BIBLIOTEKA INFOTELA

KOMUNIKACJA ELEKTRONICZNA DLA SŁUŻB MUNDUROWYCH

Cena 15 zł (w tym 0% VAT)
ISBN 83-921962-4-4

- Sieci nowej generacji
- Telefonia VoIP
- Komputery specjalistyczne
- Urządzenia zasilające
- Radiotelefony i radiostacje
- Systemy transmisji danych
- Systemy nadzoru
- Systemy okablowania strukturalnego

DIALOG
ekspert w telekomunikacji

Bezpieczny DIALOG

Telefonia DIALOG S.A. posiada

Świadectwo Bezpieczeństwa Przemysłowego

DIALOG zapewnia najwyższą jakość usług telefonicznych i internetowych oraz gwarantuje światowe standardy ochrony informacji.

→ JAKOŚĆ

→ ZAUFANIE

→ BEZPIECZEŃSTWO

www.dialog.pl | TeleCentrum 0 801 700 700

MGE UPS SYSTEMS

PULSAR STS 16
redundancja
zasilania
dla odbiorów
jednofazowych

PULSAR EVOLUTION
od 500 do 3000 VA
rack od 1 do 2U

COMET EX RT
on-line, 7/11 kVA
rack 6U

MGE
UPS SYSTEMS

www.mgeups.pl
022 511 83 45
mgeups@mgeups.pl

ISBN 83-921962-4-4
Cena 15 zł (w tym 0% VAT)
Nakład: 7000 egz.

Wydawca:

MSG – Media s.c.
ul. Stawowa 110
85-323 Bydgoszcz
tel. (52) 325 83 10
fax (52) 373 52 43
office@msgmedia.pl
www.techbox.pl

Redakcja
Marek Kantowicz
Grzegorz Kantowicz
Robert Błaszczyk

DTP
Czesław Winiecki

Marketing
Janusz Fornalik
Arkadiusz Damrath

Korekta
Ewa Winiecka

Druk
Drukarnia ABEDIK
Sp. z o.o.
85-861 Bydgoszcz
ul. Glinki 84
tel./fax (52) 370 07 10
info@abedik.pl
www.abedik.pl

SPIS TREŚCI

www.zpas.pl
www.zpas.net

Obudowy teleinformatyczne

Obudowy energetyczne

Szafy zewnętrzne dostępowe

Okablowanie strukturalne
i osprzęt telekomunikacyjny

Pulpity dyspozytorskie i sterownicze
oraz synoptyczne tablice mozaikowe

System nadzoru
ZPAS Control Oversee

Najlepszy polski wyrób
na targach Intertelecom 2005

ZPAS

Telefon: 074 / 872 0 100 (centrala)
Faks: 074 / 872 40 74, 872 55 92
e-mail: info@zpas.pl
Internet: http://www.zpas.pl

ZPAS-NET

Telefon: 074 / 872 0 122 (sekretariat)
Faks: 074 / 872 58 56
e-mail: info@zpas.net
Internet: http://www.zpas.net

Szkoccy policjanci przechodzą na Microsoft

Policja Centralnej Szkocji (Central Scotland Police) oraz Microsoft ogłosiły, iż system Microsoft Windows został wybrany jako platforma, na której będzie opierała się infrastruktura IT szkockich sił policyjnych. Zgodnie z nowym kontraktem, Policja Centralnej Szkocji wymieni technologie open source na rozwiązania Microsoft Windows Server 2003, Microsoft Windows XP oraz Microsoft Office 2003. Wymiana obejmie ponad 550 stacji roboczych oraz serwerów i, co ważne, nie wymusi na Policji Centralnej Szkocji dodatkowych kosztów związanych z modernizacją komputerów. Celem zmian jest wsparcie procesu modernizacji sił policyjnych, elastyczne zarządzanie pracą oraz usprawnienie współpracy z innymi partnerami sektora publicznego.

Policja Centralnej Szkocji będzie ściśle współpracowała z firmą Microsoft przy realizacji wielu projektów teleinformatycznych (ICT – *Information and Communication Technology*). Dotyczy to między innymi systemu zarządzania dokumentami elektronicznymi, umożliwiającego sprawniejsze reagowanie na wnioski składane na podstawie ustawy o swobodnym dostępie do informacji (*Freedom of Information Act*) oraz wewnętrznego udostępniania dokumentów pomiędzy pracownikami policji.

– *Policja Centralnej Szkocji zawsze poszukiwała perspektywicznych rozwiązań teleinformatycznych w celu ochrony społeczeństwa oraz skutecznej i ekonomicznej obsługi społeczności lokalnych* – powiedział **David Mulhern**, zastępca szefa Policji Centralnej Szkocji.

– *Biorąc pod uwagę obecne uwarunkowania ochrony bezpieczeństwa, coraz większego znaczenia nabiera stosowanie standardów ogólnokrajowych przez jednostki lokalne i usprawnianie komunikacji pomiędzy instytucjami wymiaru sprawiedliwości. Krytyczne znaczenie ma również współpraca z zaangażowanym, wiarygodnym i świadomym zagadnień ekonomicznych partnerem, który dzieli tę samą wizję i zna wyzwania, przed którymi stoją obecnie jednostki policji.*

Zgodnie z filozofią ochrony porządku publicznego „Safer Central" (zob. poniżej), stanowiącą podstawę obecnej działalności Policji Centralnej Szkocji oraz z „Operation Advance", jednym z pięciu operacyjnych filarów tej metody (zob. poniżej), jednostki policji koncentrują się obecnie na poprawie efektywności w celu usprawnienia obsługi społeczności lokalnych w centralnej Szkocji. Istotnym elementem tego procesu jest optymalne wykorzystanie posiadanych środków finansowych. Wewnętrzne badania przeprowadzone na początku 2005 roku wykazały, że infrastruktura IT stworzona w celu osiągnięcia poprawy działania policji i obniżenia kosztów działania powinna mieć następujące cechy:

- ✔ wykorzystanie typowego oprogramowania z półki zamiast aplikacji specjalnie tworzonych na potrzeby policji,
- ✔ interoperacyjność z systemami innych organizacji publicznych,
- ✔ ułatwienie pracy funkcjonariuszom poprzez umożliwienie im korzystania ze znanych technologii,
- ✔ zredukowanie liczby systemów operacyjnych,
- ✔ zwiększenie dostępu do szerokiego asortymentu oprogramowania.

Wynikiem kolejnego studium zakończonego w marcu 2005 roku było rozpoczęcie procesu negocjacji z Microsoft, który zakończył się obecnie podpisaniem trzyletniego kontraktu Enterprise Agreement.

– *Bardzo cieszy nas decyzja podjęta przez Policję Centralnej Szkocji, dzięki której będziemy mogli zademonstrować wartość produktów Microsoft, w tym ich wysoką kompatybilność. Jesteśmy niezwykle zainteresowani współpracą z policją w zakresie wprowadzania nowych produktów i usług, takich jak systemy zarządzania dokumentami i aktami oraz obsługi pracy zespołowej* – powiedział **Terry Smith**, członek kadry zarządzającej w firmie Microsoft.

Analiza korzyści doprowadziła Policję Centralnej Szkocji do decyzji o zastąpieniu wprowadzonego w 2000 roku rozwiązania, wykorzystującego oprogramowanie open source, przez produkty firmy Microsoft. Uznano, że system Microsoft Windows umożliwia optymalne wykorzystanie zaangażowanych środków finansowych i uzyskanie najlepszej funkcjonalności operacyjnej. W niektórych obszarach utrzymane zostaną jednak aktualne instalacje oprogramowania open source.

– *Choć rozwiązania open source spełniały w przeszłości nasze wymagania, to jednak coraz trudniejsze stawało się utrzymywanie tej infrastruktury w dzisiejszym silnie zintegrowanym środowisku informatycznym* – powiedział **David Stirling**, szef IT Policji Centralnej Szkocji. – *W miarę wzrostu zapotrzebowania na integrację i kompatybilność z innymi instytucjami wymiaru sprawiedliwości oraz naszymi partnerami w społecznościach lokalnych coraz większego znaczenia nabiera posiadanie podobnej infrastruktury. Zastosowanie infrastruktury opartej przede wszystkim na produktach firmy Microsoft to znakomity punkt wyjścia do dalszej integracji.*

Decyzja o wdrożeniu Microsoft Windows i Microsoft Office przyniesie Policji Centralnej Szkocji szereg korzyści. Przeprowadzona analiza wykazała, że jednostki policji uzyskają w skali roku znaczne oszczędności.

– *Wewnętrzne analizy policji wykazały, iż platforma Microsoftu jest najlepszym rozwiązaniem po wzięciu pod uwagę takich czynników, jak całkowite koszty utrzymania infrastruktury, przyjazność dla użytkownika, interoperacyjność, dostępność oraz wsparcie techniczne* – powiedział **Nick McGrath**, szef działu Platform Strategy w firmie Microsoft. – *Policja Centralnej Szkocji przewiduje, iż dzięki użyciu technologii Microsoft może zaoszczędzić 30 proc. kosztów utrzymania infrastruktury IT oraz 25 proc. czasu pracowników.*

Dzięki umowie z firmą Microsoft Policja Centralnej Szkocji będzie również mogła wprowadzić nowe metody pracy funkcjonariuszy terenowych.

– *Dotychczas nasi funkcjonariusze korzystali z narzędzi IT jedynie w komisariatach. Był to dla nas autentyczny problem podczas podejmowania decyzji dotyczących strategii reagowania na potrzeby społeczne* – dodał David Mulhern. – *W przyszłości funkcjonariusze będą mogli przebywać w miejscach, w których są najbardziej potrzebni, dysponując jednocześnie dostępem do pełnej gamy rozwiązań IT, zwiększających efektywność ich pracy.*

Główny inspektor ds. operacyjnych, **Alan Douglas**, powiedział: – *Jeśli funkcjonariusze będą mogli wykonywać swoje obowiązki bez ograniczenia dostępu do rozwiązań IT w jednej lokalizacji, usunięta zostanie przeszkoda w ich efektywnej pracy w miejscu, w którym mogą być najbardziej użyteczni.*

Wdrożenie platformy Microsoft rozpoczęło się w sierpniu, po zakończeniu akcji ochrony szczytu grupy G8 przez Policję Centralnej Szkocji.

Safer Central to podstawowa filozofia działania Policji Centralnej Szkocji. Stanowi podstawę procesu obsługi

potrzeb społeczności lokalnych poprzez logiczną analizę posiadanych informacji. Fundamentem Safer Central jest poznanie potrzeb społeczności lokalnych i właściwe na nie reagowanie. Metoda ta jest przekładana na codzienne działania policji za pomocą pięciu filarów operacyjnych: Safeguard, Overlord, Reassurance, Tundra and Advance.

Operation Advance to stosowana przez Policję Centralnej Szkocji metoda wsparcia czterech pozostałych filarów operacyjnych programu Safer Central. Jej przedmiotem jest pomyślne wdrożenie głównych inicjatyw i programów strategicznych, realizowanych obecnie przez jednostki policji. Te inicjatywy nieustannie przekształcają sposób pełnienia obowiązków przez Policję Centralnej Szkocji dzięki wprowadzeniu nowych technologii, których podstawowym celem jest zmniejszenie obciążenia funkcjonariuszy czynnościami administracyjnymi i umożliwienie im zajęcia się tym, co robią najlepiej – ochroną lokalnych społeczności.

Opracowano na podstawie materiałów firmy Microsoft

Największa w Europie sieć komunikacji IP

Z początkiem maja 2004 roku granice Polski stały się wschodnimi granicami rozszerzonej Unii Europejskiej. Najistotniejszym elementem zapewniającym szczelność i bezpieczeństwo granic jest szybka i niezawodna komunikacja. W celu zapewnienia sprawnej komunikacji pomiędzy 268 przejściami granicznymi na terenie Polski NextiraOne zainstalowała największą w Europie sieć łączności opartą na IP. Wdrożony system gwarantuje bezpieczny, centralnie zarządzany dostęp do lokalnych baz danych i informacji rządowych.

Klient

Straż Graniczna jest organem rządowym, do którego zadań należy kontrola ruchu, handlu oraz ochrona ponad 3,5 tysiąca kilometrów granicy polskiego państwa. Straż Graniczna działa za pośrednictwem centrali w Warszawie (Komenda Główna), 15 oddziałów regionalnych oraz 268 granicznych punktów kontroli i strażnic, rozmieszczonych bezpośrednio na granicy Polski.

Wyzwanie

Granica Polski to obecnie wschodnia granica Unii Europejskiej. Z tego względu zapewnienie efektywnego i bezpiecznego systemu komunikacji dla jednostek polskiej Straży Granicznej było jednym z zasadniczych wymogów stawianych przed naszym krajem jako nowym członkiem Wspólnoty Europejskiej.

Dotychczasowa sieć łączności Straży Granicznej była podzielona i opierała się na przestarzałej technologii analogowej, sporadycznie uzupełnianej o narzędzia cyfrowe. Działanie takiego systemu łączności, który nie był wiarygodny w użyciu, niepewny i trudno skalowalny, wiązało się z wysokimi kosztami jego utrzymania.

Wstępna specyfikacja przygotowana dla nowego rozwiązania zakładała wybór jednego centralnie zarządzanego systemu, łączącego wszystkie rozproszone punkty graniczne z oddziałami regionalnymi i oferującego jednakowy poziom bezpiecznego dostępu do scentralizowanych usług, w tym do rządowych baz danych i do internetu. Wybrano rozwiązanie oparte na IP ze względu na jego kompleksowość – mimo geograficznej rozpiętości – oraz z uwagi na fakt, iż stanowić będzie elastyczną platformę dla implementacji dodatkowych aplikacji.

Straż Graniczna powierzyła wdrożenie systemu firmie NextiraOne Polska. O wyborze NextiraOne zadecydowało doświadczenie firmy w integracji systemów transmisji danych i głosu, dobrze rozwinięta sieć serwisowa na terenie całej Polski, a także wiedza zdobyta przy realizacji projektów dla sektora publicznego. Ponieważ rozwiązanie dla Straży Granicznej działać miało w modelu outsourcingu zaoferowanym przez Telekomunikację Polską SA, dodatkowym atutem NextiraOne w trakcie procesu wyboru firmy wdrożeniowej była jej ponad 10-letnia dobra współpraca z TP SA.

Rozwiązanie

Dzięki wdrożeniu systemu opartego na telefonii IP polska Straż Graniczna dysponuje obecnie jednym z najnowocześniejszych systemów łączności w Europie. Rozwiązanie gwarantuje bezpieczną łączność z krajowymi systemami, takimi jak KSI (Krajowy System Informacyjny), CEPiK (Centralna Ewidencja Pojazdów i Kierowców) czy system Urzędu Repatriacji i Cudzoziemców. Zapewnia też sprawne połączenie z Systemem Informacyjnym Schengen.

Wdrożenie rozwiązania rozpoczęło się w styczniu 2003 roku i poprzedzone było 3-miesięcznym testem konfiguracji systemu przeprowadzonym w laboratorium NextiraOne. Ponieważ było to pierwsze tak duże wdrożenie rozwiązania IP w Europie, wstępna analiza była konieczna w celu sprawdzenia poprawności projektu, a w przyszłości – przyspieszenia wdrożenia rozwiązania.

Inżynierowie NextiraOne zaprojektowali ogólnopolską sieć łączności IP opartą na technologii Cisco przy wykorzystaniu istniejącej sieci transmisyjnej i kabli telefonicznych Telekomunikacji Polskiej Polpak. Pozwoliło to uniknąć kosztownych inwestycji na instalację okablowania strukturalnego w budynkach Straży Granicznej.

Wdrożenie systemu podzielone zostało na trzy fazy, z początkową koncentracją na kluczowych elementach w siedzibie Komendy Głównej i oddziałach rejonowych. Następnie zwrócono uwagę na wyposażenie granicznych punktów kontroli i strażnic, a ostatecznie – na implementację aplikacji i podłączeń do internetu. Poszczególne elementy rozwiązania były oddawane do użytku sukcesywnie w odstępach ok. 4-tygodniowych. Oddanie do użytku poszczególnych elementów poprzedzane było szczegółowymi testami poprawności działania rozwiązania.

Najbardziej złożonym problemem, jaki się pojawił podczas implementacji rozwiązania, było przeniesienie

dotychczasowych użytkowników i aplikacji na nową platformę. Przeniesienia należało dokonać tak, aby praca funkcjonariuszy Straży Granicznej nie była zakłócana, a dostęp do krytycznych aplikacji – nieprzerwany.

Jak działa rozwiązanie?

Sieć telefoniczna składająca się z ponad 6600 telefonów Cisco opiera się na lokalnych wejściach PSTN, natomiast dzwonienie wewnątrz sieci odbywa się na podstawie prywatnego planu numeracyjnego. Dodatkowo, dzięki translacjom przeprowadzanym na routerach, na każdy numer można również zadzwonić bezpośrednio z sieci publicznej. NextiraOne stworzyła także centralną książkę telefoniczną oraz aplikację umożliwiającą przesyłanie krótkich wiadomości tekstowych (SMS) pomiędzy abonentami systemu.

Każdy telefon może być podłączony do sieci komputerowej, co umożliwia bezpieczny dostęp do internetu bez potrzeby inwestowania w dodatkowe okablowanie. Dla zagwarantowania bezpieczeństwa sieć internetowa została oddzielona od sieci transmisji głosu. Funkcjonariusze i pracownicy Straży Granicznej zyskali więc nie tylko bezpieczny dostęp do internetu i usług poczty elektronicznej, ale jednocześnie rozwiązanie IP stało się podstawą do zadań związanych z e-learningiem na potrzeby własne Straży.

NextiraOne utrzymuje sieć łączności Straży Granicznej ze swojej centrali w Warszawie, wyposażonej w aplikacje do monitoringu i zarządzania oraz funkcjonalności do alokacji kosztów. Dzięki takiemu rozwiązaniu regionalni administratorzy mają zdalny dostęp do systemu z dowolnego miejsca w sieci. NextiraOne zakończyła również cykl szkoleń dla pracowników Straży Granicznej w zakresie technologii i administrowania systemem. Przeszkoleni pracownicy będą odpowiedzialni za bieżące zarządzanie systemem i jego przyszły rozwój.

