

SYSTEMY POMIAROWO – STERUJĄCE NOWEJ GENERACJI

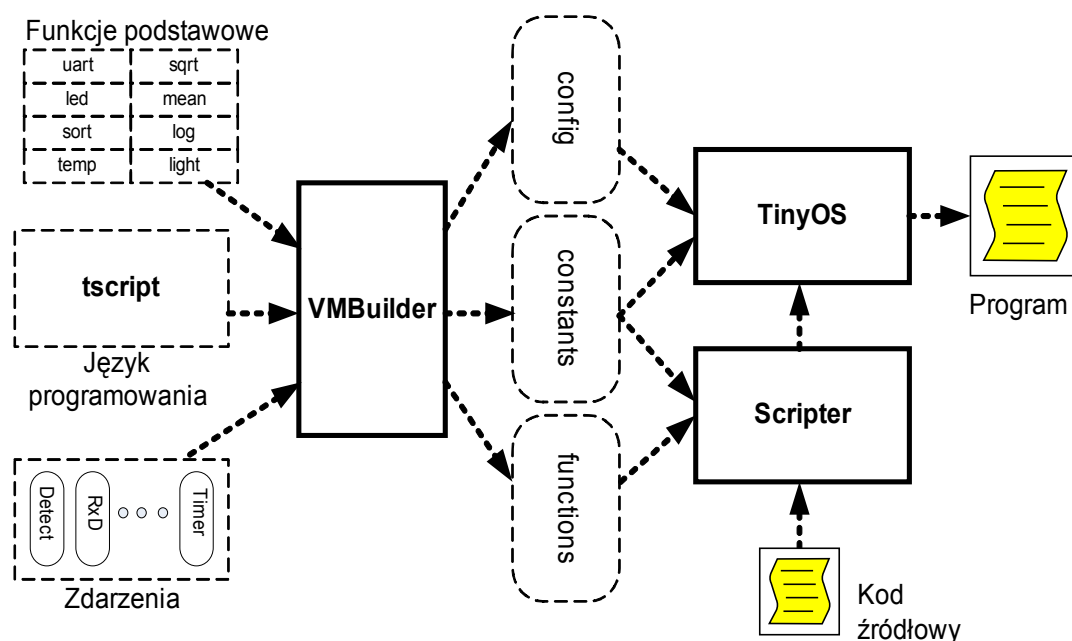
W artykule przedstawiono tendencje rozwojowe w obszarze struktury funkcjonalnej i komunikacyjnej systemów pomiarowo – sterujących nowej generacji. Zwrócono uwagę na rosnącą popularność sieci czujników z transmisją bezprzewodową w standardzie ZigBee. Podkreślono korzyści wynikające z wprowadzenia do systemów pomiarowo – sterujących funkcji routowania. Odniesiono się do zagadnień związanych z formatem XML i bezpieczeństwem przesyłanych danych w systemach pomiarowo – sterujących.

1. WPROWADZENIE

W ostatnich latach dominującym trendem w obszarze systemów pomiarowo – sterujących (SPS) jest wprowadzanie rozwiązań z dziedziny IT. Dotyczy to zarówno sieci i protokołów komunikacyjnych, systemów operacyjnych, technologii internetowych jak i technologii tworzenia oprogramowania dla urządzeń pomiarowo – sterujących stanowiących węzły SPS. Taka sytuacja wynika zarówno z możliwości jakie daje postępująca miniaturyzacja i możliwości stosowanych układów elektronicznych, dążenia do obniżenia kosztów i skrócenia cyklu opracowania urządzeń i systemu jak i wymagań dotyczących traktowania SPS jako element struktury informacyjnej przedsiębiorstwa dostępnej w trybie *on-line*. Jednym ze skutków ubocznych wprowadzania rozwiązań IT i integracji poziomu obiektowego z poziomem biurowym jest możliwość przeprowadzania ataków na SPS, co wymusza wprowadzenie na tym poziomie zabezpieczeń. Interesującym kierunkiem rozwoju SPS jest obszar prostych systemów z komunikacją bezprzewodową tzw. sieci czujników (*Sensor Networks*). W artykule ograniczono się do przedstawienia wybranych tendencji rozwojowych dotyczących struktury SPS, rozwiązań bezprzewodowych stosowanych w sieciach czujników oraz bezpieczeństwa w SPS.

