia przesyłanie informacji w formie cyklicznych raportów lub komunikatów o istotnych zdarzeniach, bezpośrednio z poziomu systemu lokalnego do skrzynki pocztowej danego użytkownika lub grupy użytkowników. Niezależnie od swojej lokalizacji użytkownik taki poprzez dostęp do Internetu może uzyskiwać dostęp do tych informacji. Ze względu na specyfikę prezentacji informacji wymiana danych tym sposobem ma charakter tylko jednokierunkowy, od procesu do użytkownika. Wynika z tego, iż idealnym zastosowaniem dla tej usługi będzie funkcja raportowania.

2.2.2. FTP

Usługa FTP jest protokołem warstwy aplikacyjnej [3]. Dokumentacja RFC959 nie definiuje interfejsu użytkownika, lecz wiele implementacji tej usługi korzysta ze standardowego powszechnie znanego zbioru poleceń. Usługa ta jest użyteczna praktycznie dla każdego typu płaszczyzn wymian. Dotyczy ona transferu plików, czyli *de facto* zbiorów danych. Zakładając, że każdy abonent posiadający wystarczająco rozbudowaną warstwę aplikacji potrafi tworzyć abstrakcyjne zbiory danych, należy przyjąć, iż o ile istnieje potrzeba transmisji tych danych do stacji odległych, można tego dokonać wykorzystując transfer plików. Jest to wygodne z tego względu, że do samego procesu pobierania danych użytkownik nie potrzebuje specjalistycznego oprogramowania, a jedynie standardowego oprogramowania klienta FTP. Idealne zastosowanie tej usługi będzie miało miejsce w systemach, gdzie abonent lokalny gromadzi dane w pliku, np. zapisy trendów wybranych parametrów, a abonent zdalny korzystający z sieci Internet podłącza się usługą FTP do systemu lokalnego i pobiera dane do wglądu lub dalszej obróbki.

Podobnie jak dla poczty elektronicznej, zastosowanie usługi nie ma nic wspólnego ze zdeterminowaną w czasie transmisją danych. Wykorzystanie usługi może mieć miejsce w transmisjach nie wymagających determinizmu. Również w kwestii bezpieczeństwa dostępu i identyfikacji użytkownika usługa posiada właściwe mechanizmy zachowania poufności udostępnianych danych. Jednak usługa ta nie jest odporna na monitorowanie danych, gdyż nazwa użytkownika i hasło przesyłane są w postaci jawnej. Dodatkowym zabezpieczeniem może być uruchamianie usługi na innym porcie niż standardowy 21 lub wykorzystywanie niestandardowych aplikacji klientów i serwerów.

2.2.3. *Telnet*

Telnet jest protokołem aplikacyjnym umożliwiającym przede wszystkim zdalną interakcyjną pracę z odległym komputerze przy wykorzystaniu wirtualnego terminala znakowego [3]. Zastosowanie tego protokołu ma sens dla wymian pionowych ze względu na możliwość definiowania usługowego interfejsu użytkownika. Warto zauważyć, że protokół definiuje mechanizm komunikacji interakcyjnej a nie samą usługę, zatem możliwe i wskazane jest wykorzystywanie tego protokołu do komunikacji w różnych usługach. Jest to możliwe i wygodne jeszcze z innego powodu. Inicjując połączenie telnetowe w większości systemów można podać opcjonalnie numer portu inicjując automatycznie tym samym połączenie z inną usługą niż standardowa usługa zdalnego terminala.

Daje to dość ciekawe możliwości. Przede wszystkim mając dostęp do standardowego klienta protokołu Telnet można korzystać z różnych usług zainstalowanych na serwerze, które współdziałają z tym protokołem. Po drugie tworząc klienta i serwera specjalizowanego można utworzyć specjalizowaną usługę realizującą dowolny zbiór zadań w ramach dziedziny wynikającej z ograniczeń niezdedeterminowanej czasowo komunikacji. Protokół Telnet jest zatem doskonałym narzędziem do tworzenia nowych usług na bazie istniejących protokołów.

Najprostszym, najwygodniejszym i najtańszym rozwiązaniem jest stworzenie aplikacji pracującej na serwerze, która wykorzystując Telnet w powiązaniu z danym portem (najlepiej niestandardowym) będzie realizować usługę dostępu do wybranej grupy danych procesowych oraz będzie zgodnie z akcją użytkownika oddziaływać na tę lub inną grupę. Aplikacja taka może stanowić proces uruchamiany zdalnie na żądanie ze zdalnego terminala i z tymże terminalem związać swoje strumienie wejścia-wyjścia użytkownika. Możliwe jest również uruchomienie takiej aplikacji jako serwera dodatkowej usługi.