NextiraOne jest światowym dostawcą zintegrowanych rozwiązań i usług telekomunikacyjnych oraz największym, niezależnym od dostawców integratorem rozwiązań telekomunikacyjnych w Europie. Centrale firmy NextiraOne mieszczą się w Paryżu i Houston, zaś oddziały działają w 20 krajach w Europie i Ameryce Północnej. Najważniejszymi partnerami NextiraOne są firmy: Alcatel, Cisco Systems, Genesys i Nortel Networks. Właścicielem firmy NextiraOne jest Platinum Equity, amerykańska firma o zasięgu globalnym, specjalizująca się w przejęciach przedsiębiorstw i strategicznym zarządzaniu nimi.

Piotr Jarmoliński
dyrektor handlowy NextiraOne Polska

Rozwiązania Teletry-Komtrans SA

Poznańska Spółka Akcyjna Teletra-Komtrans istnieje na polskim rynku telekomunikacyjnym od 1991 roku. Dysponując odpowiednią kadrą techniczną spółka mogła od początku działalności zagwarantować świadczenie profesjonalnych usług w zakresie telekomunikacji oraz możliwości prowadzenia prac badawczych. Firma specjalizuje się w produkcji i sprzedaży urządzeń telekomunikacyjnych oraz usługach instalacyjno-uruchomieniowych.

Głównym celem działalności jest oferowanie wysokiej jakości urządzeń i usług, których poziom technologiczny pozwala zaspokoić aktualne potrzeby klientów. W ciągu ostatnich lat wprowadzono na rynek kilkanaście nowych wyrobów, w tym kilka wyprodukowanych na podstawie własnych opracowań. W efekcie Teletra-Komtrans stała się jedną z największych firm telekomunikacyjnych powstałych w okresie przemian gospodarczych. Firma uzyskała certyfikat jakości ISO 9001/2000.

Systemy dostępowe xDSL

Urządzenie LR HDSL umożliwia transmisję strumienia do 2 Mbit/s po kablach miedzianych. W skład rodziny wchodzą: A1512 PL LC – uniwersalna karta liniowa pracująca jako HDSL 1- lub 2-parowy; obudowa desktop z interfejsem cyfrowym. Urządzenia udostępniają szereg interfejsów użytkownika: G.703, G.704, ISDN PRA, V.11, X.21, V.35/V.36, Ethernet 10Base-T z funkcją bridge'a lub routera.

Urządzenie LR SDSL/SHDSL to system transmisyjny w wersji Classic zgodny z normą **ITU-T G.991.2.** Posiada szeroką gamę interfejsów, takich jak: G.703, G.704, ISDN PRA, V.11, X.21, V.35/V.36. Instalując system w obudowie z interfejsem typu Ethernet 10Base-T uzyskamy modem z funkcją bridge'a lub routera.

Karty transmisyjne **LR xDSL** można instalować w panelach **A1512 SRV**. Wszystkie systemy z powyższej rodziny są objęte rozbudowanym systemem nadzoru **ASMOS**.

Systemy **LR xDSL** są stosowane w sieci Telekomunikacji Polskiej SA, w tym przez POLPAK, a także przez Netię oraz innych operatorów.

Rodzina urządzeń FlexDSL SHDSL przeznaczona jest do realizacji bardzo długich traktów SHDSL. System obsługuje i nadzoruje do 10 regeneratorów z pełną retransmisją. Dostępne są dwa typy regeneratorów: podstawowy, tylko z funkcją retransmisji (1-parowy lub 2-parowy), rozbudowany, z funkcją Add-Drop (1-parowy), dostępny interfejs G.704, opcjonalnie: nx64, RS232/485.

W zależności od konfiguracji programowej modemy FlexDSL SHDSL pracują jako systemy: 1-parowe, 2-parowe lub w trybie Multi-Point. Urządzenia obsługują interfejsy G.703, G.704, X.21, V.35, V.36. Poza tym dostępna jest także multipleksacja interfejsów E1 oraz nx64 – opcja Multi-Service.

Systemy **FlexDSL SHDSL** są stosowane przede wszystkim w sieci Telekomunikacji Kolejowej PKP.

Systemy światłowodowe OLE

W zakresie światłowodowych systemów teletransmisyjnych trzon oferty stanowią: multipleksery (**FE 80/160/320**) 2 Mbit/s strumieni E1 (G.703/G.704) o krotnościach odpowiednio 4, 8, 16 strumieni; multipleksery (**FlexGain FOM**) różnych interfejsów cyfrowych (G.703/G.704, V.35, 10Base-T) oraz zarządzalne i niezarządzalne optyczne konwertery mediów dla różnych standardów interfejsu Ethernet (10/100/1000 Mbit/s) wykorzystujące włókna jedno- i wielomodowe.

Dostęp szerokopasmowy

Tu ofertę firmy stanowi system IP DSLAM ADSL oraz modemy/routery ADSL. **Turbolink IP DSLAM ADSL** – 24- lub 48-portowy IP DSLAM jest koncentratorem łączy ADSL bazującym na platformie IP. Obsługuje najnowsze standardy ADSL/ADSL2/ADSL2+. Zaprojektowany jest dla dostawców usług w celu oferowania wielu użytkownikom doskonałej jakości usług szerokopasmowych z funkcjami takimi, jak zarządzanie pasmem, priorytetyzacja ruchu, kontrola bezpieczeństwa danych itp. Obsługa VLAN, IGMP snooping, QoS w połączeniu z szerokim pasmem zapewnia wsparcie dla aplikacji typu Video over IP. Urządzenie posiada wbudowane splittery, wymienne moduły uplink zarówno 100Base-T, jak i 1000Base-T, szeroki wachlarz nadzoru – SNMP, Telnet, RS-232 oraz bazującą na SNMP, dedykowaną aplikacją EMS pracującą pod kontrolą systemów Windows

NT/2000/XP. System ten współpracuje z szeroką gamą dostępnych na rynku modemów ADSL/ADSL2/ADSL2+ różnych producentów. Dostępny jest zarówno w wersji dla POTS (Annex A), jak i dla ISDN (Annex B) i w dwóch wersjach zasilania: ~230 V oraz – 48 V.

Systemy dostępowe PCM

Systemy abonenckie PCM 4, 11, 16 oraz 3A/2I mają zastosowanie jako rozwiązanie szybkiego i taniego sposobu zwielokrotnienia łączy abonenckich. Urządzenie 3A/2I udostępnia 3 kanały analogowe oraz 2 ISDN z dostępem BRA. Do urządzeń PCM proponowana jest szeroka gama osprzętu oraz komputerowy system nadzoru umożliwiający pomiary linii, konfigurowanie i testowanie sieci urządzeń. Nowością są systemy PCM pracujące w standardzie SHDSL. Gama urządzeń obejmuje krotności 4 i 12 analogowych linii abonenckich. Jako uzupełnienie systemu 3A/2I oferowane są urządzenia ISDN S0 Extender, które stanowią przedłużenie interfejsu BRA.

Sieci pakietowe z kompresją

NetPerformer to rodzina urządzeń do transmisji danych i mowy z kompresją w sieciach pakietowych. Urządzenia NetPerformer umożliwiają tworzenie prywatnych sieci konwergentnych dla wielooddziałowych przedsiębiorstw, banków i innych instytucji. Urządzenia integrują transmisję skompresowanej telefonii (mowa/faks/modem) oraz komutację wewnątrz sieci rozległej (funkcja rozproszonej centrali tranzytowej) z zaawansowanymi funkcjami routingu IP/IPX, bridgingu, multipleksowaniem synchronicznych i asynchronicznych kanałów cyfrowych. Urządzenia NetPerformer mogą pracować jako węzły sieciowe (komutatory *Frame Relay*, routery IP/IPX) oraz jako urządzenia dostępowe (FRAD, gateway VoIP, multipleksery kanałów cyfrowych i portów telefonicznych). Łącza WAN między urządze-

niami mogą być realizowane poprzez dedykowane kanały cyfrowe, łącza komutowane i sieci pakietowe IP/*Frame Relay*/ATM. Zastosowanie unikatowej metody priorytetyzacji, filtrowania i regulacji przepływu danych pozwala maksymalnie wykorzystać dzierżawioną przepływność dla łączy WAN.

Rozwiązania dla sieci dostępowych

Multipleksery dostępowe *NETmaster* stanowią rodzinę urządzeń, które poprzez zarządzanie strumieniami 2 Mbit/s na poziomie szczelin 64 kbit/s umożliwiają efektywne wykorzystanie dostępnych traktów E1. Multipleksery te pozwalają na dostarczanie klientom w ramach jednej linii dostępowej szeregu usług – zarówno transmisji danych, obrazu, jak i głosu (również w technologii VoIP). Stanowią one propozycję skierowaną do szerokiego grona odbiorców – urządzenia *NETmaster* mogą znaleźć zastosowanie w sieciach operatorów telekomunikacyjnych, u dostawców internetowych (ISP/ASP), integratorów sieci LAN/WAN, a także w dużych i średnich

firmach. Z jednej strony umożliwiają ograniczanie potrzebnych zasobów sieciowych do realizacji usług operatorskich, a z drugiej – gwarantują zwiększenie pojemności sieci dostępowej na odcinku *last-mile*.

Osprzęt światłowodowy

Od 2000 roku firma jest producentem **patchcordów i pigtaili światłowodowych** wykonywanych na bazie złączy AMP i Reichle & De-Massari. Teletra posiada pełen asortyment kabli połączeniowych ze złączami, takimi jak: E2000, MTRJ, FC, SC, ST, LC, LX5, MU. Oferowane kable połączeniowe są szeroko stosowane na rynku usług telekomunikacyjnych, CATV, w sieciach LAN i WAN.

Wzbogacając ofertę firma dodała również pozostałe główne elementy torów światłowodowych, takie jak **przełącznice i mufy światłowodowe** oraz – na życzenie klienta – splitery, tłumiki, systemy WDM i DWDM.

System telemonitoringu kardiologicznego

System TELE-EKG umożliwia przekazywanie elektrokardiogramów za pośrednictwem łączy telekomunikacyjnych. Składa się on z aparatów Event-Holter – osobistych aparatów noszonych przez pacjenta oraz z systemu komputerowego z oprogramowaniem Cardio-Scp służącym do archiwizacji i analizy badań przez lekarza. Rodzinę Event-Holterów stanowią 2 rodzaje aparatów:

- ✔ **EHO6** – trójelektrodowy, dwu- lub sześcioodprowadzeniowy, umożliwia rejestrację i transmisję badań oraz przesyłanie sygnału EKG „na żywo" akustycznie przez telefon, cyfrowo przez telefon komórkowy oraz cyfrowo bezpośrednio przewodem do komputera;
- ✔ **EHO8** – podobnie jak EHO6, lecz sześcioelektrodowy, ośmioodprowadzeniowy;
- ✔ **EHO3** – czteroelektrodowy, trójkanałowy przenośny aparat do rehabilitacji kardiologicznej w warunkach domowych; programowalny cykl rehabilitacji pacjenta, możliwy wybór zapisu 3 z 6 odprowadzeń przedsercowych.

Ponadto system uzupełnia aparat **PP-05 v12** – pełny, 12-kanałowy przenośny aparat EKG z dotykowym wyświetlaczem ciekłokrystalicznym współpracujący z programem CardioScp. ■

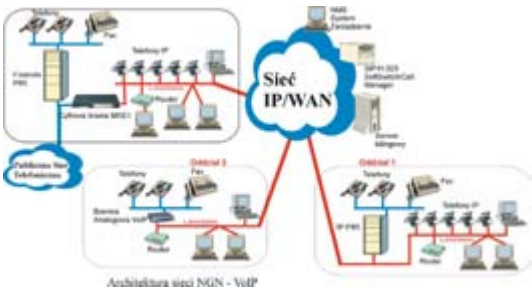
Nowoczesne sieci nowej generacji oparte na technologii IP

Od początku swojego istnienia firma Computex Telecommunication była liderem we wprowadzaniu na polski rynek najnowszych technologii w dziedzinie telekomunikacji. Jedną z nich była budowa sieci wielousługowych przeznaczonych do transmisji danych, transmisji głosu i danych multimedialnych.

Bazując na swoim doświadczeniu, mając za sobą lata praktyki oraz posiadając bogatą wiedzę w dziedzinie sieci wielousługowych (NGN – *Next Generation Network*) firma Computex Telecommunication stała się dostawcą sprzętu i technologii dla przedsiębiorstw oraz instytucji rządowych.

W skład architektury sieci NGN wchodzą przełączniki sieciowe, routery oraz szeroki wachlarz urządzeń korzystających z zaawansowanych możliwości sieci, od pojedynczych telefonów IP i bramek analogowych do dużych korporacyjnych bram VoIP z portami E1 i hybrydowych bram IP-PBX z modułami E1, FXS i FXO.

Architektura sieci NGN firmy Computex



Architektura sieci NGN - VoIP

Instalacje oparte są na sprzęcie firm AudioCodes i ArelNet zapewniającym pełną integrację z istniejącą siecią telekomunikacyjną i informatyczną. Abonenckie urzą-dzenia dostępowe wyposażone są w 2, 4, 8 lub 24 porty analogowe FXS/FXO oraz, w przypadku dużych bram korporacyjnych, w 1 do 16 portów E1. Urządzenia pracują w standardzie H.323, SIP i MGCP. Podłączenie do publicznej sieci IP realizowane jest poprzez port Ethernet 10/100Base-T. Computex dla potrzeb swoich klientów dostarcza również telefony IP integrujące klasyczną telefonię analogową z technologią IP. Umożliwia to odbieranie i wykonywanie połączeń z jednego zaawansowanego aparatu wykorzystując tradycyjną linię telefoniczną lub sieć IP.

Bezpieczeństwo i jakość

Ze względu na wykorzystanie sieci IP jako medium transmisyjnego dla rządowych systemów komunikacyjnych konieczne jest zastosowanie dodatkowych mechanizmów bezpieczeństwa i technik testowania zabezpieczeń systemów teleinformatycznych. Mechanizmy zabezpieczające używane w sieciach transmisji danych to:

- ✔ blokowanie niewykorzystanych portów przez urządzenia i aplikacje w sieci,
- ✔ access listy (dostęp dla konkretnych adresów IP),
- ✔ stosowanie połączeń SSH,
- ✔ ograniczenie listy adresów MAC,
- ✔ tworzenie wirtualnych sieci prywatnych,
- ✔ zastosowanie nowoczesnych metod szyfrowania,
- ✔ skanowanie portów w celu wykrycia „nieszczelności w sieci",
- ✔ generowanie „ataków hackerskich" w celu ustalenia poziomu bezpieczeństwa w sieci.

Główne zalety zastosowania technologii sieci nowej generacji:

- ✔ możliwość stopniowego przekształcenia kilku sieci działających w różnych technologiach w jedną zintegrowaną sieć wielousługową,
- ✔ scentralizowany system billingowy,
- ✔ integracja głosu i danych,
- ✔ większa możliwość doboru odpowiedniego operatora telefonicznego,
- ✔ centralizacja systemu oznaczająca niższe koszty utrzymania,
- ✔ szeroki wybór usług w ramach jednej sieci (telefonia, wideokonferencja, wideo na żądanie, pre-paid, poczta głosowa, www, poczta elektroniczna, e-learning, itd.),
- ✔ szybka i łatwa integracja z istniejącą infrastrukturą w sieci korporacyjnej,
- ✔ szybkie uruchamianie nowych lokalizacji (oddziały),
- ✔ mobilność: łatwa mobilność użytkowników i całych działów, numery wewnętrzne w lokalizacjach poza siedzibą,
- ✔ lepsze wsparcie dla użytkowników zwiększające wydajność,
- ✔ ograniczenie kosztów związanych z realizacją połączeń telefonicznych poprzez wykorzystanie technologii VoIP przy zachowaniu dobrej jakości połączeń (zerowe koszty połączeń pomiędzy oddziałami),
- ✔ łatwe rozszerzenie systemu o nowe usługi (przyszłe potrzeby),
- ✔ dotarcie do nowych lub odległych obszarów geograficznych i wykorzystanie sieci IP jako medium do oferowania innowacyjnych rozwiązań telekomunikacyjnych.

Firma Computex Telecommunication jest wyłącznym przedstawicielem firmy ArelNet i dystrybutorem Audiocodes w Polsce.

Dostępne rozwiązania dla przedsiębiorstw opisano na stronie firmowej pod adresem: www.computex.com.pl/voip

Nowe radiostacje, nowe możliwości

Współczesne systemy łączności wojskowej wymagają coraz większych szybkości przekazu informacji oraz zobrazowania sytuacji prowadzonych działań. Coraz większe znaczenie ma szybkie i pewne przekazywanie danych, wymiana komunikatów oraz przekazywanie drogą radiową obrazów. Istotne jest też przekazywanie pozycji obiektów ruchomych i obrazowanie jej na mapie cyfrowej, przekazywanie danych do systemów śledzenia obiektów i systemów kierowania ogniem.

Rośnie znaczenie łączności z siecią internetową, w związku z tym rosną też wymagania stawiane środkom łączności, które muszą realizować te zadania. Jednym z ważniejszych parametrów współczesnych urządzeń łączności taktycznej jest szybka transmisja danych.

Wychodząc naprzeciw tym oczekiwaniom RADMOR wprowadza do swojej oferty nowe urządzenia oraz modernizuje już produkowane. Od 2006 roku firma rozpocznie produkcję dwóch licencyjnych radiostacji F@stnet – systemu PR4G nowej generacji. Polska będzie drugim krajem, do którego Thales przekaże produkcję tych urządzeń. Koszty związane z transferem produkcji udało się częściowo pokryć zobowiązaniami offsetowymi firmy Thales Netherlands powstałymi z realizacji innego projektu. Dzięki temu armia otrzyma nowe radiostacje wytwarzane w kraju bez ponoszenia wysokich kosztów transferu technologii. Odpowiednie umowy zostały zawarte i RADMOR rozpoczął już wdrażanie technologii produkcji radiostacji F@stnet. Będą to radiostacje plecakowe RRC 9210 i pokładowe RRC 9310 w pełni kompatybilne z używanymi od 1997 roku przez polskich żołnierzy radiostacjami RRC 9200 i RRC 9500. Dzięki zastosowaniu nowych rozwiązań technologicznych radiostacje F@stnet będą posiadały nowe funkcje, a radiostacja plecakowa będzie prawie o połowę lżejsza i mniejsza od swojej poprzedniczki.