2. OPROGRAMOWANIE SPS

Współczesne SPS są ważnym elementem obiektów, procesów technologicznych i środowiska wspomagającym ich funkcjonowanie lub wręcz niezbędnymi do właściwego ich działania. W strukturze SPS wyróżnia się inteligentne węzły realizujące funkcje przetwarzające związane z pomiarami i/lub sterowaniem oraz funkcje komunikacyjne związane z wymianą informacji pomiędzy węzłami oraz wymianą informacji z aplikacjami użytkownika. Zazwyczaj, w opracowaniu węzła SPS największy jest koszt opracowania i przetestowania oprogramowania. W odniesieniu do tego zagadnienia, interesującą wydają się być koncepcja tworzenia oprogramowania użytkowego węzła polegająca na stosowaniu modułu programowego np. TiniOS, będącego prostym systemem czasu rzeczywistego, który współpracuje z tzw. maszyną wirtualną *Mate VM* opracowaną na Uniwersytecie w Berkeley oraz Intel Research Center w Berkeley [1].



Rys. 1. Elementy architektury Mate VM

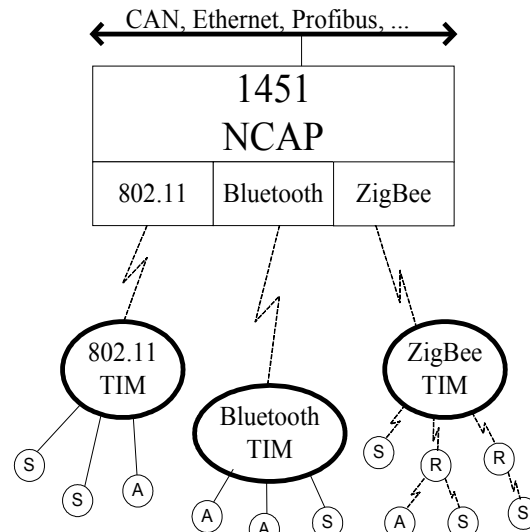
Mate VM jest modulem programowym o architekturze typu „event-driven” wykonującym polecenia prostego języka skryptowego użytkownika. Takie rozwiązanie oprogramowania węzła oznacza, że oprogramowanie użytkownika jest niewielkich rozmiarów, zatem można je szybko i bez obciążania sieci dystrybuować do już zainstalowanych węzłów. Architektura *Mate VM* pozwala użytkownikowi na utworzenie maszyny wirtualnej dopasowanej do potrzeb realizowanej aplikacji, co prowadzi do optymalnego wykorzystania zasobów. Architektura ta definiowana jest poprzez określenie trzech elementów (rys. 1): języka programowania np. TinyScript, wyborze używanych zdarzeń i funkcji podstawowych. Program użytkownika ma postać

3. STRUKTURA SPS

Po wprowadzeniu w 2000r. przez ISA w ramach IEC 61158 zaleceń dotyczących standardów komunikacyjnych, ten element struktury można uznać za zestandaryzowany. Poza standardem IEC 61158, w sieciach komunikacyjnych SPS powszechnie wykorzystuje się Ethernet przemysłowy ze stosem TCP/IP, co wymusiło potrzebę uaktualnienia poprzednio opracowanego standardu do standardu IEC 61784, który obowiązuje od 2003r. [2]. Dostępne obecnie rozwiązania komunikacyjne oferowane dla SPS pozwalają na budowę wielopoziomowej struktury SPS z możliwością przepływu informacji z poziomów najwyższych do poziomu najniższego i odwrotnie. W 2000r. ISA w ramach dokumentu ISA-95.00.01-2000 wyróżniła 4 poziomy przemysłowych SPS: *poziom 0* z konwencjonalnymi lub inteligentnymi czujnikami i elementami wykonawczymi; *poziom 1* z sieciami typu fieldbus, sterownikami PLC, regulatorami, modułami PC i lokalnymi terminalami do monitorowania i nadzorowania procesu; *poziom 2* z siecią Ethernet i z funkcjami koordynacji funkcjonowania warstwy pierwszej z poziomu stacji PC, która stanowi podstawowy interfejs operatora; *poziom 3* z funkcjami planowania i zarządzania. W rzeczywistych rozwiązaniach przemysłowych SPS struktura poziomowa może być różna i wynika ona z rzeczywistych potrzeb danego obiektu lub procesu. Model ISA należy traktować jako model odniesienia i zalecenie a nie obowiązującą zasadę zarówno dla producentów urządzeń jak i dla projektantów systemu.

