STUDIA INFORMATICA 2002
Volume 23 Number 3 (50)

Piotr GAJ
Politechnika Śląska, Instytut Informatyki

DOBÓR PROTOKOŁÓW DLA INTERFEJSÓW KOMUNIKACYJNYCH URZĄDZEŃ WSPÓŁPRACUJĄCYCH Z PRZEMYSŁOWYMI SYSTEMAMI KONTROLNO–NADZORCZYMI

Streszczenie. Artykuł dotyczy wykorzystania protokołów komunikacyjnych do przesyłu informacji w przemysłowych systemach kontrolno-nadzorczych. Główny poruszany aspekt tego zagadnienia dotyczy doboru optymalnych protokołów komunikacyjnych pracujących w warstwach interfejsów sieciowych urządzeń informatycznych obsługujących procesy przemysłowe. Analizowane są kryteria wymogów procesu, wymagań użytkownika, bezpieczeństwa dostępu oraz aspekty ekonomiczne. Wskazówki doboru nie ograniczają się do protokołów stricte przemysłowych i uwzględniają również warstwy protokołów nie mających charakteru czasowo zdeterminowanego. Szczególny nacisk położony został na sieci oparte na protokołach TCP/IP, a w szczególności ich wyższych warstwach oraz wykorzystaniu standardowych usług sieci.

PROTOCOLS SELECTION FOR COMMUNICATION DEVICES INTERACTING WITH INDUSTRIAL CONTROL SYSTEMS

Summary. This article concern to taking advantage of communication protocols to transfer data in industrial control systems. Author of this article try to show some hints of protocols selection for any kind of computer devices in industry. Described criteria are based on process requirement, user requirement, remote access security and economical aspects. The hints are not limit to industrial protocols only and take into consideration not determined protocols levels also. Characteristic stress is putting on TCP/IP based network and in particular on its higher levels and using standard network services.

1. Wstęp

We wstępie należy wyjaśnić, co kryje się pod tytułowym pojęciem przemysłowy system kontrolno-nadzorczy. Otóż jest to system informatyczny, bezpośrednio kontrolujący dany proces przemysłowy. Pod pojęciem kontroli kryją się takie zagadnienia, jak wizualizacja, monitorowanie, raportowanie oraz sterowanie. W skład takiego systemu wchodzą urządzenia pozostające w bezpośredniej interakcji z procesem, czyli wszelkiego typu sensory, oraz urządzenia wykonawcze, a także urządzenia stanowiące interfejs pomiędzy systemem a użytkownikiem – uogólniając człowiekiem.

Główny problem, który pojawia się w artykule, to w jaki sposób należy komponować zestawy protokołów na poziomie abonentów sieci systemu kontrolnego, ze szczególnym uwzględnieniem wykorzystania intersieci w tego typu systemach, oraz na co należy zwracać uwagę z punktu widzenia bezpieczeństwa prowadzenia takiej kontroli. Proponowany dobór zestawu protokołów, stanowiący optimum względem branych pod uwagę kryteriów, może dać interesujące rezultaty w porównaniu z rozwiązaniami typowymi. Modyfikacja standardowych rozwiązań warstw protokołów interfejsów komunikacyjnych, choćby nawet ograniczała zakres możliwości funkcjonalnych systemów kontrolno-nadzorczych, może okazać się atrakcyjna dla projektantów warstw komunikacyjnych takich systemów.

Dla dalszych rozważań należy mieć również na uwadze fakt, iż mamy do czynienia z wymianą informacji na najniższym poziomie całościowego systemu informatycznego obsługującego fizyczny proces przemysłowy [8]. Oznacza to, że sieć głównie przekazuje dane z wykorzystaniem wymian poziomych [6] czyli pochodzących od procesu lub dla procesu, a wymienianych przez urządzenia mające bezpośredni kontakt z tymże procesem. Do sieci o takiej właśnie charakterystyce podłączamy również interfejsy w postaci stacji SCADA [6]. Stacja taka wymusza pojawienie się wymian pionowych oraz wprowadza do systemu bardzo istotne kryterium jego projektowania, a mianowicie kryterium użytkownika. Z najniższą warstwą wymiany informacji nierozerwalnie wiąże się pojęcie determinizmu czasowego, które stanowi główne kryterium doboru protokołów w systemach przemysłowych. W artykule pojawiają się częste odwołania do wcześniejszej pracy z tego zakresu publikowanej w [7].

2. Kryteria projektowania warstwy komunikacji

Przystępując do projektowania warstwy komunikacji systemu kontrolnego, projektanci najczęściej sięgają po rozwiązania standardowe nie zastanawiając się, czy dane rozwiązanie spełnia poszczególne wymogi aplikacyjne w sposób optymalny, czy też jest nadmiarowe lub

swoje działanie opiera na statystycznym stwierdzeniu „powinno działać". Rozważenie wszystkich aspektów wdrożenia i eksploatacji systemu i dopasowanie rozwiązań do zapotrzebowań może przynieść istotne korzyści dla jego użytkownika. Przedstawiony w publikacji [7] dobór protokołów opiera się na kryteriach związanych z parametrami czasowymi wymian. Dobór taki jest skuteczny, jeżeli parametry te są najistotniejsze i nie analizuje się innych wymogów aplikacji. Poza tym dotyczy on protokołu jako całości, nie analizując jego funkcjonalnych składowych. Proponowany w niniejszym artykule dobór protokołów jest znacznie mniej formalny niż przedstawiony w [7], jednak bierze pod uwagę więcej kryteriów natury ogólnej, a mających istotny wpływ na funkcjonowanie całości, i może stanowić punkt wyjściowy dla wstępnej selekcji rozwiązań. Przedstawione tu zagadnienia doboru różnią się od doboru wynikającego z charakteru wymian. Główny punkt nacisku położony jest na taki dobór protokołów w poszczególnych warstwach interfejsów sieciowych urządzeń, aby zapewnić optymalny zestaw usług oferowanych przez sieć względem rozpatrywanych kryteriów.