Dodatkowo możliwa jest implementacja mechanizmu określania jakości pozyskiwanych danych. Nasuwają się dwie możliwości realizacji takiej usługi. Pierwsza określa (nie zapewnia) czasową spójność danych poprzez transmisję stempla czasowego wraz z danymi użytecznymi, druga określa stabilność cyklu odczytu danych na stacji klienta. Niestety, obie wiążą się z niedogodnościami. Pierwsza wymaga synchronizacji zegarów nadawcy i odbiorcy,

natomiast druga wiąże się z koniecznością posiadania specjalizowanej aplikacji klienta. W przypadku stempla czasowego czas wytworzenia wartości zmiennej powinien być dołączony do pakietu przynoszącego samą wartość, jednak, aby poprawnie interpretować wartość stempla na stacji odbiorczej, niezbędne są urządzenia umożliwiające synchronizację zegarów z dokładnością wynikającą z cyklu transmisji zmiennej. Jako takie urządzenia mogą posłużyć zegary DCF synchronizowane radiowo ze wzorca zegara atomowego. W przypadku testowania stabilności cyklu jesteśmy w stanie określić „świeżość” zmiennej cyklicznej. Mechanizm powinien funkcjonować mierząc różnicę czasu pomiędzy nadejściem kolejnych pakietów z daną zmienną. Na podstawie wyliczonej różnicy oraz zadeklarowanego czasu życia wartości zmiennej można dokonać binarnego określenia flagi świeżości dla danej wartości.

Różnice pomiędzy jedną a drugą możliwością sprowadzają się do faktu, iż określanie stabilności cyklu jest możliwe tylko dla zmiennych cyklicznych. W przypadku zmiennych aperiodycznych potrzebna jest informacja od producenta zmiennej, aby móc określić, na ile zmienna została opóźniona przez warstwy komunikacyjne. Również w przypadku zachwiania cyklu bez stempla czasowego można określić jedynie, że pakiety nie pojawiają się z zamierzoną częstotliwością. Aby określić w czasie, kiedy dana wartość została wytworzona, niezbędny jest stempel czasowy od nadawcy. Opisywane mechanizmy dotyczą innego charakteru określania jakości danych niż w przypadku opisywanego wcześniej określania na poziomie integracji systemu izolowanego z siecią Internet. Nie mamy tutaj do czynienia z przekazywaniem danych z jednego otwartego systemu komunikacyjnego do drugiego izolowanego, a jedynie z przesyłem pomiędzy abonentami w obrębie sieci Internet otwartej, pracującej na bazie TCP/IP. Podobne mechanizmy określania świeżości danych funkcjonują w firmowych rozwiązaniach, na przykład w protokole SuiteLink firmy WonderWare.

W usługach wykorzystujących protokół Telnet mechanizmy identyfikacji, kontroli dostępu czy też szyfrowania transmisji, ze względu na ich brak w samym protokole, mogą lub też muszą być wbudowane bezpośrednio w usługę.

Protokół Telnet można wykorzystać niewielkim kosztem do zdalnego monitorowania parametrów procesu. Najtańszym rozwiązaniem będzie bazowanie na usłudze zdalnego terminala znakowego i specjalizowanego programu uruchamianego zdalnie na serwerze. Jeżeli natomiast chcemy tworzyć nowe, specjalizowane usługi, niezbędna jest modyfikacja interfejsów komunikacyjnych abonentów, szczególnie w warstwach aplikacji użytkownika.

3. Integracja sieci Internet z systemem automatyki przemysłowej

Kolejnym elementem wpływającym na właściwości użytkowe systemów zdalnej wizualizacji jest określenie punktu styku pomiędzy systemem automatyki przemysłowej pracującym

z zachowaniem determinizmu czasowego [10, 1, 2] a niezdeterminowaną w czasie siecią Internet [7]. Metoda połączenia zależy będzie od: parametrów systemu automatyki, wielkości systemu, liczby i klas stosowanych w nim sieci przemysłowych najniższego poziomu, liczby i rodzaju pracujących w tym systemie stacji kontrolno-nadzorczych, sposobu rejestracji i gromadzenia informacji archiwalnych, a także od wymagań stawianych przed zdalnym systemem wizualizacji i sterowania.