W ostatnich latach obserwujemy duże zainteresowanie wykorzystaniem komunikacji bezprzewodowej reprezentowanej przez standardy opracowane przez IEEE: 802.11b/g, 802.15.1 (Bluetooth) oraz 802.15.4 (ZigBee). Wymienione standardy transmisji bezprzewodowych wybrano do stosowania w węzłach IEEE 1451.5 (rys. 2). Komunikacja pomiędzy

modułami pomiarowo – wykonawczymi TIM (ang. *Transducer Interface Module*), do których podłączone są czujniki (S), elementy wykonawcze (A) lub routery (R) a modułem sieciowym NCAP (ang. *Network Capable Application Protocol*), stanowiącym powiązanie z siecią przewodową przemysłową. Wykorzystanie transmisji bezprzewodowych pozwala realizować w prosty sposób różne topologie systemu oraz pozwala na mobilność węzłów. Te cechy pozwalają na osiągnięcie takich cech SPS, których nie dawało się łatwo zrealizować w klasycznych, przewodowych SPS.



Rys. 2. Sieci bezprzewodowe w IEEE 1451.5

3. SIECI CZUJNIKÓW

Wśród SPS dużą dynamikę zarówno w obszarze prac badawczych jak i wdrożeniowych obserwuje się w obszarze tzw. sieci czujników (ang. *Sensor Networks*) z transmisją bezprzewodową np. w standardzie ZigBee. Sieci czujników tworzą zwykle duże ilości prostych węzłów realizujących funkcje przetwarzania, funkcje pomiarowe i/lub wykonawcze. Poza modelem przetwarzania typu "*interactive*", który dominował w klasycznych SPS, w sieci czujników poza tym modelem przetwarzania można realizować przetwarzanie typu "*proactive*" [4,5]. W klasycznych rozwiązaniach SPS proste węzły zwykle były na sztywno powiązane z węzłami nadzorującymi a stosowanym modelem komunikacyjnym był model *master-slave*. W nowej generacji sieci pojawiają się węzły nienadzorowane zdolne do nawiązania relacji komunikacyjnych z węzłami sąsiednimi w sposób dynamiczny. Zwykle w tego typu sieciach występuje węzeł realizujący funkcje koordynatora, w którym zarejestrowane są węzły pracujące w danej domenie. Domena jest obszarem, w którym pracują węzły zarejestrowane i skojarzone z węzłem koordynatora. Nowy węzeł może korzystać z istniejącej infrastruktury komunikacyjnej sieci, jeżeli zostanie zarejestrowany i zostanie mu przydzielony adres logiczny. Węzeł pełniący rolę koordynatora najczęściej stanowi bramę do komunikacji ze światem zewnętrznym.

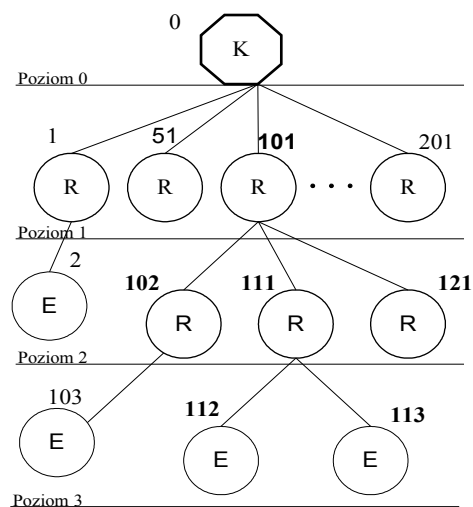
Stosowane powszechnie na przestrzeni ostatnich kilkunastu lat rozwiązania SPS bazujących na sieciach przemysłowych o strukturze magistrali i nośnikach przewodowych będą nadal stosowane, ponieważ rozwiązania bazujące na bezprzewodowych sieciach typu "*multi-hop*" nie są w stanie zagwarantować często wymaganego wysokiego poziomu niezawodności. Transmisje bezprzewodowe cechują się wysoką stopą błędów i nie zapewniają dużej przepustowości. Pomimo tego stanowią one atrakcyjną propozycję dla tej klasy obiektów, które nie wymagają szybkich reakcji na zdarzenia i tolerują występowanie błędów komunikacyjnych.