Aby przeprowadzić dobór, należy określić, jakimi przesłankami będziemy się kierowali akceptując lub odrzucając kolejne rozwiązania. Zatem wskazane jest, aby istniejące rozwiązania pogrupować w taki sposób, aby z przyjętych kryteriów można było te grupy, zwane dalej klasami rozwiązań, wyprowadzić. Jeżeli z szeregu kryteriów otrzymamy zbiór klas, to część wspólna tych klas będzie grupą rozwiązań optymalnych. Na potrzeby doboru protokołów możemy stworzyć następujące klasy definiujące określone typy rozwiązań:

- klasa rozległości systemu;

  Do klasy należą rozwiązania sieciowe, zróżnicowane pod kątem zależności konstrukcji warstw fizycznych od odległości pomiędzy abonentami. Dla przykładu, można wymienić trzy kategorie:

  1. sieci lokalne (połączenia stałe, połączenia radiowe),
  2. sieci rozległe (intersieci, połączenia radiowe, sieci telekomunikacyjne),
  3. sieci mobilne (połączenia radiowe, sieci telekomunikacyjne),

- klasa zakłóceń;

  Do klasy należą rozwiązania sieciowe, zróżnicowane pod kątem zależności konstrukcji warstw fizycznych od poziomu zakłóceń wpływających na parametry komunikacji. Dla przykładu można wymienić kilka kategorii używanych sygnałów fizycznych różnicujących wrażliwość na różnego typu zakłócenia:

  1. sygnały elektryczne,
  2. światło,
  3. fale radiowe,
  4. podczerwień,

- klasa usług sieciowych;

  Do klasy należą rozwiązania sieciowe, zróżnicowane pod kątem wykorzystywanych usług sieciowych. Można zdefiniować dwie wirtualne usługi sieciowe określające charakter dostępu do informacji. Są to:

  1. usługa lokalnego dostępu,
  2. usługa zdalnego dostępu.

  Usługa lokalnego dostępu do informacji umożliwia nam uzyskanie dostępu do danych systemowych z poziomu każdego urządzenia stanowiącego stały element składowy działającego systemu. Druga usługa, usługa zdalnego dostępu umożliwia uzyskanie dostępu do danych systemowych na zasadzie tymczasowego podłączenia abonenta do działającego systemu. Mechanizm realizacji wymian musi być przygotowany na wyprowadzenie danych z systemu do nowego abonenta i wprowadzenie nowych danych do obiegu istniejącego. Usługa ta ma istotne znaczenia przy podłączaniu intersieci do systemu komunikacyjnego.

- klasa usług transferu danych;

  Do klasy należą rozwiązania sieciowe, zróżnicowane pod kątem wykorzystywanych mechanizmów transferu danych dla każdej z usług sieciowych. W systemach przemysłowych mogą pojawić się następujące usługi przesyłu, które mogą być potrzebne na rozpatrywanym poziomie wymiany informacji. Są to:

  1. usługa cyklicznego przesyłania danych,
  2. usługa aperiodycznego przesyłania danych,
  3. usługa aperiodycznego przesyłania danych zdeterminowanego w czasie.

  Usługi przesyłu informacji muszą być związane zarówno z dostępem lokalnym, jak i zdalnym. Usługa cyklicznego przesyłania danych w przeciwieństwie do usługi aperiodycznego przesyłania danych wymaga zastosowania zestawu protokołów, który ma w składzie mechanizm gwarantujący zdeterminowany w czasie przesył danych. Jeżeli takiego mechanizmu nie ma, wówczas nie mamy do czynienia z wymianami cyklicznymi. Wynika to z faktu, że aby wymiana była periodyczna, musi być określony przedział czasu, w którym zostanie ona zrealizowana z prawdopodobieństwem równym jeden. Przedział ten jest wówczas miarą niestabilności cyklu, jednak ta niestabilność jest określona i skończona. Dla wymian, gdzie określony jest czas minimalny realizacji transakcji, a czas maksymalny jest nieokreślony, nawet dla przypadku gdy dla

$$\lim_{t \to \infty} P = 1$$

gdzie:

t – czas transakcji,

P – prawdopodobieństwo zakończenia transakcji,

cykl wymian jest niestabilny, a zatem ma charakter aperiodyczny.

Oprócz klasycznej niezdeterminowanej czasowo aperiodycznej wymiany danych, system może potrzebować usługi transmisji aperiodycznej zdeterminowanej w czasie. Jest to usługa, w której czas inicjacji transakcji nie jest przewidywalny na etapie konfiguracji sieci i zależy od jakiegoś wektora stanu systemu. Natomiast czas realizacji tej transakcji jest ściśle określony w przedziale czasu.

- klasa interfejsu użytkownika;

Do klasy należą rozwiązania sieciowe, zróżnicowane pod kątem wykorzystywanych mechanizmów prezentacji informacji użytecznej dla użytkownika. Przykładami mogą tu być:

1) urządzenia specjalizowane,
2) stacje SCADA,
3) standardowe oprogramowanie prezentacyjne protokołów aplikacyjnych.

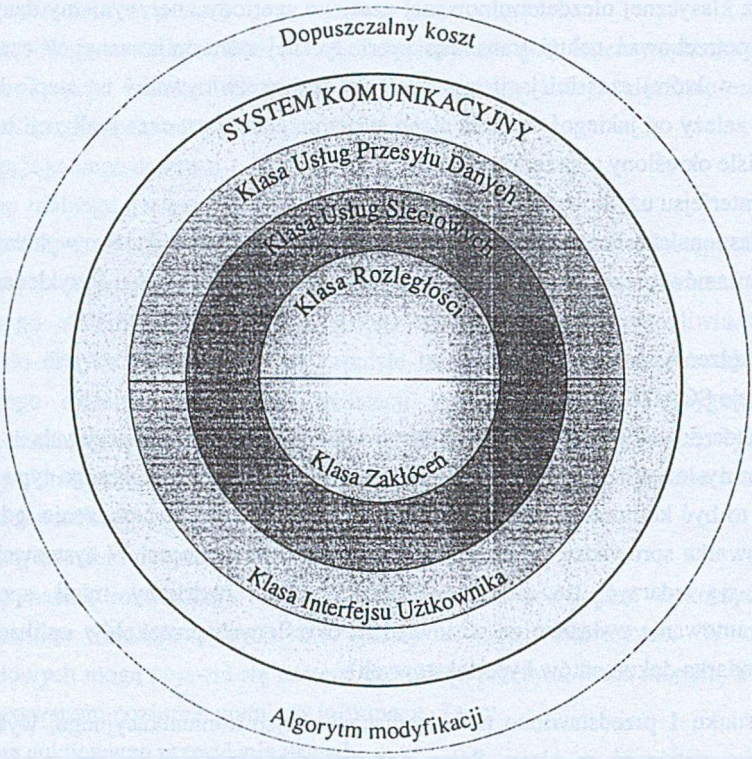
W przemysłowych systemach kontrolnych abonentami sieci są różnego typu urządzenia. Mogą to być komputery, ale najczęściej są to specjalizowane urządzenia, gdzie interfejs użytkownika sprowadza się do kilku lampek lub wyświetlacza. W systemach otwartych może się zdarzyć, że po stronie użytkownika będziemy mieli specjalistyczne oprogramowanie związane ze stosowaniem określonych protokołów aplikacyjnych (np. przeglądarka dokumentów hypertekstowych).