Istotną cechą nowych urządzeń jest czterokrotnie szybsza niż w dotychczas produkowanych modelach transmisja danych. Transmisja synchroniczna może odbywać się z prędkościami od 50 do 19200 bit/s z korekcją błędów i do 42660 bit/s bez korekcji. Do szybkiej transmisji danych (powyżej 4800 bit/s) zastosowano nową modulację wielowartościową. Wszystkie radiostacje wyposażone będą w wokoder, umożliwiający prowadzenie korespondencji w środowisku bardzo zakłóconym, pracujący z prędkościami 800, 2400 bit/s (zgodnie z normą STANAG) oraz 4800 bit/s. Nowy rodzaj pracy – multipleks – zapewnia równoczesną transmisję mowy i danych z prędkościami 1200 lub 600 bit/s. Radiostacje F@stnet umożliwiają również transfer plików oraz przesyłanie e-maili przy pomocy standardowego oprogra-

Żołnierz polskiego kontyngentu w Iraku z radmorowską radiostacją doręczną 3501

mowania, np. Microsoft Outlook. Na życzenie klienta radiostacja może zostać wyposażona we wbudowany odbiornik GPS. Możliwe jest wtedy przekazywanie i odczytywanie pozycji wszystkich radiostacji pracujących w sieci. Pozycje te mogą być wprowadzane na mapę cyfrową wraz z numerami radiostacji. RADMOR proponuje wyposażenie radiostacji pokładowych RRC 9310 w antenę zintegrowaną z anteną GPS. Dzięki temu nie ma potrzeby instalowania dodatkowej anteny systemu nawigacji satelitarnej GPS.

Nowe możliwości transmisji danych zostały również wprowadzone w radiostacji doręcznej 3501 – własnej konstrukcji RADMORU. Radiostacja w nowych wykonaniach posiada wbudowany podwójny modem: do wolnej i szybkiej transmisji danych. Pierwsza z nich służy do przesyłania danych o wielkości do 200 bajtów, np. statusów czy pozycji GPS. Do przesyłania większych plików (ponad 1000 bajtów) – takich jak obrazy, teksty czy programy – wykorzystywana jest szybka transmisja danych.

Nowe wersje radiostacji posiadają odbiornik GPS oraz oprogramowanie pozwalające uzyskać wiele funkcji związanych z obsługą informacji o położeniu geograficznym obiektów. Radiostacja może pracować na kanałach dedykowanych przeznaczonych wyłącznie dla mowy lub dla danych albo na kanałach automatycznych, gdzie możliwe jest prowadzenie rozmowy, ale transmisja danych ma priorytet. Kanały automatyczne są szczególnie ważne przy współpracy z urządzeniem GPS, ponieważ można nie tylko przesłać swoją pozycję, ale również prowadzić nasłuch foniczny. Użytkownicy nowych modeli radiostacji 3501 mają możliwość wysyłania i odbierania tzw. statusów, czyli komunikatów cyfrowych. Są one zawsze wybierane ręcznie przez operatora. Odebrany numer statusu może być przekodowany w komputerze na pełną postać alfanumeryczną.

Radiostacja 3501 jest wyposażona w interfejs RS232, poprzez który możliwe jest programowanie parametrów transmisji danych oraz przesyłanie danych z zewnętrznego źródła, np. z komputera PC. Transmisja danych z zewnętrznego źródła może mieć miejsce z pojazdu, w którym zainstalowano radiostację V3501 (samochodową wersję doręczej radiostacji) i komputer. Odbiorcą danych może być inna stacja V3501 lub stacja bazowa z kompatybilnym modemem (np. RRC wyposażona w interfejs 0423).

Tryby pracy nowych wersji radiostacji 3501:

- ✔ transmisja mowy analogowa jawna lub skramblowana,
- ✔ transmisja mowy cyfrowa skramblowana,
- ✔ transmisja mowy cyfrowa szyfrowana z zewnętrznym szyfratorem,
- ✔ selektywne wywołania tonowe,
- ✔ dostęp do sieci telefonicznej,
- ✔ synchroniczna transmisja danych z szybkością 16 kb/s i modulacją GMSK,
- ✔ asynchroniczna transmisja danych 4800–24000 b/s z modulacją 4L-FSK,
- ✔ transmisja danych 1200, 2400 b/s z modulacją FFSK,
- ✔ przesyłanie i odbiór statusów,
- ✔ odbiór pozycji GPS, jej wyświetlenie i wysłanie dalej drogą radiową.

Współczesne pole walki to nie tylko działania wojskowe, ale również, szczególnie ważne we współczesnej dobie, działania antyterrorystyczne. Wymagają one współpracy nie tylko różnych rodzajów wojsk (jednostki lądowe, lotnictwo, marynarka wojenna), ale również służb cywilnych (policja, straż pożarna, zespoły ratowników). Niestety, obecnie każda z nich wykorzystuje własne środki łączności pracujące na różnych częstotliwościach, z różnymi modulacjami i z różnymi systemami transmisji danych. W celu przeprowadzenia wspólnej operacji konieczne jest posiadanie wielu środków łączności radiowej umożliwiających łączność między różnymi służbami. Aby współdziałania służb wojskowych i cywilnych były efektywne, niezbędne jest jedno urządzenie realizujące dowolny rodzaj łączności radiowej.

Wychodząc naprzeciw takim potrzebom RADMOR prowadzi prace rozwojowe nad doręcznymi radiostacjami R3505 opartymi na koncepcji programowej architektury komunikacyjnej SCA (*Software Communication Architecture*). Są to urządzenia określane jako radiostacje programowalne (*Software Defined Radio*). Ich podstawowa idea polega na możliwości szybkiego przystosowania ich do pracy w różnych systemach radiowych wyłącznie poprzez zmianę oprogramowania urządzenia, czyli bez potrzeby wprowadzania modyfikacji w jego konstrukcji i technologii produkcji. Radiostacje takie integrują istniejące standardy radiokomunikacyjne umożliwiając transmisję mowy, danych, obrazów video, pozycji (GPS) oraz retransmisję sygnału pomiędzy różnymi sieciami wojskowymi i cywilnymi. Radiostacje przeznaczone są do łączności taktycznej bliskiego zasięgu HF/VHF/UKF dla wojsk lądowych oraz do współdziałania z wojskami lotniczymi, morskimi i ze służbami cywilnymi. Przy zdarzeniach o charakterze kryzysowym korzystać z niej mogą również służby ratownictwa lądowego, morskiego i lotniczego, a także służby publiczne koordynujące działania podczas likwidacji zagrożeń. Możliwy też jest odbiór informacji z systemu GPS o pozycji geograficznej.

Urządzenia te przeznaczone są do pracy w zakresie częstotliwości 20520 MHz. Przy jego pomocy można nawiązać łączność foniczną analogową (jawną i maskowaną) i cyfrową (jawną i szyfrowaną) oraz przeprowadzić transmisję danych. Radiostacja współpracuje z zewnętrznymi urządzeniami analogowymi i cyfrowymi, takimi jak modemy czy komputery PC.

Wszystkie opisane wyżej radiostacje pozwalają na tworzenie nowych sieci łączności radiowej. Nowoczesne funkcje realizowane przez urządzenia, a szczególnie znacznie większe prędkości transmisji danych, umożliwiają sprawne zarządzanie i dowodzenie na współczesnym polu walki. W przyszłości pozwolą na zintegrowanie działań wojska i cywilnych służb ratowniczych oraz porządkowych. ■

Komputery do zadań specjalnych

Wybór komputera o wzmocnionej konstrukcji nie należy do najłatwiejszych. Urządzenie takie musi być niezawodne i spełniać szereg wymogów. Powinno być odporne na zmienne warunki środowiskowe (opady, temperatura), być przystosowane do pracy w zapyleniu i mieć tak mocną konstrukcję, by upadek na beton nie spowodował trwałego uszkodzenia elementów wewnętrznych czy utraty danych.

Jednym z produktów spełniających wszystkie powyższe wymagania, a nawet normy sił zbrojnych wojsk amerykańskich, są komputery marki Itronix – urządzenia o wzmocnionej konstrukcji projektowane z myślą o pracy w trudnych warunkach.

Komputery przenośne Itronix spełniają najbardziej surowe normy pod względem odporności na warunki środowiskowe – należą do grupy urządzeń o najwyższym stopniu wytrzymałości (*fully-rugged*), posiadają klasę IP54 (wyjątkiem jest handhed Itronix Q-200, który posiada klasę IP67) oraz spełniają surowe normy wojskowe MIL STD 810F.

Pod względem wytrzymałości urządzenia mobilne dzieli się na 4 kategorie:

- ✔ *commercial* – to wspólne określenie komputerów do zastosowań ogólnych o ograniczonej wytrzymałości;
- ✔ *semi-rugged* – są to komputery o wzmocnionej obudowie zabezpieczającej ekran przed uszkodzeniami, jednak bez ochrony elementów wewnętrznych;
- ✔ *rugged* – komputery zaprojektowane z myślą o pracy w trudnych warunkach środowiskowych, których konstrukcja chroni elementy wewnętrzne przed uszkodzeniami. Komputery takie są zbudowane ze stopów magnezu, chroniących poszczególne elementy przed wstrząsami, pyłem, wodą czy ekstremalnymi temperaturami. Wytrzymują wielokrotne upadki na twardą powierzchnię;
- ✔ *fully rugged* – najbardziej wytrzymała klasa komputerów przeznaczonych do pracy w ekstremalnych warunkach. Obudowa oraz elementy wewnętrzne zapewniają maksymalną ochronę urządzenia. Najczęściej komputery te są projektowane pod kątem ściśle określonych zastosowań.

Pozostaje nam jeszcze wyjaśnienie znaczenia pozostałych symboli. Ponieważ zdarza się, że w ramach danej kategorii występują znaczne różnice jeśli chodzi o odporność sprzętu różnych producentów, posługują się oni dodatkowymi rankingami i testami. Do najczęściej stosowanych należą:

- ✔ IP (*Ingress Protection*) – oznacza stopień odporności urządzenia na infiltrację do jego wnętrza ciał obcych. System klas zabezpieczeń IP został ustalony przez Międzynarodową Komisję Elektrotechniczną (IEC) i pozwala upewnić się, że urządzenie wykorzystywane jest do pracy w warunkach, do jakich zostało zaprojektowane. Oznaczenie składa się z dwóch cyfr, z których pierwsza dotyczy zabezpieczenia przed kurzem, druga – przed wilgocią. Im większa cyfra w oznaczeniu, tym wyższy stopień zabezpieczeń (*klasa IP54 to połączenie dwóch oznaczeń; poziom 5 oznacza zabezpieczenie przed kurzem, a także przed dostępem do wnętrza za pomocą drutu lub infiltracją innych obiektów o wymiarach poniżej 1 mm; jedyna istniejąca wyższa kategoria to pyłoszczelność; klasa 4 oznacza zabezpieczenie przed ochlapywaniem wodą z dowolnego kierunku – ochrona przeciwbryzgowa; wyższe klasy – od 5 do 8 wskazują na poziom ochrony strugoszczelnej i zanurzenia*);
- ✔ MIL STD (*Military Standard*) oraz MIL SPEC (*Military Specification*) – to zestaw wytycznych opracowanych przez amerykańskie siły zbrojne dotyczących zastosowań militarnych.

Najważniejsze wdrożenia Itronix

Rozwiązania Itronix z powodzeniem pracują w wielu projektach specjalnych w wojsku, policji czy straży granicznej. Firmy oraz służby mundurowe wybierają ten sprzęt ze względu na jego wysoką niezawodność w warunkach polowych. W sytuacji gdy liczy się każda sekunda, a decyzje podejmowane są w dużym stresie, trzeba mieć pewność, że każde ogniwo w łańcuchu komunikacji funkcjonuje niezawodnie. Komputery Itronix okazały się takim właśnie mocnym ogniwem ze względu na bardzo dużą odporność na warunki środowiskowe (wstrząsy, upadki, wysokie zapylenie) i atmosferyczne (wysokie i niskie temperatury, wilgoć). Dzięki tym właściwościom do minimum zmniejszono ryzyko uszkodzenia w niekorzystnym otoczeniu. Dodatkowo, wybierając te urządzenia, służby dbające o nasze bezpieczeństwo zyskują możliwość równoczesnego wykorzystywania trzech kanałów komunikacji radiowej (GSM/GPRS/EDGE, WLAN i Bluetooth).

Notebook o wzmocnionej konstrukcji

Wiosną 2003 roku III Dywizja Piechoty U.S. Army, biorąca udział w działaniach bojowych w Iraku, dysponowała liczbą 2500 laptopów. Ze względu na trudne warunki środowiskowe, w których toczyła się misja, ok. 30 proc. sprzętu dwunastu różnych producentów uległo zniszczeniu. Wszechobecny piasek i zmiany temperatury okazały się zabójcze dla laptopów projektowanych do pracy typowo biurowej. W konsekwencji tych strat U.S. Army zdecydowała się przeprowadzić testy dostępnych na rynku urządzeń w celu wyboru komputera, który okaże się niezawodny w każdych warunkach.

W trakcie testów wszystkie urządzenia zostały poddane między innymi próbom zgodności ze standardem MIL STD 810F, takim jak:

- ✔ 10-minutowy test w strumieniu wody o ciśnieniu odpowiadającym ciśnieniu pompy strażackiej;
- ✔ test 26 upadków z wysokości 3 stóp na podłogę betonową;
- ✔ test w strumieniu cząstek odpowiadających rozmiarem ziarenkom piasku.

Wszystkie powyższe próby odpornościowe zwycięsko przeszedł Itronix GoBook II. Okazał się produktem, którego armia amerykańska szukała. Dodatkowo U.S. Army doceniła w urządzeniu wysokie parametry informatyczne, trzy standardy komunikacji radiowej oraz korzystne warunki umowy gwarancyjnej.

– *Komputery o wzmocnionej konstrukcji firmy Itronix cieszą się doskonałą opinią w naszych siłach zbrojnych, zarówno wśród żołnierzy jak i w Pentagonie. Wcześniejsze doświadczenia z Afganistanu i z Iraku pokazały konieczność zapewnienia nieprzerwanej pracy w trudnych warunkach polowych, a Itronix ma dużą szansę zająć dominującą pozycję na tym rynku* – powiedział kongresman **George Nethercutt**, vice chairman of Defense Appropriations Subcommittee.

Równie interesującego wdrożenia dokonano w bazie lotniczej Randolph, głównej bazie szkoleniowej sił powietrznych USA, w której prowadzone są szkolenia między innymi polskich pilotów F-16. Komputery o wzmocnionej konstrukcji wyposażono w oprogramowanie, które wykorzystując standardy komunikacji bezprzewodowej, w zabezpieczonych sieciach wojskowych, umożliwia łatwy dostęp myśliwców do dokumentacji technicznej niezbędnej podczas serwisu i obsługi naziemnej. Na terenie strefy serwisowej lotniska zbudowano bezpieczną sieć WLAN, w której komputery Itronix zostały wykorzystane jako terminale serwisowe. Podstawowym wymogiem dla takiego terminalu była jego odporność na skrajne warunki atmosferyczne i środowiskowe występujące na lotniskach, a także możliwość połączenia z siecią bezprzewodową. Dzięki temu możliwe stało się ściągnięcie instrukcji serwisowych, schematów czy kart serwisowych praktycznie w dowolnym miejscu takiej strefy. W konsekwencji technicy uzyskali łatwy i bezpieczny dostęp do potrzebnych im informacji eliminując konieczność wertowania opasłych papierowych tomów, co pozwoliło znacznie zwiększyć wydajność ich pracy. Zastosowanie w tym wdrożeniu komputerów Itronix było istotne również ze względu na fakt, iż komputery te posiadają certyfikat dopuszczający do pracy w strefie zagrożenia wybuchem.

– *Ta technologia pozwala skrócić czas procedury serwisowej o połowę, obniżając tym samym jej koszt. Patrząc indywidualnie może nie jest to dużo, ale sumując czas 139 techników otrzymujemy znaczną oszczędność* – powiedział **Rick Peyton**, technik elektroniki lotniczej.

Laptopy Itronix znalazły zastosowanie także w pracy Federalnej Policji Drogowej w Seattle. Aby zapewnić skuteczność działań patroli przy gwałtownym rozwoju miasta, koniecznością stało się zapewnienie komunikacji pomiędzy jednostkami policyjnymi. Istotnym elementem branym pod uwagę przy wyborze sprzętu był fakt, iż komputery użytkowane podczas służby w wozach patrolowych miały być odporne na wstrząsy, na które narażony jest samochód. W tym projekcie ponownie najlepszy okazał się Itronix GoBook II. – *W chwili obecnej oficerowie są w stałym kontakcie z bazą danych. W trakcie kontroli drogowej lub identyfikacji podejrzanego mogą szybko otrzymać szczegółowe informacje z centrali. Do tej pory musieli wracać do bazy lub kontaktować się z operatorem przez radio. Jednocześnie prostsze i bardziej skuteczne stało się tworzenie raportów bezpośrednio na miejscu zdarzenia* – powiedział **Mehdi Sadri**, information system manager for FWPD.

Tablet o wzmocnionej konstrukcji

W 2004 roku w regatach Cowes Week i Rolex Swan Cup załoga jachtu Spirit of Jethou, po tym jak fala sztormowa zalała kokpit, wykorzystała Itronix GoBook Tablet PC do zadań nawigacyjnych i komunikacyjnych. Woda wypełniła pomieszczenie załogi niszcząc dotychczasowy system nawigacji. Od tego momentu aż do zakończenia regat Tablet stał się podstawowym komputerem pokładowym umożliwiającym ponowne uruchomienie systemu nawigacji i przywrócenie łączności.