4. SIECI BEZPRZEWODOWE ZIGBEE

Postępująca miniaturyzacja układów elektronicznych przy jednocześnie rosnących możliwościach przetwarzania danych i coraz powszechniejsze stosowanie transmisji bezprzewodowych w sieciach typu PAN (ang. *Personal Area Network*), które są w obszarze zainteresowania projektantów SPS, otwiera możliwości budowy SPS o nowych właściwościach, które są istotne we wdrażaniu nowego modelu komunikacyjnego dopasowanego do potrzeb przetwarzania typu "proactive". Architektury klasycznych SPS z przewodowymi sieciami przemysłowymi bazują na modelach komunikacyjnych *master – slave* lub *peer to peer* i zwykle stanowią struktury sztywne. Modele te spotykamy również w wielu rozwiązaniach z nośnikiem bezprzewodowym. Ale w sieciach bezprzewodowych ze względu na brak przewodów, istnieją zupełnie inne możliwości związane z budową sieci o różnych architekturach i z mobilnymi węzłami. Przykładem takiego rozwiązania może być sieć ZigBee.

Architektury klasycznych przewodowych sieci przemysłowych (np.: Modbus, Profibus, Interbus-S, CAN, ...) lub klasycznych sieci bezprzewodowych (np.: Bluetooth, WiFi, ...) są dwuwarstwowe i zbudowane są z węzła *master* oraz węzłów *slave*. Taka architektura jest prosta we wdrażaniu i nie stwarza dużych wymagań węzłom pracującym w sieci, natomiast jest ona mało elastyczna np. w sytuacjach awaryjnych wymagających dynamicznej rekonfiguracji logicznej sieci. We współcześnie opracowywanych protokołach komunikacyjnych dedykowanych dla SPS, coraz częściej poza funkcjami przetwarzania spotyka się również funkcję routowania, która może być realizowana przez węzły dedykowane do realizacji tej funkcji, węzły pomiarowe lub sterujące. Przykładem takiego rozwiązania jest protokół sieci bezprzewodowej klasy PAN, ZigBee opracowany przez grupę 802.15.4 oraz grupę *ZigBee Alliance* pozwalający na budowanie sieci o topologii siatki, gwiazdy i gwiazdy rozszerzonej [6].

W sieci ZigBee występują trzy rodzaje węzłów: koordynator (K), router (R) i prosty (E), co stwarza możliwości budowy znacznie bardziej elastycznych architektur SPS dobrze dopasowanych do struktury projektowanego SPS i do potrzeb funkcjonalnych węzłów sieci instalowanych na danym obiekcie. W jednej domenie sieci ZigBee może pracować jeden koordynator, zdefiniowana liczba routerów oraz zdefiniowana liczba węzłów prostych realizujących funkcje pomiarowe lub sterujące. Węzły proste mogą pracować jedynie w topologii gwiazdy, natomiast węzeł routera i koordynatora mogą tworzyć wszystkie możliwe topologie dostępne w standardzie ZigBee. Ponadto występowanie węzłów realizujących funkcje routowania pozwala w sposób dynamiczny zmieniać trasy przesyłania danych w przypadku wystąpienia uszkodzeń na dotychczasowej trasie.



Rys. 3. Struktura logiczna sieci ZigBee.

Konfigurowanie sieci ZigBee wymaga zdefiniowania parametrów globalnych dla warstwy sieciowej, warstwy aplikacji oraz bezpieczeństwa. Parametry globalne niezbędne są dla wę-

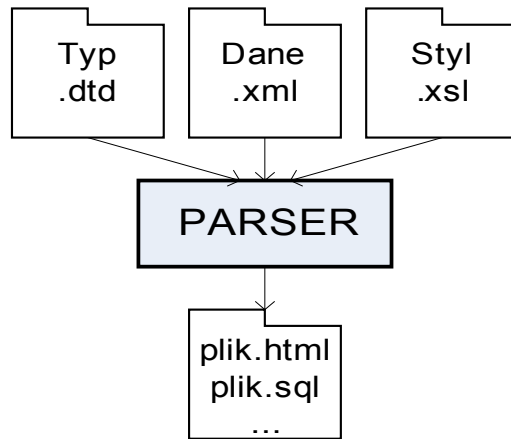
zła koordynatora w celu określenia struktury sieci. Jednym z parametrów globalnych koordynatora jest maksymalna liczba routerów w sieci oraz maksymalna głębokość sieci. Na rys. 3 przedstawiono schemat logiczny sieci ZigBee o głębokości 3. Rozmiar bloku adresowego na poziomie 0 wynosi 50, a na poziomie 1 wynosi 9. Stosowanie funkcji routowania oznacza konieczność wprowadzenia adresowania logicznego, zarządzania adresowaniem oraz określenia rozmiarów domeny, dla której będzie obowiązywał spójny system adresowania logicznego. W sieci ZigBee zarządzanie adresowaniem realizowane jest centralnie poprzez koordynator, który dla swojej domeny posiada 240 adresów logicznych przydzielanych na podstawie maksymalnej liczby węzłów, które może posiadać węzeł koordynatora lub routera, maksymalną liczbę routerów oraz głębokość sieci określającą, przez jaką maksymalną liczbę routerów w sieci może być przesłana informacja.