Na rysunku 1 przedstawiono model opisu interfejsu komunikacyjnego, wykorzystujący grupowanie rozwiązań w klasy. Samo zgrupowanie rozwiązań w ramach klas nie jest wystarczające dla wykonania doboru warstw protokołów. Niezbędne jest określenie wymogów, na podstawie których nastąpi wybór danego rozwiązania z klasy.

Istnieją przynajmniej cztery ogólne kryteria, które należy brać pod uwagę projektując warstwę komunikacji przemysłowego systemu kontrolno-nadzorczego. Są to:

1. kryterium procesu,
2. kryterium użytkownika,
3. kryterium bezpieczeństwa dostępu,
4. kryterium ekonomiczne.

Poszczególne kryteria doboru protokołów wymuszają wykorzystywanie zestawów rozwiązań należących do wymienionych powyżej klas. Można jeszcze brać pod uwagę aspekt rozwoju systemu i zastanowić się nad kryterium skalowalności, ale w niniejszym artykule skoncentrujemy się tylko na doborze optymalnego zastawu dla konkretnych potrzeb. Jednak każde nowe kryterium i wzrost liczby klas precyzuje nam bardziej grupę rozwiązań.



Rys. 1. Model interfejsu komunikacyjnego
Fig. 1. Model of communication interface

Kryterium procesu określa nam, jakie wymogi transmisji informacji wymusza charakter obsługiwanego procesu, a konkretnie jego kontroli. Możemy mieć do czynienia z procesem, który ze względów bezpieczeństwa lub poprawności prowadzenia należy kontrolować z wykorzystaniem idei *Hard Real Time* lub *Soft Real Time* [15]. Generalnie kryterium procesu warunkuje użycie protokołów deterministycznych (kryterium klasy T [7]). Jeżeli poprzestalibyśmy tylko na analizie wymogów procesu, od razu można by przejść do mechanizmu zaproponowanego w [7]. Jednak mechanizm ten nie jest najlepszy dla protokołów niedeterministycznych oraz nie uwzględnia innych kryteriów. Rezultatem określania wymogów procesu powinien być zbiór definiujący następujące klasy rozwiązań:

- klasę usług przesyłu informacji,
- klasę rozległości systemu,
- klasę zakłóceń,

Kryterium użytkownika po kryterium procesu jest drugim najważniejszym wyznacznikiem projektowania warstwy komunikacji. To właśnie użytkownik określa, w jaki sposób miałaby zachodzić interakcja pomiędzy nim a systemem, a to warunkuje rodzaj użytej komunikacji. Oczywiście może być tak, że użytkownik zna swoje potrzeby oraz możliwości

systemu, ale często zdarza się, że projektant musi użytkownikowi rozwiązanie zaproponować. Rezultatem określania wymogów użytkownika powinien być zbiór definiujący następujące klasy rozwiązań:

- klasę usług sieciowych,
- klasę rozległości systemu,
- klasę interfejsu użytkownika,

Kryterium bezpieczeństwa dostępu dotyczy możliwości dołączania tymczasowych abonentów do istniejącego systemu informatycznego. Należy rozpatrywać kwestie samej możliwości podłączenia oraz uwierzytelniania, autoryzacji i szyfrowania danych. Kryterium to ma właściwie znaczenie tylko wtedy, gdy wykorzystywane są usługi zdalnego dostępu. Kwestia bezpieczeństwa dostępu w systemach lokalnych jest przeważnie pomijana ze względu na istniejącą fizyczną ochronę dostępu do samego procesu, a zatem do systemu pracującego na tym procesie również. System kontroli stanowi zamkniętą całość, której struktura, zestaw zmiennych, adresacji i abonentów jest opracowywany na etapie projektowania i konfiguracji systemu. Problem może się pojawić, gdy tę zamkniętą całość stanowiącą system lokalny – podstawowy zechcemy modyfikować dynamicznie w trakcie jej pracy. Kwestia bezpieczeństwa dotyczy w takim przypadku dwóch aspektów:

- wprowadzania danych do systemu,
- wyprowadzania danych z systemu.

Zagadnienia z pozoru podobne są z punktu widzenia bezpieczeństwa krańcowo różne. Wprowadzenie danych do systemu może spowodować błędne jego działanie lub działanie niezgodne z celem. Dlatego niezbędne jest prowadzenie procesu uwierzytelnienia dołączanego abonenta i autoryzacji jego dostępu. Uwierzytelnienie zagwarantuje nam, iż podłączany abonent nie spowoduje uszkodzenia systemu, natomiast autoryzacja zapewni, że użytkownik nie wprowadzi zmian w działaniu systemu ponad te, które wolno mu wprowadzić.

Wyprowadzenie danych z systemu jest groźne z innego punktu widzenia. Często informacje przesyłane w systemie mogą posiadać wymierną wartość (np. parametryzacja procesu, algorytm technologiczny itp.), lub mogą przenosić informacje poufne (np. informacje o pracy operatorów itp.). Wówczas niezbędne jest prowadzenie szyfrowania danych. Jeżeli abonent ma tylko korzystać z danych, np. w celu zrealizowania zdalnego podglądu parametrów ruchowych procesu, szyfrowanie jest wystarczającym mechanizmem zabezpieczającym przed niepowołanym do nich dostępem. Rezultatem określania wymogów bezpieczeństwa powinien być zatem zbiór definiujący klasę wykorzystywanych usług sieciowych wraz z określeniem kierunków obsługi danych.

Ostatnim kryterium jest kryterium ekonomiczne, czyli kryterium bezpośrednio powiązane z możliwościami finansowymi inwestora oraz celowością użycia danych rozwiązań

względem wszystkich pozostałych kryteriów. Jest to kryterium innego typu niż poprzednie, gdyż nie wynika z niego żadna klasa rozwiązań.