Handheld o wzmocnionej konstrukcji

W 2004 roku po rozszerzeniu Unii Europejskiej Polska i Litwa – aby spełnić wymogi prawa unijnego – musiały zaostrzyć procedury kontroli na granicy z obwodem kaliningradzkim. Służba graniczna Litwy, przez terytorium której odbywa się tranzyt z i do Rosji, potrzebowała urządzeń zapewniających skuteczną komunikację w czasie kontroli prowadzonej w pociągach. Wzmocniona obudowa, dwa standardy komunikacji radiowej i prosta obsługa spowodowały, że wybrano terminal Itronix GoBook Q-100.

Jednostki policji pełniące służbę na motocyklach często spotykają się z trudnościami związanymi z dostępem do policyjnej bazy danych. Warunki, w których pełnią służbę oraz wymóg stałej komunikacji zmusiły irlandzką policję do zakupu przenośnych komputerów. W związku z tym koniecznością stał się wybór urządzenia o podwyższonej odporności na warunki pogodowe i wibracje, zapewniającego komunikację radiową (GPRS/WLAN). Wybór padł na przenośny terminal Itronix Q-100 z systemem PocketPC 2002 i z aplikacją Traffic Police.

Jednym z najnowszych projektów, w którym zastosowanie znalazły rozwiązania Itronix, jest hiszpański program Amper polegający na stworzeniu systemu do śledzenia ruchów wojsk przez żołnierzy piechoty lub przez obsługę pojazdów pozbawionych systemów dowodzenia. Testowa wersja systemu pod nazwą Elcano wykorzystuje odbiornik GPS i wzmocniony laptop Itronix połączone z dedykowanym systemem informacji geograficznej. W projekcie tym rozważane jest zastosowanie każdego z produktów Itronix.

Pokaz „mobilności extremalnej”

Ponieważ znaczna część wdrożeń Itronix związana jest z montażem sprzętu w samochodach, technicy producenta postanowili sprawdzić, jak zachowa się on podczas wypadku samochodowego. W tym celu komputer Itronix poddano testowi uderzenia eksplodującą poduszką powietrzną. Film z tego eksperymentu pokazuje, jak duże siły oddziałują na komputer w momencie uderzenia. Elastyczna matryca ulega odkształceniu i z dużą siłą zostaje zamknięta, jednak komputer nie ulega uszkodzeniu. Film z testu można znaleźć pod adresem: http://www.mobilnosc-extremalna.pl/itronix_film.wmv.

Dodatkowe informacje na temat opisywanych produktów można uzyskać w firmie Passus.

Radosław Dudzic
Product Manager, Passus Sp. z o.o.

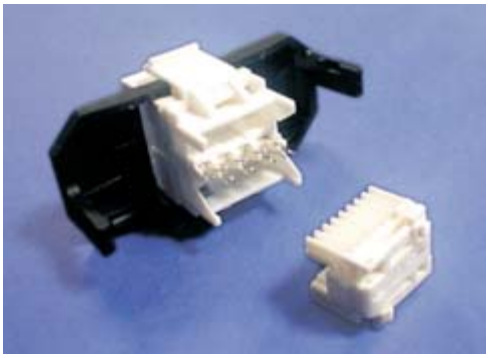
Światłowodowy i miedziany system okablowania strukturalnego firmy 3M

Firma 3M znana jest ze swojej innowacyjności i rozwiązań, które wyznaczają światowe standardy. Dysponuje kilkudziesięcioletnim doświadczeniem i unikatową wiedzą z technologii materiałów, optyki, elektroniki i informatyki, co pozwala sprostać stale rosnącym wymaganiom w teleinformatyce i utrzymać wiodącą pozycję wśród firm światowego przemysłu telekomunikacyjnego.

3M jest dostawcą komponentów sieciowych dla największych firm telekomunikacyjnych. To właśnie z laboratoriów 3M pochodzi większość stosowanych obecnie rozwiązań do łączenia kabli telekomunikacyjnych – miedzianych i światłowodowych.

Rozwiązania sieciowe Volition™ obejmują unikatowy system światłowodowego okablowania strukturalnego, zapewniający swobodę wyboru w projektowaniu i optymalizacji całokształtu architektury sieci, jak również nowoczesny system miedzianego okablowania strukturalnego kategorii 6, zapewniający pewną transmisję danych w oparciu o istniejące standardy, a ponadto pozwalający na zastosowanie w sieciach o wysokiej przepływności.

Unikatowe małogabarytowe złącze VF-45™ pomaga zredukować złożoność sieci światłowodowej, podczas gdy złącza miedziane RJ45 firmy 3M zapewniają wyjątkowo proste rozwiązania zakończeniowe, gdyż ich montaż odbywa się poprzez zacisk bez wykorzystania narzędzi. Zaciśnięcie wszystkich 8 styków odbywa się za pomocą jednego ruchu gwarantując pewne połączenie w wyjątkowo krótkim czasie. Nowe złącze kat. 6 posiada popularny standard mocowania „Keystone". Jeśli jest taka potrzeba, to można kilkakrotnie dokonywać ponownego zaciśnięcia złącza K6. Oferowane są trzy typy złącza: UTP, FTP i w pełni ekranowane STP. Wysoka niezawodność elementów połączeniowych i parametry nierzadko przewyższają standardy. Jedną z ważniejszych cech oferty rozwiązań firmy 3M jest ich różnorodność, łatwość w montażu oraz wysoka wydajność i pewność systemu.



Okablowanie kat. 6 – K6 (uchwyt Keystone)

Wtyk i gniazdo VF-45™, nowy standard – złącze małogabarytowe

Do instalacji złącza VF-45™ nie są potrzebne żadne kleje, a nowe konstrukcje wtyczki i gniazda umożliwiają połączenie w układzie dupleksowym. Zważywszy, że rozmiar tego układu jest niemal o połowę mniejszy od standardowego interfejsu dupleksowego SC, sama instalacja może być znacznie „zagęszczona". Po wyjęciu wtyczki z gniazda czoło włókien zarówno w gnieździe, jak i we wtyczce jest zabezpieczone przez automatycznie zamykające się osłony. Rowki w kształcie litery V pozwalają na precyzyjne ułożenie włókien, a wszystko to umieszczone jest w zgrabnej, zatrzaskującej się obudowie, która stanowi bezpieczną osłonę całej konstrukcji. Złącze VF-45™ jest wystandaryzowane według normy TIA/EIA – 604-7, FOCIS-7 oraz PN-EN 61754-19. Posiada również homologację Ministra Łączności nr 667/2000, wydaną na podstawie opinii technicznej nr 347/2000 Instytutu Łączności w Warszawie.

W Polsce wykonano już wiele instalacji – w tym również dla wojska, między innymi w Dowództwie Marynarki Wojennej Gdynia oraz Wojskowym Instytucie Medycyny Lotniczej w Warszawie i dla innych ważnych klientów, takich jak: Komenda Główna Straży Granicznej, HP Poland, PKO BP (500 oddziałów), BGŻ Centrala, Żywiec Trade, TP SA, Morski Port Handlowy Szczecin.

Oprócz rozwiązań sieciowych Volition™ firma 3M oferuje kompletną linię jedno- i wielomodowych światłowodowych złączy ferrulowych Hot Melt w wersji ST, SC, FC oraz LC. Wszystkie półzłącza fabrycznie wypełnione są specjalnym klejem termotopliwym i posiadają wysokiej jakości ceramiczne ferrule. Montaż przy użyciu zestawu z piecykiem na kablu światłowodowym trwa kilka minut, jest bezpieczny i tani. Złącza mają zastosowanie

Złącze Hot Melt ST

Zestaw do zarabiania złączy Hot Melt

w okablowaniu LAN budynków, są zgodne z normami krajowymi i międzynarodowymi TIA/EIA – 568, ISO/IEC 11801 i EN 50173.

Uzupełnieniem tej oferty są pigtaile i patchcordy różnych długości zakończone różnymi półzłączami. Ważnym elementem światłowodowych rozwiązań połączeniowych jest mechaniczny spaw Fibrlok™. Złącze dostępne jest zarówno do włókien jedno-, jak i wielomodowych (250 lub 900 µm). To proste połączenie gwarantuje parametry analogiczne do spawów (średnia tłumienność wtrąceniowa 0,07 dB). Zestaw montażowy jest lekki, przenośny i nie wymaga zasilania, dzięki czemu może być wykorzystywany w warunkach polowych.

Złącza mechaniczne Fibrlok™

Najistotniejsze zalety charakteryzujące nasz system, które mają kluczowe znaczenie w sieciach wojskowych, to:

- ✔ odporność na zakłócenia (EMI/EFI),
- ✔ bezpieczeństwo danych (trudny podsłuch),
- ✔ prosta instalacja i obsługa,
- ✔ mechaniczne kodowanie gniazd.

Firma 3M poza terytorium Stanów Zjednoczonych może poszczycić się również instalacjami w Europie dla NATO (Briunssum, Siedziba Regionalna NATO, Holandia, 10 podłączonych budynków), Wojsk Lotniczych w Holandii, jak również Wojsk Lądowych. Instalacje zostały wykonane w siedzibie głównej NATO w Brukseli (Belgia), we Frankfurcie – Ramstein (Niemcy), Siedziba Regionalna NATO we Włoszech.

Budynek głównej siedziby NATO w Brukseli

System Volition™ został zainstalowany w obiektach wojskowych w Hiszpanii, Norwegii, Holandii, Wielkiej Brytanii, Czechach.

3M Poland Sp. z o.o.
Al. Katowicka 117, 05-830 Nadarzyn
tel. (22) 739 60 00, fax (22) 739 60 03

Beata Sałyga
tel. (22) 739 61 00 lub 0-600 27 80 19
e-mail: bsalyga@mmm.com

Zapraszamy do odwiedzenia naszej strony internetowej: http://www.3M.pl http://www.3mtelecommunications.com

Rozwój planowania awaryjnego dla strategicznych obiektów teleinformatycznych

W obecnym czasie, kluczem do przywrócenia normalnego stanu po awarii i zachowania ciągłości operacji biznesowych jest odporność systemów z punktu widzenia biznesu. Ciągłe wykorzystywanie nowych technologii, zmusza do używania takich rozwiązań, dzięki którym będzie można wciąż chronić najnowsze rozwiązania teleinformatyczne i technologiczne. Ramy czasowe, w jakich potrzebna jest dostępność do urządzeń teleinformatycznych to 24/7/365 – oznacza to, że sukces działania Disaster Recovery Centre po awarii mierzony jest już w milisekundach.

Wielu klientów Distaster Recovery Center pochodzi z sektorów, w których nie można sobie pozwolić na najkrótsze nawet przerwy. Są to klienci lub instytucje, które często stosują ośrodki zapasowe, aby zapewnić ciągłość działalności informatycznej. Po wydarzeniach z 11 września władze zajmujące się regulacją usług finansowych skupiły się na zapewnieniu wszystkim większym instytucjom odpowiednich planów awaryjnych. W niektórych dużych krajach, a szczególnie w Stanach Zjednoczonych, na osobach pełniących funkcje dyrektorów generalnych spoczywa odpowiedzialność za ochronę danych w ich firmach. Spółki, które utracą dane, niezależnie od przyczyny, przechodzą w stan likwidacji w ciągu 14 miesięcy od daty utraty danych – stąd też możliwość zapewnienia odzyskiwania danych jest kwestią podstawową.

Jednakże kluczem do powrotu do normalnego stanu operacyjnego po awarii jest nie tylko nadmiarowość (redundancja), lecz głównie odporność systemu lub sieci. Aby zapewnić ciągłość działania nawet podczas kataklizmów, takich jak klęski żywiołowe, problemy z oprogramowaniem, terroryzm internetowy czy też wady w projekcie systemów zasilania elektrycznego Data Center, technologia musi zostać wyposażona w rozwiązanie zapewniające niezawodność już na etapie projektu.

Tolerancja błędu

Większość nowych ośrodków zapasowych Data Center jest obecnie budowana daleko od głównych centrów przetwarzania danych. Na podstawie badań przeprowadzonych przez SwissRE, ponad 50 proc. awarii jest związanych z pogodą, jednakże terroryzm również pochłania coraz większe koszty. Według wyników badań, projekty infrastruktury teleinformatycznej oraz systemu elektrycznego muszą charakteryzować się tolerancją wobec wad. Przykładowo, jedno zwarcie nie powinno spowodować zatrzymania funkcjonalności całego budynku. Usterka tego rodzaju powinna zostać opanowana, ponieważ projekt posiada tolerancję uszkodzeń, która stanowi część operacyjnej niezawodności obiektu. Należy wiele uwagi poświęcić kwestii niezawodności w projektach systemów UPS, gdyż znajdują się one w samym sercu każdego Data Center.

Wszyscy wiemy o niedawnych przypadkach, gdy miasta, takie jak Londyn. Nowy Jork, Toronto, Warszawa, Kopenhaga, czy Rzym, pogrążyły si w ciemnościach. W każdym z tych przypadków nastąpiło to z różnych przyczyn – błędu ludzkiego, braku elektryczności, rozregulowaniu systemu, itd. W Europie, zakłady energetyczne są w stanie zaspokoić dopływ prądu w 99,9 proc. (tzn. 999). Dostępność procentowa jest mierzona jako stosunek średniego czasu naprawy (MTTR) do średniego czasu pomiędzy awariami (MTBF), tzn. dostępność = (1 – MTTR/MTBF) x 100. Wskaźnik MTBF można zwiększyć za pomocą wyższej niezawodności sprzętu oraz korzystając z produktów, które posiadają certyfikaty niezależnych organizacji, np. TUV, KEMA oraz Veritas. Ważne jest, aby zarówno sprzęt jak i instalacja jako całość posiadały zdefiniowaną tolerancję uszkodzeń. Mając to na uwadze, po przeprowadzeniu testów fabrycznych, konieczne jest wykonanie testów integralności systemu (SI), który obejmuje wszystkie kluczowe komponenty Data Center – i to zanim zostanie ono przekazane klientowi. Podczas testów integralności systemu, należy dokonać symulacji błędów na różnych poziomach obwodów elektrycznych oraz pozycji mechanicznych w ośrodku Data Center. Ten rodzaj symulacji testów może wykazać solidność projektu systemu, sprzętu oraz instalacji. Testowanie SI pozwala wysunąć na plan pierwszy wszelkie kwestie dotyczące braku kompatybilności pomiędzy różnymi komponentami platformy systemowo-sprzętowej.

Ochrona

MTTR może zostać skrócony poprzez zastosowanie zdalnej diagnostyki on-line (np.: Power Management System) oraz skorzystanie z usług wykwalifikowanych ekspertów, którzy w krótkim czasie potrafią dokonać napraw. Właściwy asortyment części zapasowych powinien być dostępny 24h na dobę, 7 dni w tygodniu. Zwykła dostępność użytkowania na poziomie 99,9 proc. może spowodować 9-godzinne wyłączenie sprzętu lub kilkanaście krótkich wyłączeń (awarii) sprzętu, czy też częściowych wyłączeń. Ponieważ zakłady energetyczne nie muszą gwarantować ciągłości w dostawie swoich usług, instytucje i firmy muszą chronić się przed

taką utratą zasilania. Rzeczywiście, żadna instytucja o charakterze strategicznym dla struktur państwa lub biznesu nie może akceptować takiego poziomu dostępności, dlatego też, niezbędne jest posiadanie ośrodków Data Center wspieranych przez rozwiązania systemowe UPS oraz zapasowe generatory, aby móc zapewnić ochronę dla rdzenia infrastruktury teleinformatycznej.

Aby osiągnąć wysoki poziom niezawodności systemu UPS, należy użyć jednostek, których projekt spełnia standard podwójnej konwersji – IEC 62040. Innymi słowy, sprzęt teleinformatyczny o krytycznym znaczeniu dla biznesu jest chroniony przed wszelkimi problemami związanymi z jakością zasilania na wejściu do UPS-a, niezależnie czy są one związane z napięciem (wartość i przebieg) czy z częstotliwością.

Ważne jest zwrócenie uwagi, iż niektóre UPS-y rotacyjne, a także mały procent UPS-ów statycznych może nie być opartych na budowie podwójnej konwersji.

UPS-y statyczne

UPS-y statyczne wykorzystują baterie akumulatora, aby zapewnić odpowiedni czas potrzebny dla zapewnienia ochrony podczas utraty zasilania lub jego niskiej jakości. Przy takim zabezpieczeniu generatory rezerwowe mają wystarczającą ilość czasu na rozruch i dalsze zasilanie UPS-ów. Przy dużych ośrodkach Data Center warto skorzystać z akumulatorów zaprojektowanych tak, aby posiadały 10 lat żywotności zgodnie ze standardem BS6290 część 4-1997. Niezbędne jest również zainstalowanie systemu monitorowania akumulatorów (np.: brytyjski Cell Watch), który będzie opierał się na technologii sprawdzającej rezystancję wewnętrzną. Jednak, w przeciągu kilku lat bardzo prawdopodobne jest, że baterie akumulatorów zostaną zastąpione przez technologię ogniw paliwowych.

Autonomia akumulatorów może opierać się na wymaganiach, które ustala klient, ale w tego rodzaju aplikacjach jest to zazwyczaj podtrzymanie zasilania na okres 10-30 minut. Zapasowe wytwarzanie energii jest również niezbędne dla zapewnienia napięcia przy długotrwałych przerwach w dostawie prądu, a także, aby zapewnić zasilania dla mniej istotnych obciążeń, takich jak klimatyzacja, oświetlenie, itd.

Rozwiązania redundantne a modułowe

Dobrą praktyką jest posiadanie nadmiarowości n+1 nawet na poziomie zasilania zapasowego, natomiast istotne jest, aby UPS-y były zaprojektowane zgodnie z nadmiarowością n+n. (Jeżeli n stanowi minimalną wymaganą wartość potrzebną do wsparcia obciążenia krytycznego, przykładowo dla UPS'ów o mocy pozornej 2x500 kVA, nadmiarowość n+1 oznaczałaby UPS-y w układzie redundantnym 3x500 kVA, a n+n – UPS-y o napięciu 4x500kVA.) Ważnym jest zastosowanie zewnętrznego scentralizowanego bypassu statycznego (CSB) dla każdego równoległego nadmiarowego systemu UPS. CSB zapewnia wysoki poziom odporności w porównaniu z prostymi systemami UPS o strukturze modułowej. Dzieje się tak ze względu na to, że wartość napięcia przełącznika statycznego STS (Static Transfer Switch) CSB jest ustalona wg. napięcia systemowego, natomiast modułowy system UPS jest zależny od przełącznika statycznego, którego wartość napięcia jest ustalona jedynie dla wartości napięcia konkretnego modułu, tj. zazwyczaj wynosi jedynie 20 proc. napięcia.