Najprostsze z rozwiązań dostępu wykorzystują wbudowane serwery takich protokołów jak: http, smtp, czy ftp. Serwery te związane są w rozwiązaniu sprzętowym z sygnałami pomiarowymi i binarnymi oraz informacjami zbieranymi drogą cyfrową pochodzącymi wprost z obiektu. Na przeciwnym biegunie znajdują się rozwiązania portali internetowych pobierających informacje pochodzące z systemów klasy SCADA, systemów przemysłowych baz danych, systemów planowania i przygotowania produkcji i udostępniające je w postaci portali internetowych. Do rozwiązań pośrednich można zaliczyć funkcje serwera usług internetowych realizowane w postaci wydzielonych modułów stacji kontrolno-nadzorczych klasy SCADA.

3.1. Stacja kontrolno-nadzorcza jako serwer danych wykorzystywanych w procesie wizualizacji

Umieszczenie funkcji związanych z wymianą informacji w jednym z modułów stacji kontrolno – nadzorczej umożliwia dobrą izolację systemu automatyki przemysłowej od sieci Internet (rys.5). Jakikolwiek ruch przychodzący z sieci rozległej zostaje zatrzymany na poziomie urządzenia pośredniczącego, którego funkcję pełni w tym przypadku stacja kontrolno - nadzorcza. Stacja ta 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 wydzielone stanowisko komputerowe, będące jednocześnie składnikiem rozproszonego systemu SCADA bądź też dla mniejszych instalacji funkcje te mogą być łączone w pojedynczej stacji kontrolno-nadzorczej i realizowane przez jeden z jej modułów.

Wykorzystanie stacji kontrolno-nadzorczej jako elementu pośredniczącego pomiędzy systemem automatyki przemysłowej i siecią Internet powoduje izolację 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.

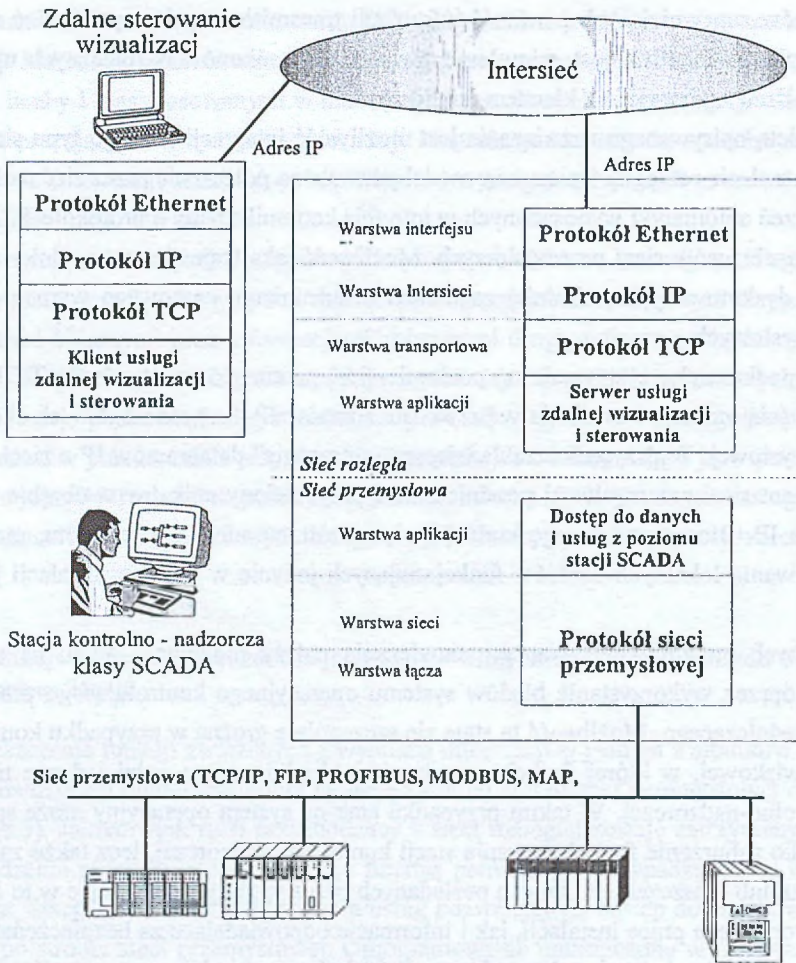
Zwiększenie bezpieczeństwa systemu można uzyskać dzięki wprowadzeniu szeregu mechanizmów kontroli dostępu, jak np. mechanizmów uwierzytelniania i autentyfikacji oraz

mechanizmów zapewniających poufność informacji transmitowanych poprzez sieć rozległą. Na tym poziomie możliwe jest zaimplementowanie mechanizmów bezpiecznych usług, jak np. mechanizmu szyfrowania z kluczem publicznym.