5. FORMAT DANYCH XML

XML stał się powszechnie wykorzystywanym formatem opisu przesyłanych informacji w Internecie. Korzyści wynikające ze stosowania XML (prosta i czytelna i samodokumentująca się forma dokumentu, szybsza komunikacja, przenośność pomiędzy różnymi platformami) mogą być osiągnięte nie tylko w obszarze Internetu, ale również w obszarze SPS [7]. Przesyłanie informacji pomiarowych lub sterujących w postaci samoopisujących się dokumentów XML ułatwia ich interpretację po stronie odbiorcy. W klasycznych rozwiązaniach po to, ażeby po stronie odbiorcy przesyłane informacje były właściwie odczytywane, należało odbiorcę poinformować jakiego rodzaju informacja i od kogo będzie przychodziła. Jakakolwiek zmiana po stronie nadawcy wymagała zmian po stronie odbiorcy. Takie rozwiązanie w znacznym stopniu ograniczało krąg odbiorców informacji. Poniżej przedstawiono przykład dokumentu XML dla przetwornika ciśnienia:

```
<urządzenie>przetwornik
  <identyfikacja>
    <typ>PT-2000</typ>
    <wielkosc>cisnienie wzgledne</wielkosc>
    <producent>OBR Metrol</producent>
  </identyfikacja>
  <pomiar>
    <jednostka>bar</jednostka>
    <wartosc>24.7</wartosc>
  </pomiar>
  <serwis>
    <instalacja>12.12.2006</instalacja>
    <operator>Nowak Jan</operator>
    <dokladnosc>0.5</dokladnosc>
  </serwis>
</urządzenie>
```

Przyjęta w XML strategia polegająca na rozdzieleniu informacji na mniejsze bloki pozwala na pokonanie niedogodności występujących np. w HTML. Plik XML jest podzielony na trzy części, które mogą być przesyłane razem lub oddzielnie (rys. 4).



Rys.4. Pliki XML

Ponieważ dokument XML zawiera jedynie dane (data.xml), to informacja o strukturze danych (scheme.dtd) i o sposobie ich prezentacji (style.xsl) zawarta jest w dwóch oddzielnych dokumentach. Parser na podstawie informacji z tych trzech części tworzy format końcowy. ISA, po wprowadzeniu unormowania dla standardu komunikacyjnego IEC 61158, a następnie IEC 61784, wprowadziła kolejne unormowanie IEC 61499 dotyczące bloków funkcyjnych w rozproszonych przemysłowych SPS, w którym wykorzystano XML do definicji nowych bloków funkcyjnych proponowanego modelu systemu. Obserwowane w tym obszarze działania oraz rosnąca popularność wprowadzanych profili dziedzinowych lub urzędziowych XML np. SML (*Sensor Markup Language*) wskazują na to, że XML może stać się w niedługim czasie podstawowym językiem wymiany danych w SPS.

6. BEZPIECZEŃSTWO W SPS

Z chwilą, kiedy w SPS zaczęto stosować standardowe protokoły komunikacyjne i systemy operacyjne, a sieci fieldbus stosowane na poziomie obiektu połączono z sieciami komputerowymi na poziomie biurowym lub z Internetem, stały się one narażone na ataki zarówno z wnętrza firmy jak i z sieci poza nią. Sytuacja ta zmusiła projektantów i użytkowników SPS do wdrożenia polityki bezpieczeństwa. W ostatnich kilku latach wzrosła liczba ataków przeprowadzanych na różne obiekty. Skutki ataków mogą być bardzo różne i najczęściej zależą od rodzaju obiektu. Oficjalnie nie jest prowadzona statystyka takich ataków, ale do najbardziej spektakularnych należy zaliczyć ataki na system sterowania gazociągami Gazprom w Rosji (1998), stację uzdatniania wody w Queensland w Australii (2000), system zabezpieczeń w elektrowni atomowej w Davise-Besse w USA (2003). W sierpniu 2003 oraz w maju 2004 zaatakowane zostały systemy sygnalizacji i sterowania firm kolejowych CSX Transportation w USA oraz RailCorp w Australii. Skutek ataków był taki, że przez połowę dnia nie kursowały pociągi [8].