Serwery typu blade-servers

Od czasu rozwoju blade-servers dobrze jest posiadać zestawy generatorów, które cechują się znakomitą kompatybilnością z współczynnikiem mocy przy obciążeniu pojemnościowym. Gwarantuje to dodatkowe zabezpieczenie w przypadku, gdy przy wystąpieniu awarii zasilania, cały system UPS przechodzi w tryb obejściowy. Z uwagi na fakt, że więk-szość systemów teleinformatycznych generuje zakłócenie harmoniczne, wskazane jest ograniczanie rozchodzenia się takiego „zanieczyszczenia" poprzez korzystanie z Aktywnych Filtrów Harmonicznych. Pomaga to w redukcji rozmiaru przewodu zerowego, tj. pozwala zmniejszyć koszty miedzianych przewodów, a także eliminuje ryzyko pożaru i kłopoty z samoczynnym wyłączaniem zabezpieczeń. UPS-y należy wyposażyć w odpowiednie aktywne filtry harmoniczne, aby zapewnić utrzymanie poziomu zniekształcenia prądu (THDI) na poziomie 5 proc. lub nawet niższym, niezależnie od obciążenia systemu. To rozwiązanie mogłoby pomóc w realizacji zaleceń G5/4 dotyczących zapobieganiu zakłóceniom.

W celu ograniczenia szkód spowodowanych przez wadliwe źródło, należy skorzystać z przełączników do przenoszenia napięcia statycznego (STS) na poziomie jednostki rozdzielania napięcia (PDU – Power Distribition Unit), dzięki czemu jakakolwiek awaria, która wystąpi zostanie ograniczona tylko do danej części obwodu, a odporność całego systemu pozostanie nienaruszona. Takie jednostki STS działają bardzo szybko (czas przełączania wynosi 2-5 milisekund), dlatego mogą przełączyć napięcie krytyczne z jednego źródła na drugie bez narażania funkcjonalności serwerów.

Wbudowany projekt

Każdy system UPS już na etapie projektowania musi mieć przewidzianą swoją nadmiarowość oraz niezawodność. Gdy projekt jest sprawdzany pod względem punktów awaryjnych, wskazane jest przeprowadzenie testów fabrycznych dla każdego komponentu, tj. systemów UPS, aparatury rozdzielczej, zapasowych zestawów generatorów, itd. Nawet podczas testów fabrycznych dobrze jest przeprowadzić symulację zwarcia po stronie odbiorów, aby pomóc w pomiarze poziomu tolerancji uszkodzeń systemu UPS. Również należy ocenić wyniki testu krokowego do 100 proc. obciążenia systemu UPS oraz generatorów. Zalecane jest użycie odpowiednich systemów monitoringu komponentów o decydującym znaczeniu, takich jak baterie akumulatora UPS, z tego względu, że może to pomóc zespołowi Zarządzania Obiektem na podjęcie proaktywnych działań niezbędnych w celu uniknięcia awarii wewnątrz centrum Odzyskiwania Danych.

Oczywiście, niczym nie można zastąpić planowanej i regularnie przeprowadzanej kompleksowej konserwacji, która powinna również obejmować sprawdzenie komponentów odgrywających decydujące znaczenie, tj. UPS, bypass'y, akumulatory podczas rozładowywania, PDU's oraz aparatury rozdzielczej.

Obudowy teleinformatyczne ZPAS dla służb mundurowych

Komunikacja elektroniczna stanowi obecnie jeden z ważniejszych obszarów funkcjonowania społeczeństw. Jest nową formą komunikacji, wykształconą głównie w wyniku rozwoju kultury masowej i procesu globalnej standaryzacji. Komunikacja elektroniczna nie stanowi jednak atrybutu społeczeństwa masowego, a raczej jest właściwa gospodarce opartej na wiedzy (przy czym zakres stosowania, oprócz gospodarki, obejmuje kontekst socjokulturowy i wszelkie inne dziedziny życia nowoczesnych zbiorowości).

Mówiąc o komunikacji elektronicznej napotykamy problem braku jasnej definicji pojęcia. Dokonując pewnych uogólnień stwierdzić można, że powszechne są dwa sposoby rozumienia, opisu i interpretacji funkcjonowania komunikacji elektronicznej. W rozumieniu pierwszym jest to sposób wymiany informacji, najczęściej w formie dokumentu elektronicznego. Jedną z cech takiej komunikacji elektronicznej jest aktywny udział użytkownika w procesie komunikacji, co powoduje, że omawiane pojęcie można postrzegać jako odniesienie do środka i formy przekazu, w ujęciu klasycznych teorii komunikacji, w tym społecznej. Drugie rozumienie pojęcia pozwala jako komunikację elektroniczną uznać komunikację realizowaną z wykorzystaniem technik telekomunikacyjnych i informatycznych. W tym przypadku znaczącym czynnikiem staje się zabezpieczenie teletechniczne komunikacji, ze szczególnym uwzględnieniem rozwiązań technologicznych, systemów i poszczególnych urządzeń służących transmisji informacji, najczęściej danych. Podział na obszary można rozbudowywać, doprowadzając np. do szczegółowej systematyki z odwołaniem do różnych dziedzin nauki lub dokonując innych form klasyfikacji komunikacji elektronicznej. Powyższe omówienie samego pojęcia miało za zadanie wskazanie właściwego obszaru komunikacji, do którego zamierzam się odnieść. Z perspektywy producenta obudów teleinformatycznych podstawowym zadaniem będzie zastosowanie produktów teletechnicznych w komunikacji elektronicznej, m.in. wykorzystywanych jako zaplecze sieci i systemów służb mundurowych.

Obudowy teleinformatyczne ZPAS SA – szafy kompatybilne SZBk

Produkowane przez ZPAS SA wyroby (przede wszystkim obudowy teleinformatyczne i okablowanie strukturalne) do służb mundurowych trafiły wraz z rozwojem technologii informacyjnych i wprowadzaniem komputeryzacji w policji, wojsku czy w jednostkach alarmowych, gdzie stosowane urządzenia wymagały szczególnego zabezpieczenia ich działania.

W tym sektorze szerokie zastosowanie znajdują obudowy teleinformatyczne marki ZPAS (głównie przeznaczone do zabudowy urządzeń 19" i 21"): szafy serii SZB, szafy serwerowe SZB SE, szafy kolokacyjne DSR. Powszechnie używane są również szafki wiszące ze stelażem 19" (obecnie szafki SD, SJ, SU), a w niektórych przypadkach swoje zastosowanie znajdują szafki SKI 10", które standardowo wykorzystywane są do instalacji sieci LAN.

Istnieje jednak specjalna grupa obudów ZPAS dedykowana dla potrzeb służb mundurowych: szafy kompatybilne SZBk zgodne z wymogami EMC. Tego rodzaju obudowy przeznaczone są do zastosowania wewnątrz pomieszczeń z urządzeniami emitującymi fale elektromagnetyczne. Skuteczność ekranowania zakłóceń szaf SZBk została potwierdzona niezależnymi badaniami dwóch ośrodków: Instytutu Telekomunikacji i Akustyki Politechniki Wrocławskiej oraz Agencji Bezpieczeństwa Wewnętrznego w Warszawie. Gwarancją jest także posiadanie przez ZPAS SA certyfikatów jakości klasy ISO 9001 i ISO 14001, co jednak obecnie stanowi już normę dobrze funkcjonującego przedsiębiorstwa.

Szafy SZBk są kompatybilne z dominującą linią produkcyjną obudów teleinformatycznych ZPAS, co pozwala na zastosowanie wyposażenia dodatkowego tej serii i wykorzystanie rozwiązań występujących w szafach SZB, SZB SE czy DSR. Ta kompatybilność nabiera znaczenia zwłaszcza w sieciach o rozbudowanej strukturze, wykorzystującej różne typy obudów teleinformatycznych, co pozwala na łatwą zmianę konfiguracji i dyslokacji urządzeń – elementów systemu, sieci lub podsieci. Szczegółowy opis wyposażenia dodatkowego obudów teleinformatycznych znajduje się na stronach internetowych www.zpas.pl.

Krzysztof Karwowski
ZPAS SA
kk@zpas.pl

Produkty ZPAS-NET

Oferta produkcyjna ZPAS-NET Sp. z o.o. skierowana jest głównie do branży IT, energetyki, ciepłownictwa oraz innych branż przemysłu. ZPAS-NET zrealizował także wiele zamówień dla straży granicznej, wojsk ochrony pogranicza, straży pożarnej, policji oraz służb więziennych. W 2003 roku na Pokojowych Targach Wojskowych LOGISPOL 2003 otrzymaliśmy puchar jako Nagrodę Dowódcy Pomorskiego Okręgu Wojskowego za „pulpit dowodzenia". Oferta ZPAS-NET obejmuje następujące wyroby:

- ✔ elementy okablowania strukturalnego i osprzęt telekomunikacyjny,
- ✔ szafy zewnętrzne dostępowe,
- ✔ szafy i rozdzielnice NN z wyposażeniem elektrycznym,
- ✔ pulpity dyspozytorskie i sterownicze,
- ✔ synoptyczne tablice mozaikowe,
- ✔ rozproszony system zdalnego nadzoru ZPAS Control Oversee.

Wyroby ZPAS-NET dzięki nowoczesnym rozwiązaniom pozwalają na połączenie grup produktów branży informatycznej i energetycznej. Wszystkie te produkty w sposób bezpośredni lub pośredni pozwalają w optymalny sposób rozbudować infrastrukturę służącą komunikacji elektronicznej sektora energetycznego. Bezsprzecznie coraz większe znaczenie i rangę zyskują systemy monitoringu pracy urządzeń oraz warunków klimatycznych, jakie panują w otoczeniu tych urządzeń. Zarządzanie i kontrola dostępu osób uprawnionych do prac serwisowych, związanych z prawidłową eksploatacją obiektu, nabiera nowego znaczenia w erze wysokiej specjalizacji. Sposób, niezawodność oraz bezpieczeństwo przesyłania i archiwizowania informacji dzisiaj stanowią najważniejsze kryteria, jakim mają odpowiadać systemy elektroniczne. Innowacyjność, rozumiana jako poszukiwanie i wdrażanie nowych rozwiązań technologicznych, jest jednym z istotnych czynników skutecznej konkurencji w warunkach dzisiejszego, globalnego rynku.

System nadzoru ZPAS Control Oversee

System stanowi kompleksowe rozwiązanie umożliwiające budowę tanich i niezawodnych układów zdalnego nadzoru z funkcjami pomiarowo-regulacyjnymi. System jest skalowalny i w pełni niezależny od platformy sprzętowej, bazodanowej i systemowej. Jego architektura umożliwia łatwą rozbudowę o obsługę nowych urządzeń, technologii komunikacyjnych i elementów wizualizacji.

Integralną częścią systemu jest oprogramowanie do tworzenia paneli operatorskich umożliwiających wizualizację stanów aktualnych lub archiwalnych, zdalną zmianę nastaw i konfigurowanie układów lokalnej automatyki.

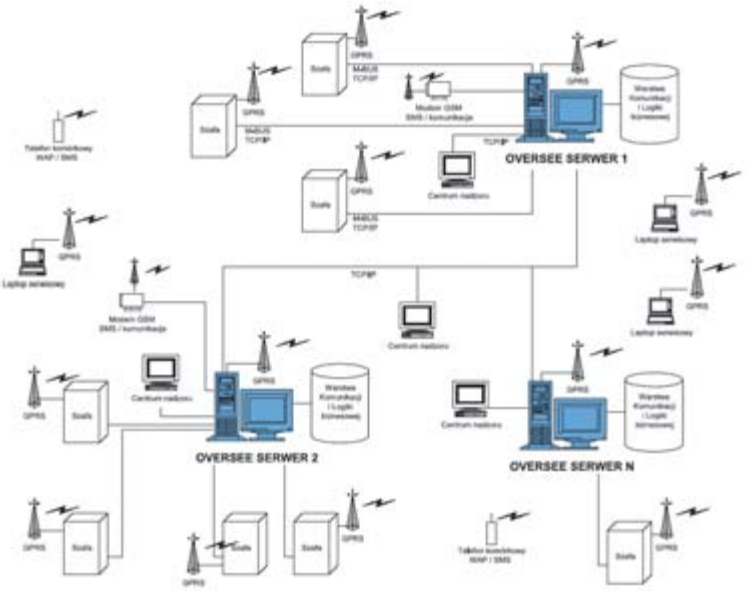
Centralną część systemu ZCO stanowi rozproszony system nadzoru, oparty na nowoczesnych technikach inżynierii oprogramowania, m.in. technologii J2EE (Java 2 Enterprice Edition) i JMX (Java Management Extentions), zbudowany z trzech warstw: komunikacyjnej, logiki biznesowej i prezentacji.

Warstwa komunikacji ma budowę modułową, gdzie poszczególne moduły, przystosowane do systemu operacyjnego i urządzeń, nadzorują komunikację z warstwą logiki biznesowej. Podłączenie nowych urządzeń wymaga dopisania nowego modułu komunikacyjnego, niezależnego od innych funkcjonujących już w tej warstwie modułów, ale nie wymaga wprowadzenia zmian w warstwach logiki i prezentacji. Podstawowym zadaniem warstwy logiki biznesowej jest zarządzanie zbieranymi przez warstwę komunikacji danymi, przetwarzanie ich, optymalizowanie oraz udostępnienie dla warstwy prezentacji, a także sterowanie urządzeniami warstwy komunikacji przy pomocy rozkazów pochodzących z warstwy prezentacji. Ważną rolę, z punktu widzenia bezpieczeństwa systemu, pełnią zastosowane w tej warstwie mechanizmy replikacji i archiwizacji danych, kontroli dostępu i uprawnień oraz rejestracji i obsługi zdarzeń wyjątkowych.

Warstwa prezentacji umożliwia korzystanie z danych udostępnianych przez warstwę logiki biznesowej niezależnym aplikacjom klienckim, przeglądarkom internetowym i urządzeniom mobilnym (np. PDA, telefony komórkowe). System umożliwia dostęp do informacji o obiekcie niezależnie od jego lokalizacji, a dostęp do dowolnego obiektu jest możliwy z każdej uprawnionej lokalizacji. System archiwizuje dane o obiektach i udostępnia mechanizmy ich przeglądania. Dzięki multiserwerowej architekturze oraz procesowi optymalizacji połączeń system jest szybki i niezawodny w przypadku awarii sprzętu komputerowego i zasilania. System ZPAS Control Oversee na XVI Międzynarodowych Targach Łączności INTERTELECOM 2005 otrzymał puchar za najlepszy polski produkt wystawy.

System nadzoru, kontroli i sterowania pracy urządzeń z wykorzystaniem technologii ze swobodnie programowalnym sterownikiem

ZPAS Control Oversee System jest cyfrowym systemem automatyki pozwalającym na budowę efektywnych, tanich i niezawodnych układów pomiarowo-regulacyjnych. Jest on przeznaczony do zastosowania w profesjonalnych zintegrowanych systemach zarządzania budynkami oraz obiektami przemysłowymi. W zakresie sterowania instalacjami grzewczo-wentylacyjnymi, produkującymi i dystrybuującymi energię cieplną, wodę,



gaz i energię elektryczną oraz kontrolę dostępu i sygnalizację alarmową.

Dzięki wykorzystaniu komunikacji w oparciu o standardową magistralę M-Bus pomiędzy jednostką centralną i specjalnie zaprojektowanymi modułami obiektowymi otrzymano optymalne rozwiązanie rozproszonej architektury pozwalające na łatwą rozbudowę i skalowalność systemu.

M-Bus jako międzynarodowy standard przesyłania danych z urządzeń rozliczeniowych pozwala na pozyskiwanie ich w oparciu o proste i tanie interfejsy, sieć o dowolnej topologii i hierarchicznej strukturze, a w efekcie większą skuteczność i prostotę oprogramowania. Swoboda w tworzeniu topologii sieci oraz zasilanie jej elementów w ramach własnej struktury dodatkowo obniżają koszty budowanych układów.

W zakresie oprogramowania system oferuje unikatową koncepcję archiwizacji tworzącą rozproszoną obiektowo bazę danych pomiarowych. Każda jednostka centralna posiadając odpowiednio duże zasoby pamięciowe zapisuje dane w swojej pamięci. Następnie dzięki prostemu i taniemu systemowi wizualizacji następuje udostępnianie ich użytkownikowi oraz uzupełnianie archiwów na dysku twardym stacji operatorskiej. Jednocześnie system współpracuje z dowolnymi pakietami wizualizacyjnymi typu SCADA.

Prosta, szybka i tania zabudowa elementów systemu możliwa jest dzięki zastosowaniu obudów zgodnych z powszechnie stosowanym standardem dla elektrycznej aparatury połączeniowej małej mocy.

Sieciowy system pomiaru i nadzoru warunków klimatycznych z wykorzystaniem technologii 1-Wire

Ze względu na dużą elastyczność i otwartość technologii, firma ZPAS-NET zdecydowała się rozszerzyć swoją ofertę dotyczącą urządzeń i systemu monitoringu o urządzenia pracujące na magistrali 1-Wire. Aby zbudować sieć 1-Wire, wystarczy podłączyć czujnik do „kostki" z przetwornikiem, dodać do tego przewód sygnałowy. W wersji minimalnej jest to pojedynczy przewód (2-żyłowy), by zapewnić zasilanie i transmisję danych. Do pojedynczej magistrali (master bus), można przyłączyć wiele urządzeń pracujących w trybie slave. Każde urządzenie podrzędne ma indywidualny, 64-bitowy adres, dzięki czemu jest łatwo identyfikowane nawet w dużej sieci. Sieć komponentów typu 1-Wire może być przyłączona pojedynczą magistralą komunikacyjną bezpośrednio do PC lub do sterownika. Technologia ta pozwala również na budowanie większych sieci o dowolnej topologii bez wykorzystania koncentratorów. Jeżeli zajdzie potrzeba rozdzielenia podsieci, można to zrobić przy zastosowaniu hubów 1-Wire. Ze względu na różnorodność oferowanych komponentów, dostępność materiałów i niskie ich ceny, sieci 1-Wire stają się niezwykle użyteczne w monitoringu serwerowni, szaf teleinformatycznych oraz tworzeniu systemów inteligentnych budynków. Należy zaakcentować niezawodność i funkcjonalność współdziałania tej technologii z systemem monitoringu ZPAS Control Oversee, który umożliwia gromadzenie, przetwarzanie i udostępnianie danych.