Bardzo często, szczególnie w polskich realiach, kryterium możliwości finansowych jest nadrzędne. Jest to oczywiste, gdyż jeśli brak odpowiednich środków, to nie sposób zrealizować wymagań użytkownika, bezpieczeństwa czy nawet procesu. Pojawia się zatem możliwość progowego skalowania rozwiązań, gdzie progiem jest dopuszczalny koszt. Do analizy przy doborze rozwiązań ciekawszy jest jednak aspekt ich ekonomicznej optymalizacji. Można powiedzieć, że szybka sieć wraz z pełnym zestawem usług i zabezpieczeń spełni wszystkie kryteria. Pojawia się jednak pytanie, czy taka sieć jest ekonomicznie uzasadniona względem tych kryteriów. Dlatego przy doborze rozwiązań niezbędne jest kryterium zabezpieczające użytkownika przed przepłacaniem. Przydatne jest zatem określenie algorytmu priorytetowej modyfikacji rozwiązań komunikacyjnych w funkcji kosztów. Rezultatem określania wymogów ekonomicznych powinien być zatem zbiór definiujący:

- możliwości finansowe inwestora (próg kosztów),
- zasady priorytetowego zubażania i wzbogacania rozwiązań (algorytm modyfikacji).

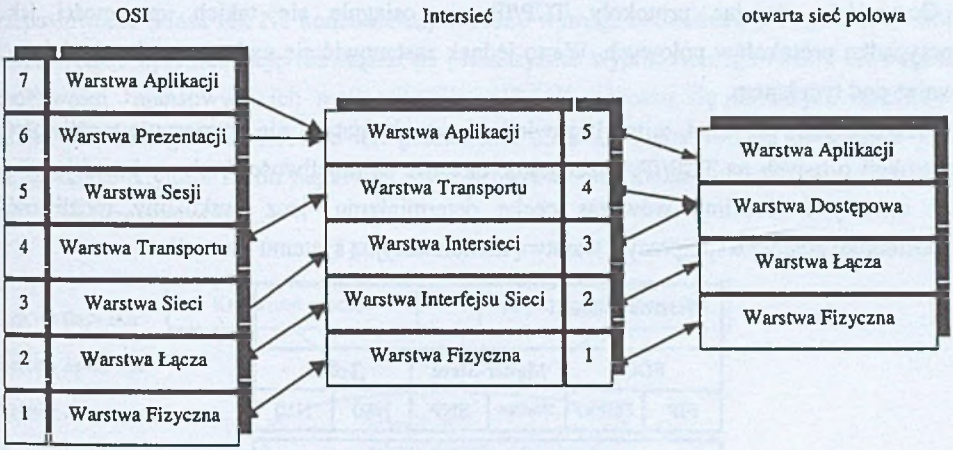
Powyższe kryteria nie są jedynymi, jakie można by stworzyć. Wydaje się natomiast, że dość dobrze klasyfikują istotne parametry rozwiązań komunikacyjnych umożliwiając tym samym ich skuteczny dobór. Kryteria procesu, użytkownika oraz bezpieczeństwa stanowią kryteria systemowe, gdyż pochodzą od elementów składowych systemu. Kryterium ekonomiczne jest kryterium dodatkowym, mającym za zadanie pomóc dopasować skonstruowany system do możliwości i potrzeb inwestora.

3. Możliwości konstrukcyjne interfejsów

Opisując możliwości konstrukcyjne interfejsów komunikacyjnych abonentów sieciowych wygodnie jest korzystać z modelu warstwowego budowy tych interfejsów. W tym celu w dalszej części artykułu posiłkować się będziemy standardem siedmiowarstwowym OSI oraz modelem pięciowarstwowym intersieci [1].

Sieci polowe (sieci przemysłowe) zarówno z jednego, jak i z drugiego modelu praktycznie wykorzystują tylko warstwę fizyczną, łącza i aplikacji. Reszta warstw nie jest potrzebna ze względu na charakter pracy sieci. Na potrzeby uwzględnienia możliwości zdalnego dołączania abonentów do sieci polowej należy w stosie protokołów tejże sieci wykorzystać dodatkową warstwę, która będzie obsługiwać dane ze strumienia przetwarzanego poza systemem lokalnym. Warstwa taka będzie musiała obsłużyć zadania

intersieciowe łączenie z mechanizmami bezpieczeństwa dostępu. Dla uproszczenia warstwę fizyczną i łącza będziemy dalej traktować jako warstwy fizyczne.



Rys. 2. Modele warstwowe sieci
Fig. 2. Models of network layers

W praktyce jeżeli nie chcemy tworzyć nowych protokołów, to nie ma możliwości korzystania z poszczególnych warstw protokołów polowych w odseparowaniu od innych, a w szczególności nie możemy dołożyć nowej warstwy pomiędzy warstwy istniejące. Zatem nie sposób zmodyfikować protokół MODBUS czy WorldFIP przystosowując go do pracy w środowisku intersieciowym. Dokonanie tego jest możliwe jedynie przez rozseparowanie sieci polowej od intersieci przez zastosowanie specjalizowanej bramy [4, 5].

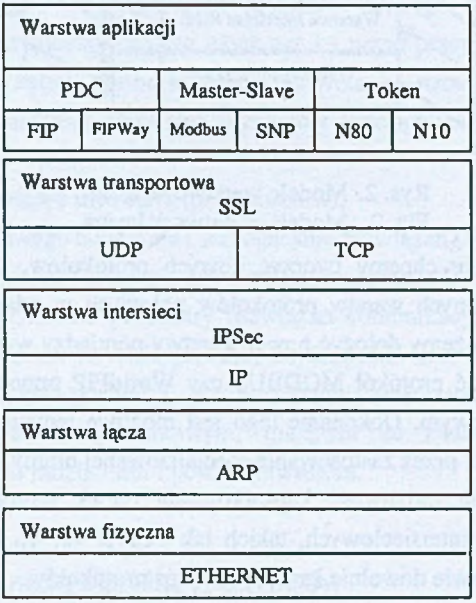
Alternatywą staje się możliwość kapsułkowania ramek protokołów przemysłowych w pakietach protokołów intersieciowych, takich jak TCP/IP [2, 4]. Dla tak konstruowanej komunikacji możemy prawie dowolnie kształtować stos protokołów.