W 2004r., uznana firma konsultingowa ARC opublikowała wyniki przeglądu dotyczącego stosowanych technik zabezpieczeń wśród wybranych aplikacji przemysłowych SPS [9]. W 5% analizowanych przypadków SPS, które były podłączone do sieci zewnętrznych nie stosowano żadnych zabezpieczeń a 34% systemów było izolowanych od sieci zewnętrznych. W 24% systemów stosowano sprzętowe zapory ogniowe, a w 18% zapory ogniowe i programy antywirusowe. W 14% systemów stosowane były kanały szyfrowane VPN.

Trudność w rozwiązywaniu zagadnień związanych z bezpieczeństwem polega na tym, że poziom zabezpieczeń jest związany zarówno z kosztami, które należy ponieść w celu wdrożenia takiej architektury systemu, która będzie odporna na ataki, jaki i kosztami wynikającymi ze skutków udanych ataków. Z projektowego punktu widzenia istnieją dwa podejścia w rozwiązywaniu tego problemu. Jedno polega na podejściu "*Defense-in-depth*", polegające na zaprojektowaniu kilku stref ochronnych, a drugie "*hard perimeter*", polegające na utworzeniu jednego potężnego, trudnego do sforsowania „muru” zabezpieczającego.

Rosnąca liczba skutecznych ataków na SPS spowodowała zapotrzebowanie na opracowanie standardu lub przewodnika związanego z tworzeniem bezpiecznych architektur SPS. Jako jedno z pierwszych zaleceń dotyczące technik zabezpieczeń dla SPS należy uznać opracowanie w ramach ISA przez komitet SP99 (*Manufacturing and Control System Security*) standardu S99 opublikowanego w 2004r [10]. Równolegle w 2004r. grupa robocza WG10 komitetu TC65 IEC rozpoczęła prace nad wprowadzeniem profili bezpieczeństwa dla protokołów komunikacyjnych typu fieldbus zdefiniowanych w standardzie IEC 61784. Profile komunikacyjne związane z bezpieczeństwem zostaną ogłoszone w 2006r. jako standard IEC 62443 (*Security for Industrial Process Measurement and Control – Network and System Security*), natomiast głosowanie nad końcową wersją zaplanowano w połowie 2007r.

LITERATURA

- [1] Levis P., Culler D.: A Tiny Virtual Machine for Sensor Networks.
www.cs.berkeley.edu/~pal/pubs/mate.pdf
- [2] Felser M.: The Fieldbus Standards: History and Structure. Technology Leadership Day, 2002, Organised by MICROSWISS Network, HTA Luzern, Oktober 2002. staff.hti.bfh.ch
- [3] Cornett K.: Standard for a Smart Transducer Interface for Sensor and Actuators – Wireless Communication Protocols and TEDS Formats. Motorola, June 2003.
grouper.ieee.org/groups/1451/5/2003/P1451.5
- [4] Akyildiz I., F., Su W., Sankarasubramaniam Y., Cayirci E.: A Survey on Sensor Networks. IEEE Communication Magazine, August 2002, pp. 102-114.
- [5] Sikora A.: Design Challenges for short-range wireless networks. IEE Proceedings – Communications on line no.20040742, 2004.
- [6] ZigBee Specification. ZigBee Alliance, June 2005.
- [7] Pinceti P.: How will XML impact industrial automation. www.isa.org, June 2002.
- [8] Zdung D., Naedele N., von Hoff T., Cervatin M.: Security for Industrial Communication Systems. Proceedings of the IEEE, Vol. 93(6), June 2005, pp. 1152-1177
- [9] Forbes H.: Plant Floor Network Practices In Today's Factories and Plants. ARC 2004-53EMHLP, December 2004.
- [10] ISA SP99: Security Technologies for Manufacturing and Control Systems, Instrumentation Systems and Automation Society. ISA-TR99.00.01-2004, March 2004.