Inną zaletą opisywanego rozwiązania jest możliwość integracji różnego typu sieci przemysłowych z siecią rozległą. Opisywany model pozwala na połączenie przez 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 dyskusowanych 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 sieci Internet każdy abonent sieci przemysłowej powinien mieć przydzielony unikalny w obrębie sieci Internet adres IP. Biorąc pod uwagę kurczącą się przestrzeń adresową Internetu, możliwość wykorzystywania lokalnych adresów funkcjonujących jedynie w obrębie instalacji jest bardzo ważna.

Do słabych punktów opisywanego rozwiązania należy możliwość ataku na sieć wewnętrzną poprzez wykorzystanie błędów systemu operacyjnego kontrolującego pracę urządzenia pośredniczącego. Możliwość ta staje się szczególnie groźna w przypadku konfiguracji jednostanowiskowej, 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 tę 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.



Rys. 5. Separacja sieci przemysłowej na poziomie stacji SCADA
 Fig. 5. Industrial network separation on SCADA level

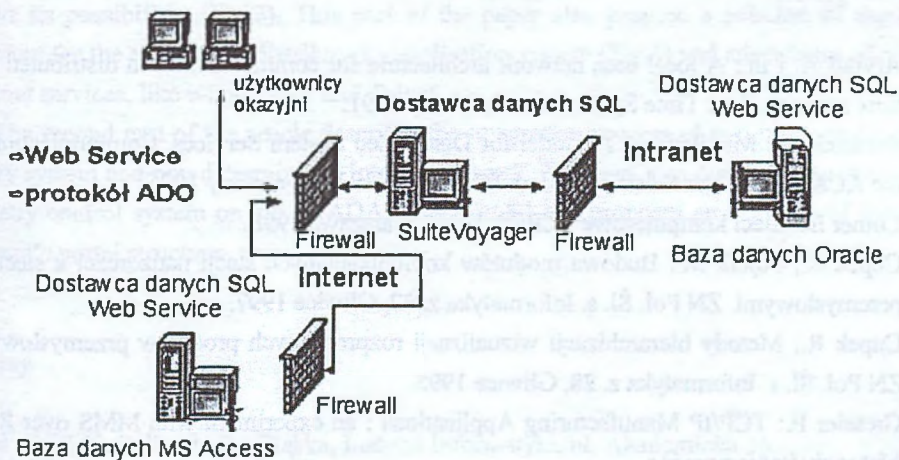
Drugą wadą rozwiązania opartego na przedstawionym modelu jest ograniczanie dostępu wyłącznie dla autoryzowanych użytkowników. Sytuacja taka sprawia, iż staje się niemożliwe wykorzystanie szeregu usług związanych z publicznym dostępem do danych, jak np. prezentacja wybranych informacji poprzez strony WWW.

Wreszcie opisane rozwiązanie niezbyt dobrze nadaje się do systemów, w których występuje większa liczba 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 lep-

szym rozwiązaniem wydaje się opisana poniżej architektura z zastosowaniem komputera - bastionu.

3.2. Przemysłowy portal intranetowy

Elementem pozwalającym na integrację informacji wymienianych na poziomie przedsiębiorstwa są przemysłowe portale informacyjne konstruowane na poziomie sieci Intranet. Portale te umożliwiają spójną prezentację informacji pochodzących z różnych źródeł, takich jak: systemy wizualizacji klasy SCADA, systemy przemysłowych baz danych, systemy śledzenia produkcji, systemy gospodarki zasobami, czy też systemy planowania i przygotowania produkcji. Ze względu na znaczną skalę złożoności rozwiązania te realizowane są często na poziomie całego przedsiębiorstwa operując wielokrotnie na ogromnej ilości danych bieżących i danych archiwalnych. Ze względu na złożoność realizowanych zadań poszczególne funkcje realizowane są przez system rozproszony umieszczony w strukturze sieci wewnętrznej przedsiębiorstwa. Przykładową strukturę przemysłowego portalu intranetowego zrealizowanego na bazie pakietu oprogramowania SuiteVoyager firmy WonderWare przedstawiono na rys. 6.