Uzupełnieniem do urządzeń na magistrali 1-Wire jest sterownik umożliwiający podłączenie sieci do rozproszonego systemu monitoringu ZPAS Control Oversee. Dzięki niemu można już przy niewielkich nakładach monitorować i sygnalizować warunki w wielu oddalonych od siebie obiektach.

Roman Głaz
ZPAS-NET sp. z o.o.

PKI – lek na całe zło, czyli bezpieczeństwo informacji

Nieustanny rozwój technologii IT powoduje rewolucyjne zmiany w posługiwaniu się informacją. Dokument elektroniczny, coraz skuteczniej wypiera swego tradycyjnego, papierowego poprzednika począwszy od momentu zapisu informacji, poprzez wysyłkę i odbiór, aż po archiwizację i długookresowe przechowywanie. Wzrost liczby przetwarzanych dokumentów elektronicznych oraz ich transmisja przez publiczne czy wydzielone łącza pociąga za sobą wzrost e-przestępczości. W ostatnich latach użytkownicy odnotowują znaczące nasilenie prób włamania do systemów informatycznych oraz kradzieży danych. O tym, że próby te bywają udane przekonali się niedawno klienci jednego z polskich banków, z którego kont zniknął blisko milion złotych. Straty wynikające z opisanej sytuacji mają wymiar nie tylko ekonomiczny, ale także społeczny, gdyż utrata zaufania do instytucji finansowej może przyczynić się nawet do jej upadku.

Jak natomiast mierzyć straty będące skutkiem kradzieży danych z systemów wykorzystywanych przez policję, wojsko, straż graniczną lub inne służby mundurowe? W przypadku prób kradzieży informacji z wyżej wymienionych systemów mamy, bez wątpienia, do czynienia z działaniami o charakterze szpiegowskim lub terrorystycznym. Skutki takich działań mają wymiar, poza ekonomicznym i społecznym, także polityczny i są zazwyczaj znacznie poważniejsze. Dlatego też niezbędne jest stosowanie narzędzi odpowiednich do skali zagrożenia i gwarantujących najwyższy poziom bezpieczeństwa przetwarzanych danych.

Infrastruktura klucza publicznego – PKI (*Public Key Infrastructure*) zajmuje szczególne miejsce wśród rozwiązań dotyczących zabezpieczania danych elektronicznych, ponieważ systemy konstruowane na bazie PKI łączą w sobie ochronę dokumentów (podpis elektroniczny, szyfrowanie), kontrolę dostępu do pomieszczeń i obiektów (zarządzanie uprawnieniami i monitorowanie wykorzystania uprawnień) oraz systemy uwierzytelniania i autoryzacji do systemów informatycznych (aplikacje, bazy danych, serwery).

Unizeto Technologies SA jest wyróżniającym się dostawcą kompleksowych rozwiązań z dziedziny PKI. Współpraca spółki z odbiorcami dotyczyć może dowolnego obszaru wyżej wspomnianej tematyki, począwszy od audytów bezpieczeństwa systemów informatycznych, poprzez kompleksowe dostawy sprzętu i oprogramowania, wdrożenie, integrację i serwis rozwiązań typowych lub dedykowanych oraz usługi szkoleniowe.

W przypadkach gdy decydujące znaczenie ma aspekt ekonomiczny i pozwalają na to wymogi bezpieczeństwa, możliwe jest skorzystanie z systemów utrzymywanych na serwerach Unizeto (outsourcing) bądź samodzielna budowa dedykowanego rozwiązania przez klienta przy udzielonym wsparciu Unizeto.

40 lat na rynku, ponaddziesięcioletnia aktywność w obszarze technologii kryptograficznych, siedmioletnie doświadczenie w świadczeniu usług certyfikacyjnych związanych z podpisem elektronicznym oraz kadra ponad 200 wysoko wykwalifikowanych specjalistów to zaplecze firmy. Ponadto realizacja największych w Polsce wdrożeń dotyczących infrastruktury klucza publicznego zakończonych sukcesem, referencje zadowolonych klientów, także spośród służb mundurowych, stawiają Unizeto Technologies SA wśród partnerów godnych zaufania.

Oferta software'owa Unizeto Technologies obejmuje trzy podstawowe grupy rozwiązań:

- ✔ oprogramowanie serwerowe,
- ✔ gotowe aplikacje klienckie,
- ✔ narzędzia programistyczne do implementacji funkcjonalności PKI w innych systemach.

Wszystkie procedury realizowanych przez Unizeto Technologies procesów są zgodne z ISO 9001:2000 oraz AQAP 2110. Firma przeszła także pozytywnie audyt weryfikujący zgodność z kryteriami WebTrust określonymi dla centrów certyfikacji świadczących usługi związane z podpisem elektronicznym i znakowaniem czasem.

Posiadane koncesje:

- ✔ Koncesja MSWiA na wykonywanie działalności gospodarczej w zakresie wytwarzania oraz obrotu wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym;
- ✔ Koncesja na prowadzenie działalności gospodarczej w zakresie usług ochrony mienia realizowanych w formie zabezpieczenia technicznego.

Od grudnia 2004 roku Unizeto Technologies SA ma przydzielony Kod Podmiotów Gospodarki Narodowej NATO (*NCAGE – NATO Commercial and Government Entity Code*).

Jacek Wojtala
zastępca dyrektora
Sektor Służb Mundurowych
Unizeto Technologies SA
www.unizeto.pl; www.certum.pl

www.unizeto.pl

UNIZETO TECHNOLOGIES SA

Producent i integrator rozwiązań informatycznych

Podpis elektroniczny i kontrola dostępu

Unizeto Technologies SA

- producent, dostawca i integrator systemów tworzących infrastrukturę klucza publicznego oraz aplikacji wspierających wykorzystanie podpisu elektronicznego

CERTUM
Powszechne Centrum Certyfikacji

- certyfikaty kwalifikowane
- certyfikaty niekwalifikowane
- znakowanie czasem

Systemy Kontroli Dostępu

wykorzystujące kryptograficzne karty mikroprocesorowe stykowe i bezstykowe

- systemy jednokrotnego logowania do systemów informatycznych
- do stacji roboczych
- do pomieszczeń
- systemy Rejestracji Czasu Pracy

Unizeto Technologies SA posiada koncesje Ministerstwa Spraw Wewnętrznych i Administracji:
- na wytwarzanie wyrobów oraz obrót wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym,
- na prowadzenie działalności gospodarczej w zakresie usług ochrony mienia w formie zabezpieczenia technicznego.

www.certum.pl

UNIZETO CERTUM

POWSZECHNE CENTRUM CERTYFIKACJI

INFOTEL'S LIBRARY

ELECTRONIC COMMUNICATIONS FOR OPERATIONAL SERVICE

Price 15 zł (0% VAT incl.)
ISBN 83-921962-4-4

- Next generation networks
- VoIP telephony
- Specialized computers
- Powering devices
- Radio-telephones and radio stations
- Data transmission systems
- Control systems
- Structural cabling systems

DIALOG
expert in telecommunications

Protected DIALOG

Telefonia DIALOG S.A. acquired

Certificate of Industrial Security

DIALOG guarantees the highest quality of voice and data transmition services on the basis of worldwide recognized standards of information security.

→ QUALITY

→ RELIANCE

→ PROTECTION

www.dialog.pl | TeleCentrum 0 801 700 700

MGE UPS SYSTEMS

PULSAR STS 16
power supply
redundancy
for single phase
equipment

PULSAR EVOLUTION
from 500 to 3000 VA
1U or 2U
in the rack

COMET EX RT
on-line, 7/11 kVA
rack 6U

MGE
UPS SYSTEMS

www.mgeups.pl
022 511 83 45
mgeups@mgeups.pl

ISBN 83-921962-4-4
Price 15 zł (0% VAT incl.)
Issue: 7000 copies

Publisher:

MSG – Media s.c.
Stawowa 110 Str.
85-323 Bydgoszcz
phone (52) 325 83 10
fax (52) 373 52 43
office@msgmedia.pl
www.techbox.pl

Editing Team
Marek Kantowicz
Grzegorz Kantowicz
Robert Błaszczyk

DTP
Czesław Winiecki

Marketing
Janusz Fornalik
Arkadiusz Damrath

Proof-read
Ewa Winiecka

Printing office
ABEDIK
Sp. z o.o.
85-861 Bydgoszcz
Glinki 84 Str.
phone/fax (52) 370 07 10
info@abedik.pl
www.abedik.pl

LIST OF CONTENTS

www.zpas.pl
www.zpas.net

Data and telecommunication enclosures

Industrial enclosures

Outdoors cabinets

Structured cabling and telecommunication accessories

Control and dispach desks

ZPAS Control Oversee

ZPAS

Telephone: +48 (074) 872 0 100 (head office)
Fax: 074 / 872 40 74, 872 55 92
e-mail: info@zpas.pl
Web pages: http://www.zpas.pl

ZPAS-NET

Telephone: 074 / 872 0 122 (head office)
Fax: 074 / 872 58 56
e-mail: info@zpas.net
Web pages: http://www.zpas.net

Central Scotland Police migrates to Microsoft

Central Scotland Police and Microsoft Ltd. announced that Microsoft Windows has been selected as the police force's platform of choice. Under the new contract, Central Scotland Police will replace some open source technologies with Microsoft Windows Server 2003, Microsoft Windows XP and Microsoft Office to support the police modernization agenda, flexible working arrangements and better engagement with other public sector partners. The migration will affect over 550 workstations and servers. What is the most improtant, will not require any extra costs of hardware upgrade.

Central Scotland Police and Microsoft will work together closely on a range of information and communication technology (ICT) projects. These will include an electronic document management system for better response to requests under the Freedom of Information Act, and document sharing for police staff that will help deliver best practices and achieve better value for money.

– *Central Scotland Police has always been forward-thinking in its use of information and communication technology to help protect the public and provide efficient and value-for-money services to communities* – said **David Mulhern**, deputy chief constable for Central Scotland Police. – *In the current security environment there is a growing need for local force systems and national standard systems to converge where possible, and to streamline communication with criminal justice partners. Having a committed, reliable and value-conscious software partner that shares our vision and recognizes the challenges facing modern policing is critical.*

Through the "Safer Central" policing philosophy (see below), which underpins the way in which Central Scotland Police currently operates, and Operation Advance, one of the five operational pillars of the philosophy (see below), the force has been focused on improving efficiency to deliver more effective frontline service to communities in Central Scotland.

A key factor in that drive has been value for money, and a review of the police force's information technology (IT) department at the start of 2005 concluded that Central Scotland Police would achieve better value and greater efficiency through the following changes:

- ✔ immediate use of off-the-shelf programs to reduce the need for customized applications,
- ✔ greater compatibility with partner organizations' ICT systems,
- ✔ increased staff satisfaction through use of familiar technology,
- ✔ reduced number of operating systems,
- ✔ increased access to a wider range of software products.

This was followed by an extensive study completed by the police force in March 2005 that resulted in

Central Scotland Police's decision to work with Microsoft through a new three-year Enterprise Agreement.

– *Naturally we are delighted with the conclusions arrived at by Central Scotland Police, which enable us to prove the value and interoperability that Microsoft products offer. We look forward to working with the police force to introduce new products and services, including document and record management and collaboration technology* – said **Terry Smith**, senior director for Microsoft Ltd.

The benefits-based evaluation led Central Scotland Police to prefer a Microsoft solution over its legacy open-source solution that was introduced in 2000. Microsoft Windows was judged to offer the best overall value for money and operational functionality. In some areas open source installations will be retained.

– *Although an open-source solution met our needs in the past, it was becoming more difficult to maintain in the increasingly joined-up environment of today* – said **David Stirling**, head of ICT for Central Scotland Police. – *As the need for increased integration and compatibility with other criminal justice agencies and community partners grows, the value of similar infrastructures becomes more important. A shift to a largely Microsoft infrastructure gives us the ideal platform from which to drive this convergence forward.*

The decision to implement Microsoft Windows and Microsoft Office will bring a number of benefits to Central Scotland Police. The study showed that the police force will achieve significant annual savings. Charteris plc, a Microsoft partner, is providing training and consultancy.

– *Central Scotland Police is basing its IT system on the Microsoft platform because its internal study shows that it offers the best value in total cost of ownership, ease of use, interoperability, reliability and support* – said **Nick McGrath**, head of Platform Strategy for Microsoft Ltd. – *Central Scotland Police estimates that it could save 30 percent on IT maintenance costs and 25 percent of IT staff's time by using Microsoft technology.*

The Microsoft agreement also paves the way for Central Scotland Police to introduce new ways of working for its frontline police officers.

– *Previously our police officers could only access the wide range of IT solutions available to assist them in their work from their base location. This presented real difficulties when deciding on strategies to respond to community concerns* – Mulhern said. – *In the future, officers will be able to go to where they can be most effective and at the same time access the full range of IT solutions, which will enable them to do their job better.*

Operational Chief Inspector **Alan Douglas** added: – *For staff to be able to carry out their duties without the restriction of having their IT facilities at only one location will remove a barrier to efficient working and shall allow them to complete all their duties from the place where they can be most effective.*

Implementation of the Microsoft platform began in August, following Central Scotland Police's involvement in the policing of the G8 Summit.

Safer Central is the over-riding philosophy by which Central Scotland Police carries out its day-to-day business. It underpins the process by which all aspects of Central Scotland Police's communities' concerns are addressed and it endeavours to target these issues in an intelligence-led and meaningful way. Listening to community concerns and responding in an appropriate manner is the cornerstone of the Safer Central philosophy. The philosophy is implemented on a daily basis through five operational pillars – Safeguard, Overlord, Reassurance, Tundra and Advance.

Operation Advance is Central Scotland Police's approach to providing support to the four other operational pillars of Safer Central. It is achieved through successful implementation of key strategic initiatives and developments, currently taking place throughout the police force. These initiatives continue to transform the way Central Scotland Police delivers its services by the introduction of new technology, with a key aim to reduce the burden of paperwork, giving officers more time to do what they do best – policing their communities.

Based on Microsoft Corp. information

Europe's largest IP communication network

The borders of Poland form the eastern boundary of the newly-enlarged European Union. One of the most important elements required to keep the borders tight and secure is fast and reliable communication. NextiraOne has installed the continent's most extensive IP network to link all 268 border crossing points, providing added security through centrally-managed access to local databases and government information.

The Client

Straż Graniczna is a government unit operating on Poland's borders, specialising in the regulation of trade and traffic across the country's 3500 km frontier. It operates through its main headquarters in Warsaw and 15 branch offices which direct 268 checkpoints and sentry points, located directly on the border itself.

The Challenge

Poland now constitutes the European Union's eastern boundary so an efficient communication system on its borders was essential as part of its new legal, commercial and security obligations.

The current network was fragmented, based mainly on obsolete analog technology supplemented by occasional digital equipment. This resulted in high maintenance costs for a system which was both unreliable and not easily scalable.

Initial specifications favoured a single, centrally-managed system which linked all the highly dispersed border points with their branch offices, offering the same level of secure access to centralised services including key government databases and the Internet. An IP telephone solution was selected for this complex and geographically distributed network as it would establish a flexible platform for new applications and integration. Additionally, a centralised Network Management System could be established to monitor the data, voice and Ethernet networks.

Straż Graniczna commissioned NextiraOne Polska to implement the system due to its expertise in voice and data systems integration, well-developed Polish service network and knowledge of public sector project management. The company could also build upon 10 years of successful co-operation with national telecoms operator, Telekomunikacja Polska SA (TP SA) whose outsourcing model enabled the government to finance the construction of such a capital-intensive scheme.

The Solution

Straż Graniczna now has one of the most modern communication tools in Europe, including guaranteed secure links to domestic systems such as KSI (Domestic Information System), CEPiK (Central Vehicle and Driver Register) and the Repatriation and Foreign Office system. It also permits efficient links to the Schengen Information System, which is at the heart of Europe's zone of easy cross-border travel.

Implementation began in January 2003, following the three-month laboratory test of a full system configuration by NextiraOne. As this was destined to be the largest IP installation in Europe, pre-analysis was essential to prove the concept and accelerate its eventual installation.

NextiraOne Polska engineers designed a nationwide IP telephone network based on Cisco equipment and utilising the existing transmission network and cabling laid by Telekomunikacja Polska Polpak. This feature enabled significant savings to be made over the cost of new structural cabling in Straż Graniczna buildings.

System implementation was divided into three phases, initially concentrating on the key elements within the headquarters and branch offices. Attention was then transferred to equipping the checkpoints and sentry points, followed finally by the installation of the applications and Internet

access. Specific blocks of the system were launched at approximately 4-week intervals with each release being preceded by detailed system tests.

The most challenging aspect of the installation was the transfer of users and applications to the new platform as these migrations could not interrupt the 24 hour work of Straż Graniczna officers or deny access to critical applications.

How does it work?

The telephone network, comprising over 6600 Cisco phones, is based on local PSTN links whilst calls between the locations are made through the IP system using a private number plan but each phone can also be reached directly from the public network, thanks to router translation. NextiraOne has established a central phonebook database and the facility for short text messages (SMS) has proved popular as it allows announcements to be sent simultaneously to previously-defined groups of users.

Each phone can be connected to a PC network, allowing secure Internet access without the need for extra cabling: in order to guarantee security, the Internet network has been located on a different VLAN to the voice traffic. In addition to email and operational use, Straż Graniczna employees now access the Web for e-learning programs to update skills and participate in additional training.