Warstwa fizyczna i warstwa łącza muszą wystąpić w każdym rozwiązaniu ze względu na fakt, iż w każdej sieci musi istnieć mechanizm współpracy z medium transmisyjnym oraz mechanizm obsługi ramek i kontroli poprawności ich transmisji. Z punktu widzenia doboru warstw najistotniejsza jest możliwość modyfikacji warstwy dostępowej (transportowej) oraz aplikacji. Na rysunku 3 został przedstawiony schemat interfejsu opartego na protokołach TCP/IP. Interfejs zakłada przesyłanie danych użytecznych z wykorzystaniem deterministycznego mechanizmu wymiany danych zaimplementowanego na poziomie warstwy aplikacji oraz mechanizmu bezpiecznego połączenia z uwierzytelnieniem, autoryzacją i szyfrowaniem danych zaimplementowanego na poziomie warstwy transportowej lub intersieci. Dzięki umieszczonemu najwyżej mechanizmowi kontroli wymian całość przepływu informacji w sieci staje się zdeterminowana w czasie, pomimo niedeterministycznym metodom dostępu do łącza (CSMA/CD) na poziomie standardu

ETHERNET. Dzieje się tak, o ile sieć jest siecią wydzieloną bez możliwości realizacji usług zdalnych, czyli inaczej jest siecią zamkniętą.

Oczywiście stosując protokoły TCP/IP nie osiągnie się takich sprawności jak w przypadku protokołów polowych. Warto jednak zastanowić się nad optymalizacją doboru również pod tym kątem.

Przedstawiony przykład, mimo iż zawiera szereg alternatyw, nie wyczerpuje możliwości konstrukcji opartych na TCP/IP. Szczególnie ciekawe są możliwości budowy interfejsu dla sieci otwartych. Tracimy wówczas cechę determinizmu, lecz zyskujemy możliwość bezpośredniej zdalnej współpracy z warstwą komunikacyjną systemu kontroli.

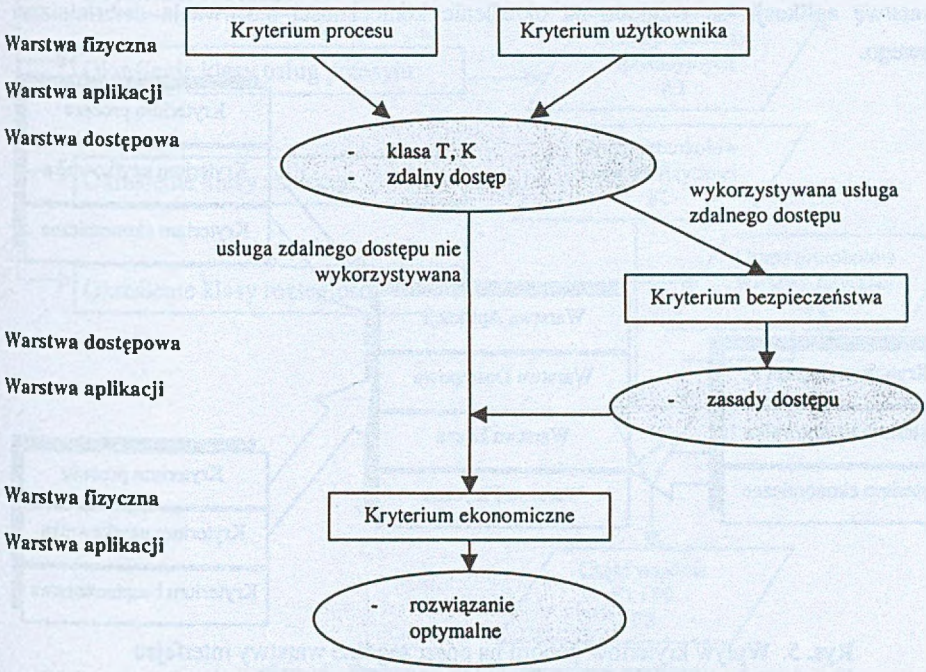


Rys. 3. Przykłady konstrukcji interfejsu opartego na TCP/IP
Fig. 3. Sample of interface construction based upon TCP/IP

4. Dobór warstw protokołów

Przedstawione wcześniej kryteria można stosować zarówno w celu przeprowadzenia doboru całych zestawów protokołów, jak i do selekcji poszczególnych warstw, z których można utworzyć optymalny zestaw. Algorytm korzystania z kryteriów jest prosty. Punktem wyjściowym do analizy jest określenie wymogów z kryterium procesu oraz kryterium użytkowników. Wyznaczony rodzaj usług przesyłu oraz rodzaj interfejsu użytkownika determinuje klasę T protokołów, natomiast wyznaczony rodzaj usług sieciowych określi nam

sposób dołączania abonentów oraz konieczność korzystania z kryterium bezpieczeństwa. Dla otrzymanego zbioru rozwiązań można stosować kryteria ruchu [7] w celu dobrania przepustowości (klasa K). Na końcu należy określić wymogi ekonomiczne i zgodnie z nimi przeprowadzić optymalizację rozwiązań na płaszczyźnie wypracowanego zbioru rozwiązań i możliwości finansowych ich realizacji. Klasy T i K odnoszą się do całych zestawów protokołów, dlatego bezpośrednie ich przełożenie na analizę warstwową nie zawsze jest realizowalne. Kryteria ruchu najłatwiej jest zastosować dla finalnej konstrukcji, testując ją pod kątem przepustowości.



Rys. 4. Schemat doboru rozwiązania z wykorzystaniem kryteriów
Fig. 4. Schema of solution selection based upon criteria using