Rys. 6. Przykładowa struktura przemysłowego portalu intranetowego
Fig. 6. Example of industrial intranet's portal structure

Zaletą systemów wizualizacji bazujących na przemysłowych portalach intranetowych jest spójna postać prezentowanych danych pochodzących z różnych źródeł. Oprócz funkcji związanych z wizualizacją informacji o procesie przemysłowym, rozumianą w sposób zbliżony jak miało to miejsce w przypadku systemów SCADA, portale te pozwalają na organizację wymiany informacji pomiędzy poszczególnymi ogniwami przedsiębiorstwa za pomocą poczty elektronicznej, stron informacyjnych, czy też interakcyjnych formularzy. Umieszczenie

portalu w wewnętrznej wydzielonej sieci przedsiębiorstwa pozwala na stworzenie bardziej odpornego systemu zabezpieczeń opartego na wielostopniowym mechanizmie ścian ogniowych oraz na powiązanie go z polityką bezpieczeństwa prowadzoną na poziomie przedsiębiorstwa.

Dostęp do informacji jest zazwyczaj limitowany w funkcji uprawnień poszczególnych użytkowników, a menu dostępnych operacji jest personalizowane w odniesieniu do grupy użytkowników lub też bezpośrednio dostosowywane do potrzeb konkretnych użytkowników systemu. Przemysłowe portale intranetowe w odróżnieniu od rozwiązań bazujących na systemach stacji kontrolno – nadzorczych wymagają niemal ciągłych czynności pielęgnacyjnych prowadzonych przez służby informatyczne przedsiębiorstwa. Przejście pomiędzy systemami opartymi na architekturze SCADA a systemami portali intranetowych może mieć charakter płynny i obejmować stopniowe wprowadzanie danych dotyczących wizualizacji do funkcjonujących w wielu przedsiębiorstwach portali intranetowych wykorzystywanych dotychczas na poziomie zarządzania przedsiębiorstwem.

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. Gressier E.: *TCP/IP Manufacturing Applications : an experiment with MMS over RPC*. Materiały konferencyjne
7. Grzywak A.: *Problemy integracji sieci komputerowych*. *ZN Pol. Śl. s. Informatyka z. 23, Gliwice 1993*.
8. Ham A., Kumara E.: *Global Collaborative Manufacturing and the World-Wide Web Integrated Design and Manufacturing in Mechanical Engineering*. IDMMME'96. Avril 1996. Nantes. France.
9. Kwiecień A.: *Analiza przepływu komunikatów w komputerowych sieciach przemysłowych*, praca habilitacyjna, Politechnika Śląska, Gliwice 1998.

10. Torngren M.: Fundamentals of Implementing Real –Time Control Applications in Distributed Computer Systems, Journal of Real Time Systems 1996.

Recenzent: Dr inż. Włodzimierz Boron

Wpłynęło do Redakcji 19 kwietnia 2003 r.

Abstract

The paper contains two parts. The first part describes, on the evolutionary background, the methods and types of intranet services usable in the visualisation industry systems. The paper discusses (Fig.1) the classical method of connecting two SCADA stations with the use of the Remote Procedure Call (RPC) standard, for data transfer between them. The paper also shows advantages and disadvantages of this method. Additionally, it describes the method of using classical Internet services for data transfer between two industrial SCADA systems and shows its possibilities.(Fig.2). This part of the paper also propose a solution of the tool's structure for the creation of distributed visualisation system (Fig.3) and advantages of another Internet services, like e-mail, FTP and Telnet.

The second part of the article describes the integration process of two parts: real-time industry system and non deterministic Internet network. This part also discuss separation of the industry control system on the SCADA level (Fig.5.) and proposes an example of industrial intranet's portal structure.

Adresy

Rafał CUPEK: Politechnika Śląska, Instytut Informatyki, ul. Akademicka 16,
44-101 Gliwice, Polska, rafal@inf.polsl.gliwice.pl

Piotr GAJ: Politechnika Śląska, Instytut Informatyki, ul. Akademicka 16, 44-101 Gliwice,
Polska, pgaj@top.iinf.polsl.gliwice.pl.

Andrzej KWIECIEN: Politechnika Śląska, Instytut Informatyki, ul. Akademicka 16,
44-101 Gliwice, Polska, andrzej@top.iinf.polsl.gliwice.pl