NextiraOne maintains the network from a central site in Warsaw, equipped with software tools for monitoring, management and cost allocation functions: regional administrators have remote access to the system from any point on the network. Comprehensive technological and administrative training programmes have already been completed for the Straż Graniczna employees who will eventually be responsible for system management and further network enhancements.

Piotr Jarmoliński
Sales Manager NextiraOne Polska

Teletra-Komtrans SA solutions

Teletra-Komtrans SA was founded in September 1991, on initiative of the R&D Office and Prototype Department, employees of the former WZT Telkom – Teletra state factory. We produce and distribute telecommunication equipment, provide installation, maintenance and start-up services.

Our position at the market is connected with the quality of the offered coherent technical solutions dedicated to our customers. We offer a wide range of transmission (xDSL, OLE) systems and Digital Access Systems/Multiplexers of the best worldwide telecommunication companies, also covering solutions for voice and data transmission with compression. We are leading Polish producer of the wide sort of optical patchcords equipped with SC PC, SC APC, FC PC and E-2000 PC connectors as well as APC and MTRJ optical fibre connectors. In addition we are the exclusive producer of the Remote Cardiologic Monitor system (Tele-ECG). The system enables transmission of the ECG graph through the GSM and GPRS systems to the dedicated Diagnostic Cardiologic Centre. In July 1999, we were granted a Quality Certificate issued by TÜV Rheinland EUROQUA that confirms the compliance of the implemented Quality Management System with the international standard ISO 9001.

XDSL Access Systems

LR HDSL system transmits and receives 2 Mbps symmetrically via copper pairs. The family consists of: A1512 PL LC – universal line card working as 1- or 2-pair HDSL; desktop housing with digital interface. A variety of available user interfaces: G.703, G.704, ISDN PRA, V.11, X.21, V.35/V.36, Ethernet 10Base-T with bridge/router functionalities.

LR SDSL/SHDSL is the transmission system in Classic version, compliant with **ITU-T G.991.2.** A variety of interfaces: G.703, G.704, ISDN PRA, V.11, X.21, V.35/V.36. This system installed in the housing with Ethernet 10Base-T interface is the modem with bridge /router functionalities.

Transmission cards **LR xDSL** can be installed in **A1512 SRV** subracks. All systems from the above family can be managed via **ASMOS** management system. **LR xDSL** systems are present in TP SA network (including POLPAK) and are applied also by Netia and other operators.

FlexDSL SHDSL family is considered to build long range SHDSL links. This system supports and manages up to 10 repeaters with full retransmission. Two repeater types are available: basic, only with retransmission (1-pair or 2-pair), extended, with Add-Drop function (1-pair); G.704 interface available, optional: nx64, RS232/485. Depending on the software configuration FlexDSL SHDSL modems are working as 1-pair, 2-pair systems or Multipoint mode. These devices support G.703, G.704, X.21, V.35, V.36 interfaces. A multiplexing of E1 and nx64 interfaces is also available – Multi-Service option. FlexDSL SHDSL systems are applied mostly in Railway Telecom network.

OLE – Optical Fiber Systems

The main optical systems in our offer are: **FE 80/160/320** – E1 multiplexers (G.703/G.704) 4, 8, 16 interfaces accordingly; **FlexGain FOM** – multiplexers with variety of interfaces (G.703/G.704, V.35, 10BaseT); we offer also manageable or non-manageable optical media converters for different Ethernet standards (10/100/1000 Mbps) for SM or MM fibre.

Broadband Access

We offer IP DSLAM ADSL system and ADSL modems /routers. Using the latest ADSL/ADSL2/ADSL2+ technology, **Turbolink IP DSLAM ADSL** has been designed for Network Service Providers to offer excellent services to multiple subscribers with features

such as bandwidth management, traffic prioritization, data flow security control etc. Depending on version this device offers 24 or 48 ADSL ports with built-in splitters. DSLAM supports replaceable 100/1000BaseT or FX uplink/subtend modules. Up to 8 devices can be cascaded and managed as one unit.

The Turbolink IP DSLAM is interoperable with any industry standard ADSL, ADSL2 and ADSL2+ modem over the local loop.

Pair Gain Systems

Pair Gain Systems 4, 11, 16 and 3A/2I are the solutions for quick and cheap multiplication of subscriber links. 3A/2I device offers 3 analogue and 2 ISDN BRA interfaces. We offer a variety of accessories for Pair Gain Systems and also the management system, allowing line measurement, devices configuration and tests; The new feature in Pair Gain family are devices working in SHDSL. These are Pair Gain devices with 4 and 12 analogue interfaces. As an addition to the 3A/2I device we offer **ISDN S0 Extender**, dedicated for range extention of ISDN BRA links.

Packet Networks With Compression

NetPerformer multi-service access platform is a key to successful and cost-effective converged network that can be flexibly architected to support a variety of applications including toll by-pass, videoconferencing, distance learning and more. Combining the

functionality of data router and a voice gateway in a single device, NetPerformer consolidates all communications traffic onto a single, bandwidth-efficient network infrastructure with a leading edge of QoS.

Solutions For Access Networks

The ***NETmaster*** family of Access Multiplexers is designed to manage 2 Mbps data streams on the 64 kbps slots level and supports a wide range of network interfaces, TDM or IP-based, enabling to make an optimum use of available resources. The NET-

master multiplexers enable to provide the users with a wealth of services, including voice, data and video, over a single access line. NETmaster devices are designed for telecommunication operators, ISPs/ASPs, LAN/WAN integrators, and large and medium-sized enterprises. On the one hand, NETmaster minimizes the network resources necessary to provide carrier services. On the other, it can be used to increase the capacity of the last-mile access networks.

Optical Fibre Accesories

Since 2000 we manufacture **optical fiber patchcords and pigtails** made on the basis of AMP and Reichle & De-Massari connectors. We offer full range of cables with connectors like: E2000, MTRJ, FC, SC, ST, LC, LX5, MU. Our cables are widely applied on the market of telecom services, CATV, in LAN and WAN networks.

As an addition to our offer we have also optical fiber accesories like **distribution frames and splice closures** and, on customer request, we deliver splitters, attenuating patchcords, WDM and DWDM systems.

Cardiac Telemonitoring System

TELE-ECG System allows to receive ECG signals by various telecommunication connections, including GSM mobiles. In this way, ECG examinations could be made in different places. The system consists of **Event-Holters** – personal devices carried by the patient and **CardioScp software** allowing acquisition and analysis of ECG records. The family of Event Holters consists of 3 device types:

- ✔ **EHO6** – three electrodes, two or six simultaneous leads, powered with 2 x 1,5V battery, exhausted battery signalling, option to make two heart Wilson leads from among leads V1 to V6, or six limbal leads I, II, III, aVR, aVL, aVF;
- ✔ **EHO8** – just like EHO6, but six electrodes, eight simultaneous leads;
- ✔ **EHO3** – four electrodes, three simultaneous leads, powered with 2 x 1,5V battery, exhausted battery signalling, option to make three leads from among V1-V6, option to make course of a rehabilitation run desined to be used by patients who need to be rehabilitated at home.

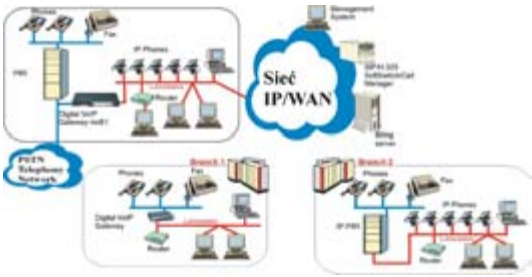
Another device included in this system is **PP-05 v12** – full, 12 lead portable ECG device with touch-sensitive LCD display, also cooperating with CardioScp software. ■

New Generation IP networks implementation

Since 1982 Computex Telecommunication is a leading provider of new generation telecommunication IP solutions in the polish market. Computex NGN (Next Generation Network) solutions are based on low cost, scalable, high quality and reliable multiservice platform which enables to provide data, voice and multimedia services.

In base of the years of experience in implementation of VoIP-NGN networks, Computex Telecommunication became a leading integrator and supplier of IP technology for enterprise customers and government institutions.NGN projects include routers, switches and a large variety of IP equipment like IP phones, analog VoIP gateways, digital VoIP gateways, hybrid IP- PBX gateways with FXO, FXS and E1 interfaces.

Computex NGN solutions architecture



Computex IP solutions are based on Audiocodes and ArelNet equipment which are pioneers in the VoIP market and providers of value added services market segments. AudioCodes company is a market leader in voice compression technology and is a key originator of the ITU G.723.1 standard for the emerging Voice over IP market. Analog Media Gateways and MediaPack Series – The MediaPack™ Analog Media Gateway product family is based on AudioCodes' field-proven and best-of-breed VoIP technology. Featuring 2, 4, 8 or 24 analog ports, the gateways connect analog terminals, PBXs or key systems to the IP network using FXO or FXS connectivity. Compliant with multiple protocols including SIP, H.323, MGCP and MEGACO, the Analog Media Gateways enable flexible deployment and interoperability for the evolving next generation networks. Digital Gateways (2000 series) – With up to 16 E1/T1 digital trunks, the Mediant™ 2000 VoIP media gateway supports G.711 (PCM), G.723.1, G.729A channels. The Mediant 2000 has a dual power supply and complies with NEBs level 3 as well as SIP, H.323, MGCP and Megaco protocols.

Arelnet offers the customers a complete IP telephony solution including:

- ✔ VoIP Gateway (i-Tone Prime and i-Tone MiniPrime),
- ✔ Softswitch/Gatekeeper,
- ✔ Supplementary services,
- ✔ Routing control capabilities,
- ✔ IN services,
- ✔ Cellular to VoIP unique services,
- ✔ Subscriber management,
- ✔ Comprehensive Distributed Network Management (i-Tone NMS),
- ✔ Prepaid solutions (i-Tone Prepaid System) – Enhanced SS7 signaling gateway for integration with the PSTN (i-Tone SIU).

SECURITY and QUALITY

Using IP network as a transmission media for the institutional and government customers Computex utilizes additional security mechanisms and testing procedures which enable to provide high quality and secure:

- ✔ Blocking ports which are not used in the network by equipment and applications,
- ✔ Access list (IP filtering),
- ✔ SSH secure voice and data transfer,
- ✔ MAC address filtering,
- ✔ Secure VPN networks creation,
- ✔ Utilization of coding methods,
- ✔ Ports scanning.

Computex New Generation Networks main advantages:

- ✔ Gradual transformation of different kind of networks in one integrated multiservice network,
- ✔ Centralized management and billing,
- ✔ Data and voice integration
- ✔ Possibility to select the most appropriate telephony and data providers,
- ✔ Low maintenance and operation costs,
- ✔ Large variety of services in one integrated network (telephony, video on demand, e-learning, pre-paid, video conference, e-mail, web, etc.),
- ✔ Fast deployment of new localizations (branches),
- ✔ Mobility (easy displacement of single users and groups of users, easy phone extensions mobility),
- ✔ Low telephony expenses between branches,
- ✔ Easy deployment of new services.

Computex Telecommunication is the exclusive representative of ArelNet and Audicodes distributor in Poland.

More information about Computex Telecommunications solutions can be found at our Web page: www.computex.com.pl/voip

New radio stations, new features

Modern military communication systems require higher and higher speeds of information transfer and visualising of a situation on the battlefield. Fast and reliable data transfer, message exchange and transfer of pictures via radio have greater and greater significance. The transmission of geographical location of mobile objects and displaying them on a digital map, transfer of data to object tracking systems and fire guiding systems is also important.

The access to the Internet network becomes more and more significant. Therefore the demands made for communication means which must realise these tasks are still growing. One of the most important parameters of modern tactical communication is the fast data transmission.

Meeting these expectations RADMOR consequently introduces new equipment into its offer and modifies this already manufactured. Beginning from 2006 RADMOR company starts the production of two licensed F@stnet radio stations – the new generation of the PR4G system. Thus Poland will be the second country to which the Thales company transfers the production of this equipment. The costs connected with the production process transfer will be partly covered by offset commitments of the Thales Netherlands company arisen by the realisation of another project. Therefore Polish army will get new radiostations produced in Poland without additional expenses. The adequate acts of law have been signed and RADMOR already began implementation of the production process for the F@stnet radiostations.

They will be RRC 9210 manpack and RRC 9310 vehicle radiostations which are fully compatible with the RRC 9200 and RRC 9500 radiostations already used by Polish soldiers since 1997. Due to modern technical solutions the F@stnet radiostations have new functions and the manpack station is almost twice lighter than its predecessor.

The data transmission speed four times higher than in the previously produced models is the important feature of new equipment. The synchronous data transmission can be realised with the rates of 50 to 19200 b/s with error correction and 42660 b/s without this correction. New multilevel modulation has been used for fast data transmission (over 4800 b/s). All radiostations are equipped with the vocoder enabling voice communication in the environment with high interference. The vocoder works with rates of 800, 2400 b/s (according to STANAG standard) and also with 4800 b/s.

"Multiplex" – the new operation mode ensures simultaneous transmission of voice and data transfer with the rates of 1200 or 600 b/s. The F@stnet radiostations enable also the transfer of files and E-mails using standard software e.g. Microsoft Outlook. On the

Handheld radiostation 3501 in Iraq

customer request the radiostation can be equipped with the internal GPS receiver which makes possible to transmit and receive geographical positions of all radiostations operating in the network. The position can be entered into the digital map together with the monitored radiostation identification number. RADMOR recommends to equip the RRC 9310 board radiostations with GPS antenna integrated with the VHF antenna so eliminating the need of additional antenna installation for the Satellite navigation system GPS.

New possibilities of data transmission have also been introduced into the 3501 handheld radiostation which is the own design of RADMOR. New models of the radiostation have two modems built-in: one for slow and second for fast data transmission.

The first one is used for transmissions of short data of up to 200 bytes length e.g. statuses or GPS position. The fast transmission is used for transfer of lager files such as pictures, texts or computer programs.

The 3501 handheld radiostation new versions have the GPS receiver built-in and the special software makes available many functions for processing of the information on GPS locations of different objects.

The radiostation can operate on channels dedicated either only for voice or only for data transmission as well as on channels allowing both: voice and data with automatic switching from voice to data but the data transmission has the higher priority than the voice.

The automatically switched channels are very convenient where using the GPS functions is necessary as it is then possible not only to send geographical position but also to monitor the voice traffic in the channel. The users of new 3501 radiostation can also send and receive so called statuses that is the digital messages. They are always chosen manually by the operator. The received status number can be converted into its full alphanumeric form in the computer.

The 3501 radiostation is equipped with the RS232 interface used for programming data transmission parameters from PC and sending or receiving data from external DTE (e.g. PC). The data transmission from an external source may take place. For example, in a vehicle equipped with the V3501 radiostation (it is the vehicle version of 3501 handheld radiostation) and PC computer.

The data can be then exchanged with another V3501 radiostation or base station having the compatible modem (e.g. RRC 9200 or RRC 9500 equipped with the 0423 interface).

The operation modes of the 3501 new versions are as follows:

- ✔ analogue open or scrambled voice transmission,
- ✔ scrambled digital voice transmission,
- ✔ digital ciphered voice transmission with external encryption device,
- ✔ tone selective call,
- ✔ access to telephone network,
- ✔ synchronous data trasmission with the rate of 16 kb/s with GMSK modulation,
- ✔ asynchronous data transmission with the rate of 4800–24000 b/s with 4L-FSK modulation,
- ✔ data transmission with the rate of 1200 and 2400 b/s with FFSK modulation,
- ✔ transmission and reception of statuses,
- ✔ reception of GPS position from GPS receiver, its display on own display and sending it via radio.

The modern “battlefield” means not merely military operations but also anti-terror operations, particularly important today. They require co-operation not only between various military forces (land army, airforces, navy) but also with civil services (police, fire brigade, rescue teams). Unfortunately, as so far, each of these forces uses its own communication means working on different frequencies with different modulations and different data transmission systems.

To carry on any common operation it is necessary to have many radio communication means enabling the communication between various services. To make the co-operation of military and civil services efficient it is necessary to have one sophisticated device realising any type of radio communication.

To meet such requirements RADMOR conducts research and development works over handheld R 3505 radiostation which are based on the software communication architecture concept – the SCA (*Software Communication Architecture*). The 3505 radiostations are so called Software Defined Radio. Their principle idea is based on very fast adjustment to operation in various radio systems by changing exclusively the device software (program) that is without any modification in their physical structure or production process. Such radiostations integrate existing radio communication standards thus permitting the transmission of voice, data, pictures, video, position (GPS) and retransmission of the signal between different military and civil networks. The radiostations are intended for use in the HF/VHF/UHF short range tactical communication for land armies and co-operation with air forces, navy and civil services. By events having the crisis character they can be also used by land, marine and air rescue services as well as by public services which co-ordinate operations by liquidation of threads.

The reception of GPS information on geographical position is possible.

The devices are designed for use in frequency bands from 20 MHz to 520 MHz. It is possible to have analogue (open or masked) and digital (open or enciphered) voice communication and to realise data transmission. The radiostation co-operates with external analogue and digital equipment such as modems or PC computers.

All radiostations described above allow to build new radio communication networks. The modern functions realised by these devices and significantly higher data transmission rates enable efficient management and commandment on the modern battle field. In the future they allow the operation integration of the army and civil rescue and administration services. ■

Special tasks computers

It is not easy to choose the rugged construction computer. This kind of device has to be reliable and meet many different standards. It should be resistant to changeable weather conditions (rain, temperature), adjusted to work in dusty environment and it should also have rugged construction so that any dropping on the concrete surface would not cause serious damage of internal elements or loss of data.

Products which meet all these expectations and even the requirements of the U.S. Armed Forces are Itronix computers – rugged devices designed to work in extreme conditions.

Itronix mobile computers meet even the most severe specifications in the area of resistance to environment conditions. They belong to the group of devices which are classified as fully-rugged, they are in the class IP54 (except hand-held Itronix Q-200, which is in the class IP67) and they meet severe military specifications MIL STD 810 F.