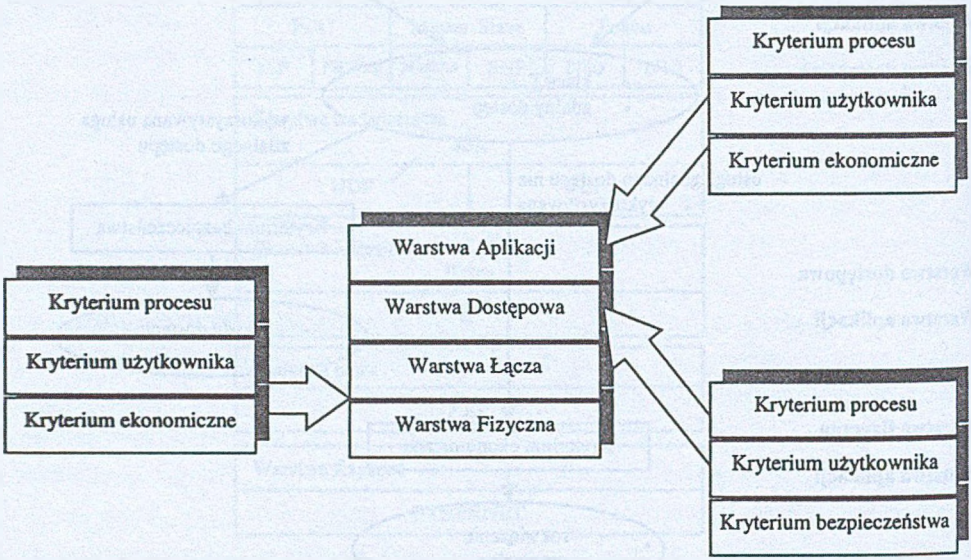
Na rysunku 4 przedstawiono schemat postępowania przy doborze rozwiązania bazując na przedstawionych powyżej kryteriach. Szare pola zawierają grupy rozwiązań z cechami określonymi na podstawie analizy wcześniejszych kryteriów.

W kwestii zależności przedstawionych kryteriów z warstwami protokołów interfejsu należy przeanalizować rysunek 1 pod kątem zależności pomiędzy klasami rozwiązań a warstwami protokołów. Na rysunku 1 środek modelu stanowią warstwy fizyczne, natomiast każdy kolejny pierścień systemu komunikacyjnego odzwierciedla kolejne warstwy protokołów. Możemy zatem stwierdzić, iż kryteria procesu i użytkownika mają bezpośredni wpływ na warstwę aplikacji oraz określają konieczność istnienia warstwy dostępowej.

Natomiast kryterium bezpieczeństwa wpływa tylko na konstrukcję tejże warstwy dostępowej. Warstwy niższe zależą głównie od kryterium procesu, użytkownika i ewentualnie od aspektów ekonomicznych.

Na rysunku 5 zostały przedstawione zależności pomiędzy poszczególnymi kryteriami a warstwami protokołu. Z rysunku tego wyraźnie widać, że najistotniejsze przy doborze są kryteria procesu i użytkownika. Wpływają ona na każdą z warstw interfejsu.

Proces może wymuszać rodzaj warstwy fizycznej ze względu na swój charakter (np. generowanie silnych zakłóceń) lub lokalizację (np. konieczność stosowania radia). Może również wymagać zdalnej parametryzacji i monitoringu. Najistotniejszy jednak wpływ ma on na warstwę aplikacji, ze względu na określenie konieczności stosowania determinizmu czasowego.

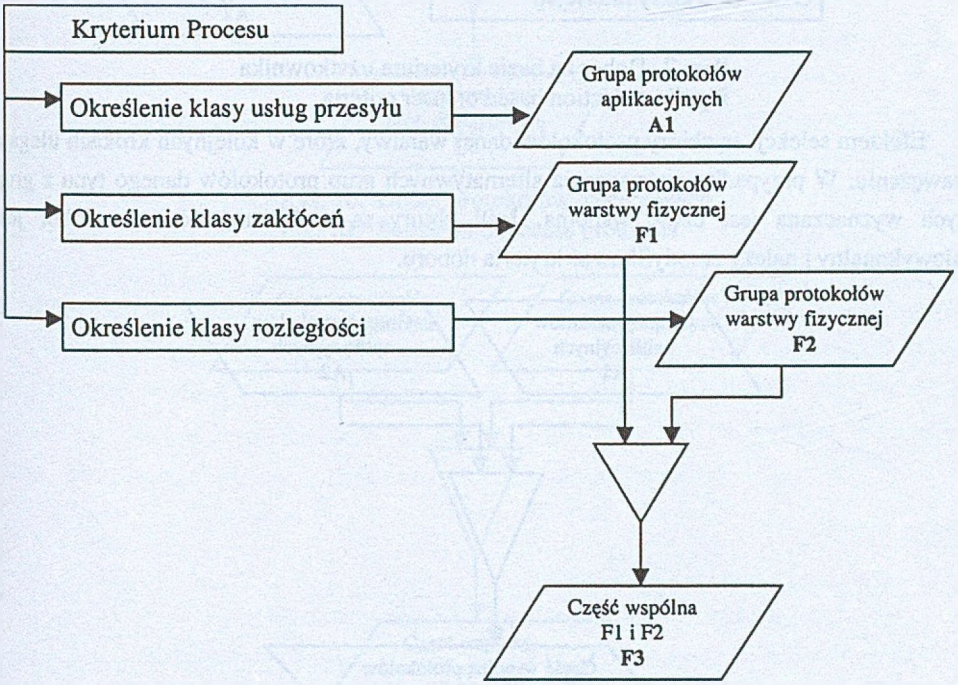


Rys. 5. Wpływ kryteriów doboru na poszczególne warstwy interfejsu
Fig. 5. Selection criterions influence on individual interface layer

Na dobór medium mogą wpływać również preferencje użytkownika (np. użytkownik może wymagać mobilności). Użytkownik podobnie jak proces może wymagać zdalnego dostępu do systemu. Może on również specyfikować rodzaj użytego interfejsu aplikacyjnego, a więc wpływać na wykorzystywane protokoły aplikacyjne.

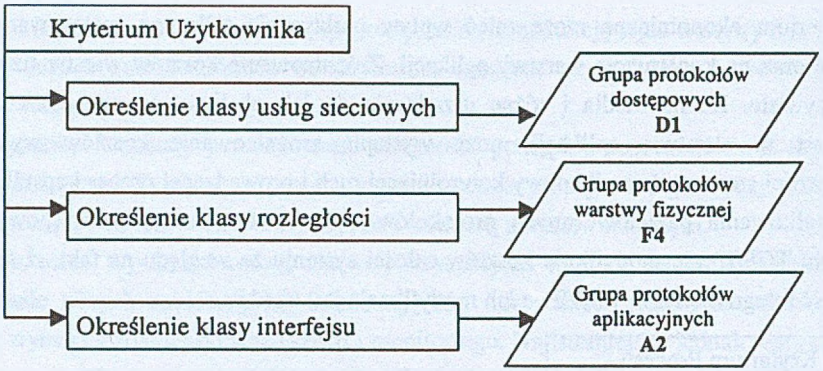
Kryterium bezpieczeństwa, jeśli jest brane pod uwagę, określa tylko budowę warstwy dostępowej, a konkretnie stosowanie mechanizmów uwierzytelniania, autoryzacji i szyfrowania danych. Jeżeli kryteria procesu i użytkownika nie wymagają usług zdalnego dostępu, warstwa dostępowa może zostać pominięta, tworząc tym samym zamknięty system komunikacyjny.

Kryterium ekonomiczne może mieć wpływ praktycznie tylko na zastosowane łącze fizyczne oraz na konstrukcję warstwy aplikacji. Zróżnicowanie kosztów warstw fizycznych jest oczywiste. Różne media i różne urządzenia do ich obsługi generują różne koszty. Natomiast w warstwie aplikacji może wystąpić zróżnicowanie kosztów wynikające z możliwości stosowania nadbudowy kontrolującej ruch i prowadzącej proces kapsułkowania i dekapsułkowania pakietów innych protokołów. Zastosowanie warstw dostępowych dla protokołu TCP/IP nie modyfikuje kosztów całości systemu ze względu na fakt, iż stanowią one część integralną stosu TCP/IP, a ich modyfikacja jest zbędna.



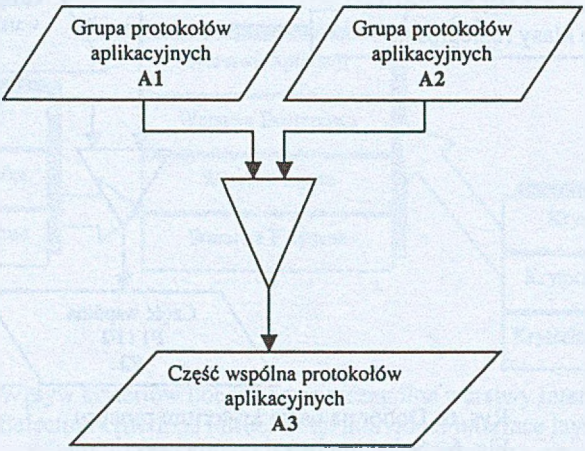
Rys. 6. Dobór na bazie kryterium procesu
Fig. 6. Selection based on process criteria

Można zatem pokusić się o zbudowanie ogólnego algorytmu doboru bazującego na przedstawionych kryteriach oraz klasach rozwiązań. Na rysunku 6 oraz na rysunkach poniższych przedstawiono algorytm postępowania dla poszczególnych kryteriów.

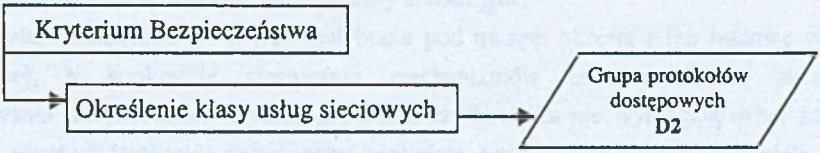


Rys. 7. Dobór na bazie kryterium użytkownika
Fig. 7. Selection based on user criteria

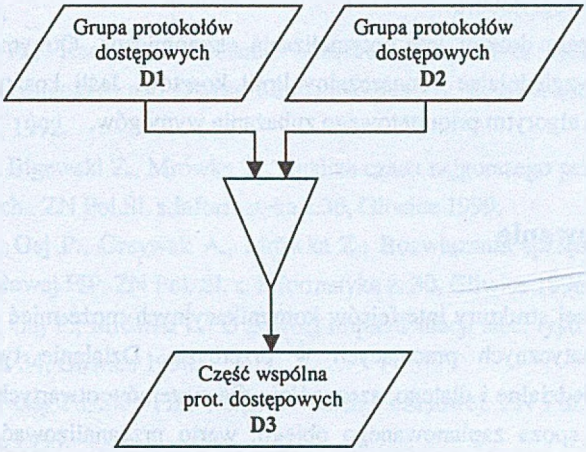
Efektem selekcji są zbiory protokołów danej warstwy, które w kolejnych krokach ulegają zawężeniu. W przypadku wyznaczenia alternatywnych grup protokołów danego typu z grup tych wyznaczana jest część wspólna. Jeśli zbiory są rozłączne, wówczas dobór jest niewykonalny i należy zmodyfikować kryteria doboru.



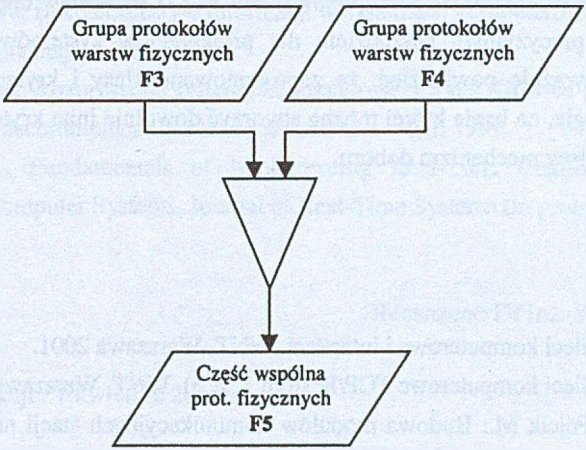
Rys. 8. Dobór protokołów aplikacyjnych
Fig. 8. Selection of application protocols



Rys. 9. Dobór na bazie kryterium bezpieczeństwa
Fig. 9. Selection based on security criteria



Rys. 10. Dobór protokołów dostępowych
Fig. 10. Selection of access protocols



Rys. 11. Dobór protokołów warstw fizycznych
Fig. 11. Selection of physical protocols

Otrzymane grupy protokołów A3, D3 i F5 spełniają wymogi systemowe, a co za tym idzie są wystarczające i optymalne do zbudowania wymaganego systemu komunikacyjnego. Kolejnym krokiem jest optymalizacja zbioru względem kryterium ruchu oraz kryterium ekonomicznego.

Dla poddania analizie ruchu niezbędne jest wykonanie analizy czasowej otrzymanego zestawu i wyznaczenia przepustowości minimalnej i maksymalnej. Na tej podstawie można dokonać dobrania rozwiązania optymalnego względem kryterium ruchu (klasa K). Jeżeli

z kryterium ruchu okaże się, iż protokoły nie spełniają wymogu przepustowości, należy zmodyfikować wymogi doboru.

Kolejnym etapem doboru jest optymalizacja ekonomiczna. Otrzymany zestaw należy poddać ocenie uwzględniając dopuszczalny limit kosztów. Jeśli koszty są przekroczone, należy zastosować algorytm priorytetowego zubażania wymogów.

5. Podsumowanie

Dobór właściwej struktury interfejsów komunikacyjnych może mieć duże znaczenie dla systemów informatycznych pracujących w przemyśle. Działanie tych systemów jest niezwykle odpowiedzialne i dlatego, szczególnie dla systemów otwartych, gdzie pojawić się może informacja spoza zaplanowanego obiegu, warto przeanalizować, jakie są wymogi stawiane przed tym systemem. Na tej podstawie można dobrać rozwiązanie bezpieczne, które zadowoli obsługę procesu, użytkownika systemu jak i inwestora, co nie jest bez znaczenia. W połączeniu z mechanizmami zaproponowanymi w [7] przedstawione propozycje metod doboru są dość precyzyjnym narzędziem dla projektantów systemów komunikacyjnych. Należy jednak wyraźnie powiedzieć, że zaproponowane klasy i kryteria są przykładowe. Istotna jest ideologia, na bazie której można stworzyć dowolnie inne kryteria i klasy, tworząc jeszcze dokładniejszy mechanizm doboru.

LITERATURA

1. Comer D.: Sieci komputerowe i intersieci. WNT, Warszawa 2001.
2. Comer D.: Sieci komputerowe TCP/IP (tom 1, 2, 3). WNT, Warszawa 2001.
3. Cupek R., Fojcik M.: Budowa modułów komunikacyjnych stacji nadzorczej z sieciami przemysłowymi. ZN Pol. Śl. s. Informatyka z. 32, Gliwice 1997.
4. Cupek R., Kwiecień A.: Ocena przydatności protokołu TCP/IP dla sieci przemysłowych najniższego poziomu. Materiały konferencyjne SCR'01, AGH, Kraków 2001.
5. Cupek R.: Protokół TCP/IP w systemach wizualizacji procesów przemysłowych. ZN Pol. Śl. s. Studia Informatica Vol. 22 Number 3, Gliwice 2001.
6. Cupek R.: Metody hierarchizacji rozproszonych procesów przemysłowych. ZN Pol. Śl. s. Informatyka z. 28, Gliwice 1995.
7. Gaj P., Kwiecień A.: Kryteria doboru protokołów komunikacyjnych w sieciach przemysłowych. ZN Pol.Śl. s.Informatyka z.45 Gliwice 2001.
8. Gaj P.: Szybka sieć przemysłowa a system wizualizacji – problem interfejsu. ZN Pol.Śl. s.Informatyka z.36 Gliwice 1999.

9. Grzywak A.: Bezpieczeństwo w sieciach rozproszonych. ZN Pol. Śl. s. Informatyka z. 24, Gliwice 1993.
10. Halang W. A., Real-Time Systems: Another Perspective, Real Time Systems: Abstractions, Languages and Desing Methodologies, K. M. Kavi (ed.) IEEE Computer Society Press, 1992.
11. Kwiecień A., Bigewski Z., Mrówka Z.: Analiza czasu najgorszego przypadku w sieciach przemysłowych.. ZN Pol.Śl. s.Informatyka z.36, Gliwice 1999.
12. Kwiecień A., Gaj P., Grzywak A., Mrówka Z.: Rozwiązania sprzętowe i programowe sieci przemysłowej FIP. ZN Pol. Śl. s. Informatyka z. 30, Gliwice 1996.
13. Kwiecień A., Gaj P., Mrówka Z.: O pewnej implementacji sieci typu FIP. ZN Pol. Śl. s. Informatyka z. 34, Gliwice 1998.
14. Kwiecień A., Gaj P.: Sieć FIP, wstęp do analizy czasowej. ZN Pol. Śl. s. Informatyka z. 28, Gliwice 1995.
15. Kwiecień A.: Analiza przepływu informacji w komputerowych sieciach przemysłowych. Wydawnictwo Jacka Skalmierskiego, Gliwice 1999.
16. Praca zbiorowa: Bezpieczeństwo informacji w systemach komputerowych. Wydawnictwo Jacka Skalmierskiego, Gliwice 2002.
17. Praca zbiorowa: Rozproszone systemy komputerowe. Pronet, Gliwice 1994.
18. Russell T.: Telecommunications Protocols. McGraw-Hill 1999.
19. Tomgren M., Fundamentals of Implementing Real-Time Control Applications in Distributed Computer Systems, Journal of Real-Time Systems (in press), 1996.

Recenzent: Dr inż. Włodzimierz Boroń

Wpłynęło do Redakcji 17 kwietnia 2002 r.

Abstract

Actually there are many kind of industrial network solutions and many protocols. The main problem in this paper is how we should put together set of protocols on the network subscriber level of control system, with taking detailed into consideration using internetwork in this kind of system, as well as how take note of security point of view of doing this control.

To pass selection one should qualify with which one premises oneself directed accepting or rejecting following solutions. So advisable is existing solutions to group in such manner so that from accepted criterions one can was these groups, named farther classes of solutions, to

lead out. If from row of criterions we will receive gathering of classes, then part common these of classes will be group of optimum - solutions.

We should create following classes of solutions: class wide of system, class of disturbances, class of network services, class of services of transfer given, class of interface of user. On figure 1 one represented model of description of communication interface, using assembling of solutions in classes. Indispensable is qualification of requirements on the ground of which will choice given solutions from class. Exist at least four general criterions, which one should take under attention projecting layer of communication of industrial control system. This are criterion of process, criterion of user, criterion of safety of access, economic criterion.

In practice if we do not want to create of new official protocols, then does not have possibility of profiting from each layers of field protocols in separating from other, and in peculiarities not We can add new layers among existing layers. So not manner to modify protocol MODBUS or WorldFIP adapting him to work in internetworking environment. Execution this is possible only by separate field network from internetwork by use specialised gates [4, 5].

With alternative becomes possibility capsulation of frames of industrial protocols in packs of internetwork protocols such as TCP/IP [2, 4]. For so constructed of communication We can almost at will shape stack of protocols.

One can so to attempt for construction general algorithm of selection basing oneself on introduced criterions and classes of solutions. On drawing 6 and on after-mentioned drawings one represented algorithm of conduct for each criterions. Effect of selection are sets of protocols given layers, which in following steps yield to narrow down.

In case of delimitation of alternative groups of protocols of given type the common part is marked from these groups. If sets are separable then selection is unrealisable and one should modify criterions of selection.