If it comes to resistance mobile devices divide into groups:

- ✔ *Commercial* – the common grade of portable computer, possessing limited durability;
- ✔ *Semi-rugged* – portable computers with rugged armor which protect display, but with no internal protection;
- ✔ *Rugged* – these devices are rugged "by design," meaning they offer internal components and cases engineered from the ground up for harsh use. Rugged computers offer magnesium alloy on structural components; resist vibration, dust, water and temperature extremes; and can take repeated drops onto hard surfaces without failure;
- ✔ *Fully rugged* – the most durable class of ruggedized computers, these fully rugged "by design" devices offer incredible durability for use in the most hostile environments. Fully rugged units offer maximum environmental protection and often come with customized, application-specific features and specifications.

While these four categories provide a broad description of toughness and protection, ruggedization can still vary within each category, depending on individual manufacturers and models. In fact, a number of different ratings and standard tests are typically cited by manufacturers to help establish a computer's degree of ruggedization. Some of the more common include:

- ✔ IP (*Ingress Protection*) – a set of enclosure protection standards governed by the International Electrotechnical Commission (IEC) which help to ensure that device is used in conditions for which it has been designed. The rating is composed of two numbers. The first indicates protection from solid objects; the second refers to protection from water. The bigger is the number, the better protection the device has (*IP54 class is a combination of two meanings; level 5 means dust protection and resistance to infiltration by using a wire or other objects smaller than 1 mm; the only higher existing category is "dust-tight"; class 4 means protection against spraying and splashing water; higher classes – from 5 to 8, indicate protection against water jets and submersion*);
- ✔ MIL STD (*Military Standard*) and MIL SPEC (*Military Specification*), a series of performance and manufacturing guidelines set by the U.S. Armed Forces for military use.

The most important Itronix's implementations

Itronix's solutions successfully work in many special projects in the army, police or border police. Companies and national service choose this equipment because of its high operational reliability in the field conditions. In the situation when every second is important and decisions are made under pressure, it is important to have certainty that everything in the chain of communication functions without failure. Itronix computers turned out to be this hardest link because of high environment conditions resistance (shock, falls, dust) and atmospheric conditions resistance (high and low temperatures, humidity). Because of these factors the risk of damage in unfriendly environment had been minimized. Additionally, choosing these devices enables public services to simultaneously use three different wireless networks (GSM/GPRS/EDGE, WLAN and Bluetooth).

Ultra-rugged laptop computer

In the spring of 2003 the 3rd U.S. Army Infantry Division, taking part in battlefield operations in Iraq, had vested with 2500 laptop computers. Because of difficult weather conditions about 30% of the equipment from twelve different companies had been destroyed. Ubiquitous sand and changes of temperature were disastrous to indoor designed laptops. In consequence of these loses, U.S. Army decided to test all available devices, in order to choose a computer which will be reliable in every conditions. During the test all devices

were tested if they are compatible with MIL STD 810F standard which include:

- ✔ 10-minute test in the water jet under the pressure which matches the pressure from the fire brigades pump;
- ✔ 26 drops from the height of 3 feet onto solid concrete;
- ✔ test in the grain-of-sand-sized particle beam.

All of above tests were successfully completed by Itronix GoBook II. It appeared to be the product which U.S. Army was looking for. Additionally, U.S. Army appreciated high performance of the device, the fact that it operates in three standards of radio communication and favorable guarantee conditions.

– Ruggedized computers built by Itronix have developed a great reputation with our armed forces, both in the field and at the Pentagon. Recent experiences in Afghanistan and Iraq have demonstrated the importance of situational awareness for our forces and the uninterrupted performance of computers in austere environments. Itronix, with its innovative partner Trident Systems, has an opportunity to field solutions that will dominate this growing market – said U.S. Congressman **George Nethercutt**, who serves as vice chairman of the Defense Appropriations Subcommittee in the House.

Equally interesting implementation has been made in the Randolph Air Force Base, the main training base of the U.S. Air Forces, in which among others Polish F-16 pilots were trained. Ruggedized computers were equipped with software which using wireless communication standards in secure military networks, enables easy access to engineering specification of the aircrafts which is essential while servicing and maintaining aircrafts. At the point of maintenance secure WLAN has been built. Itronix computers have been used here as service terminals. The main requirement for such a terminal was its resistance to extreme weather and environment conditions and the possibility to connect with wireless network. The wireless, rugged computers allow aircraft technicians to work more efficiently at the point of maintenance rather than having to rely on tedious, error prone methods of packing up the information and walking from hangar to hangar or flight room to flight room to sort through reams of maintenance manuals and schematics or to manually log maintenance updates and information.

– This technology enables us to cut transit time in half, thus saving the Air Force money. This might not sound like a lot, but when you add up the time of 139 maintenance technicians, it is a lot – said **Rick Peyton**, an avionics technician.

Itronix laptop computers are also used in Federal Way Police Department (FWPD) in Seattle. The city found itself rapidly expanding, and FWPD's old technology just wasn't keeping pace with the department's needs. It was necessary to ensure communication between police units. The important factor which was taken into consideration while choosing the equipment was the fact that computers used in the squad cars has to be shock resistant which are present in vehicles. In this project again, the ITRONICS GoBook II was the best one. – *Officers now have a live connection to our records database. If they stop a suspicious car or need to run a person's name, they can get detailed information very quickly. Before, they'd have to go back to the office to get that additional information, or they'd radio our records department. At the same time it is easier and more effective to create reports at the place of accident* – said **Mehdi Sadri**, information system manager for FWPD.

Itronix rugged tablet

In the 2004 main regattas at Cowes and the Rolex Swan Cup the crew of Spirit of Jethou yacht after their cockpit has been flooded by storm wave used Itronix GoBook Tablet PC to navigation and communication tasks. The previous navigation system has been destroyed by water. From this moment up to the end of regattas Tablet was the main inboard computer enabling reconstruction of navigation system and reestablishing connection.

Rugged handheld

In 2004 after Polish and Lithuanian accession to the European Union, in order do meet new European Union regulations, it was necessary to sharpen control procedures on the border with Kaliningrad. Lithuania State Border Guard Service needed devices which ensure effective communication and rapid means of checking train passengers. Rugged casing, two standards of the radio communication and easy operation caused that the Itronix GoBook Q-100 terminal has been chosen.

Police units using motorcycles very often face problems connected with access to the police databases. The conditions in which they operate and the need of continuous communication forced the Irish police to buy mobile computers. In connection with this it was necessary to choose the rugged device, resistant to weather conditions and vibrations and ensuring radio communication (GPRS/WLAN). The choice was mobile terminal Itronix GoBook Q-100 with PocketPC 2002 system and Traffic Police application.

One of the recent projects in which Itronix solutions are used is the Spanish program Amper, establishing the system enabling monitoring the movements of armies by soldiers or by vehicles without command. Test version of this system named Elcano uses GPS receiver and rugged laptop Itronix connected with dedicated system of geographical information. In this project the usage of every Itronix product is being considered.

Extreme Mobility Show

Because great majority of Itronix solutions is connected with installing devices in cars, product technicians decided to test how they behave in the situation of car accident. To do it Itronix computer was tested by exploding airbag. The film from this experiment shows how big forces influence computer in the moment of bump. Elastic matrix were deformed and closed with big force, but the computer is not destroyed. The film from the test is available from http://www.mobilnosc-extremalna.pl/Itronix_film.wmv.

More information on these products are available from Passus company.

Radosław Dudzic
Product Manager, Passus Sp. z o.o.

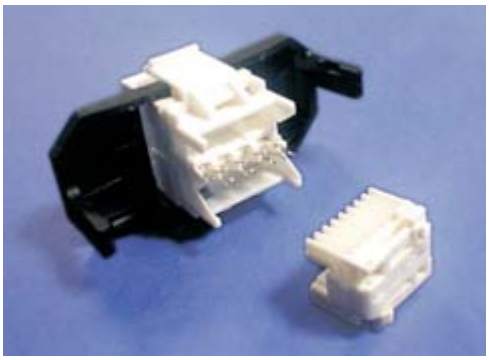
3M Fibre and Copper Structural Cabling Systems

3M is well known in any field of life – is the biggest innovative supplier of solid solutions for copper and fibre optic telecommunication system world-wide. We offer products that deliver innovative copper, test and fibre solutions that help you expand the services of your telecommunications network, including proven product for splicing, connecting, terminating, protecting and testing.

Volition™ Network Solutions include fibre cabling system providing "freedom of choice" in the design and optimalisation of the overall network architecture. Fibre optic cable is the ultimate transmission medium for secure networks. It also includes a state of the art voice and data copper cabling system, including a Category 6 offering and giving "significant channel performance headroom" over existing standards and helping a broad range of customers to migrate to high bandwidth.

A variety of easy to install and innovative connectivity solutions insuring high performance, and reliable systems form part of the offer. The revolutionary VF-45™ small form factor fibre connector has helped in reducing the complexity of the fibre networking, while the 3M RJ45 copper products offer simple termination solutions – jacks snap on without tools – with built-in reliability features and component performance exceeding existing standards. All 8 copper conductors are effortlessly terminated in one simple operation resulting in reliable interconnection in record time. New Category 6 Jack has keystone mounting format. With its compact size, integral shutter, and tool less termination, the K6 Jack from 3M ensures smart, reliable and quick installation. If a wiring mistake is made you can re-use your K6 Jack several times. Three formats are offered: UTP, FTP, STP. 3M products work to solve your problems and meet your needs. 3M Volition Category 5e and 6 copper cabling systems comprise patch panels, patch cords, jacks, cables and faceplates that offer maximum performance at an economic cost.

VF-45™ plug and socket, new standard – compact size connection



Cat. 6 cabling – K6 (Keystone mounting)

The system features the breakthrough Volition™ VF-45™ connector, which is rapidly becoming the standard in fibre to-the-deskop networking. Having the same look, feel and footprint as the familiar RJ45 copper connector and twice the port density of traditional fibre connectors the VF-45™ multimode and singlemode duplex connectors feature unsurpassed ease of termination, reliability and performance. For enhanced levels of security, a keyed version is available to physically control access to classified networks. The VF-45™ connector is standardized by TIA/EIA – 604-7, FOCIS-7 and PN-EN 61754-19.

Also in Poland there was made a lot of military installation for example for Polish Navy, Border Guard Headqauter and several banks.

As well as Volition™ Network Solutions, 3M offers a complete line of singlemode & multimode ferruled fibre optic connectors including Hot Melt in ST, SC and LC style. To completed this, connectors are also available terminated as pigtails or patch cords in a variety of lengths. The plugs are factory pre-filled with special Hot Melt adhesive which ensures,

Hot Melt ST Connector

Hot Melt optical fibre connector assembly system

in combination with an oven, a fast and reliable assembly solution. All connector types are equipped with high-precision ceramic ferules. Different boot colours are available to guarantee identifiable channel separation. Hot Melt can be use in LAN building wiring, to expand existing networks in conformance with national and national and international standards bodies TIA/EIA – 568, ISO/IEC 11801 and EN 50173. The Fibrlok™ is a mechanical splice, available for single & multimode fibres, which can used wherever quick and secure splice connectors are required. This connector is a universal splice for both 250 to 900 µm coated fibres.

Fibrlok™ mechanical splice

The most important advantages of our system which are key issue in military telecommunication networks are:

- ✔ interference resistance (EMI/EFI),
- ✔ data security (hard to tap),
- ✔ simple installation and servicing,
- ✔ mechanical socket coding.

3M is proud of big installations for example in the Regional Headqauter of NATO Briunssumin (Netherlands), NAVY and AIR-force, Military Land-force, Ministry of defence in Finland, Ministry of

NATO Headquarters – Brussels, Belgium

Defence in Czech Republic, NATO Italy's head-quarter in Naples and Latina, NATO Headquarters in Brussels (Belgium), NATO sites in Italy, UK military (top secret networks).

3M Poland Sp. z o.o.
Al. Katowicka 117, 05-830 Nadarzyn
phone (22) 739 60 00, fax (22) 739 60 03

Beata Sałyga
phone (22) 739 61 00 or 0-600 27 80 19
e-mail: bsalyga@mmm.com

Please visit our websites:
http://www.3M.pl
http://www.3mtelecommunications.com

Contingency planning evolution for strategic telecom and IT systems

MGE UPS SYSTEMS

The key to disaster recovery and business continuity today is operational resilience. As the relentless application of technology continues we must attempt to create an arena in which we can protect these technological advancements. Our reliance on 24/7/365 Telecom and IT availability means that the success of any Disaster Recovery Centre is measured in milliseconds.

Many Disaster Recovery Centre customers come from the sectors, where even the shortest power failure is not accapteble. Events of 9/11 have focused the minds of the financial services regulators to ensure that all major institutions have suitable contingency plans in operation. In some major countries, especially the USA, CEOs are legally responsible for protecting their organisation's data. Companies that lose their data, for whatever reason, go into liquidation within 14 months of the loss, so the ability to recover data is vital.

However, the key to disaster recovery is not just redundancy; the resilience of the system or the networks is critical. Resilience must be applied to technology at the design stage to ensure continuity even during a cataclysmic event, which may be natural disasters, software problems, cyber terrorism or latent design defects in the electrical support systems of the data centre.

Fault tolerance

Most of new multiple data recovery centres are now being built far away from main data-processing hubs. According to the SwissRE study, over 50 per cent of disasters are weather-related but terrorism is getting expensive too. In view of this, infrastructure and electrical system design needs to be fault-tolerant. For example, a short circuit should not stop the functionality of the whole building. A malfunction such as that should clear itself because of its fault tolerant design which is part of the operational resilience. Since UPSs are at heart of any data centre, a high degree of attention must be paid to resilience in UPS system design.

We are all aware of recent blackouts in London, New York, Toronto, Warsaw, Copenhagen and Rome. There were different reasons for each blackout - human error, shortage of electricity, deregulation, and so on. In Europe, electricity utilities can just about meet 99.9 per cent, (i.e. 999) of availability. Percentage Availability is measured as a ratio of Meantime to repair

Meantime To Repair (MTTR) and Meantime Between Failure (MTBF), i.e. Availability = (1-MTTR/MTBF) x100. MTBF can be increased by means of enhanced equipment reliability and using products that are independently certified by recognised bodies e.g. TUV, KEMA and Veritas. It is important to make sure that both the equipment and the installation as a whole shall be fault tolerant. In view of this, following factory witness tests it is imperative to carry out system integrity (SI) testing that includes all the key components of the Data Centre prior to hand over to client. During the SI testing one needs to simulate faults at various levels within the electrical circuits and the mechanical items within the Data Centre. This type of simulated testing can prove the robustness of the system design, equipment and the installation. SI testing would bring to the fore any issues related to non-compatibility between different packages or equipment.

Protection

MTTR can be reduced by use of remote on-line diagnostics and use of skilled experts carrying out repairs within short space of time. Correct range of spares need to be available on 24/7 basis. Normal utility availability of 99.9 % can result in 9 hours of blackout or several short blackouts and some brown outs. As the utility companies are not required to guarantee continuity, organisations also have to protect themselves against these power losses.

Certainly, no “startegic” institution can accept this poor level of availability, so it is essential, therefore, to have data centres backed up with UPS systems and standby generation to protect their core Telecom and IT infrastructure

In order to achieve a high level of resilience with a UPS system, units which comply with dual conversion design as per IEC 62040 must be used. In other words, critical IT load is protected against any power quality issues at the input of the UPS whether it is voltage or frequency related. It is important to note that some of the rotary UPSs, and a small percentage of static UPS may not be of dual conversion design.

Static type UPS

Static type UPSs utilise battery banks to provide adequate back up time to provide cover during Mains loss or poor quality from the utility supply. This allows enough time for the stand-by generators to fire up and support the UPSs. For the large Data Centres it is worth using ten year design life batteries in accordance with BS6290 Part 4 1997 standard. It is also necessary to install a battery monitoring system that is based on Impedance-check technology. However it is very likely that in few years time the battery banks will be replaced with Fuel Cell technology.

Battery autonomy can be based on requirements set by the client, but 10-30 minutes is the common figure used in this type of industry. Standby generation is also essential to cover for long outages and also to support non-essential loads, for example, air conditioning, lighting, and so on.

It is good practice to have n+1 redundancy even at the standby generation level, whereas it is critical for UPSs to go with n+n redundant design. (Ifn is the minimum requirement to support the critical load, for example, 2x500 kva UPSs, then n+1 redundancy would mean 3x500 kva UPSs and n+n would mean 4x500 kva UPS.) It is important to utilise an external centralised static by-pass (CSB) per each parallel redundant UPS system. CSB provides a very high degree of resilience when compared to simple modular parallel UPS systems. The reason being that CSB static switch is rated for the system load whilst the modular type UPS system depends on static switch that is rated only for the individual module rating i.e typically only 20 per cent of the load.

Blade servers

Since the growth of Blade servers it is good to have generator sets that have excellent compatibility with leading power factor imposed by Blade servers. This will provide added resilience in the event of the entire UPS system going into bypass mode during a mains loss situation. Since most of the IT loads generate harmonics it is good practice to limit propagation of such pollution by using Active Harmonic Filters. This helps to reduce the size of the neutral conductor, i.e., saves copper cost and eliminates fire risk and nuisance tripping of circuit breakers. UPSs need to be provided with suitable active harmonic filters to ensure that the current distortion (THDI) level is held at 5% or lower, regardless of loading on the UPS system. This would help to meet the anti-pollution recommendation G5/4.

In order to limit the damage caused due to a faulty source the static load transfer switches (STS) need to be used at power distribution unit (PDU) level so that any fault is limited to that part of the circuit and system resilience is not affected. These STS units are very fast acting (2-10 millisecond switching time) hence they can switch the critical load from one source to the other without jeopardising functionality of the servers.

In-built design

Each UPS system needs to have built-in redundancy and resilience at the design stage. Once the design is checked for any dormant or hidden points of failure, it is good practice to carry out factory witness tests for each individual item, i.e., UPS systems, switch gear, standby generator sets and so on. Even during factory witness testing it is good practice to simulate short circuit on the load side to help measure the fault tolerance level of the UPS system and its components. Also evaluate 100 per cent load step performance of the UPS system and standby generators. It is recommended that suitable critical component monitoring systems such as UPS battery banks monitoring are deployed, as this type of monitoring would help the Facilities Management team to take proactive steps necessary to avoid an internal disaster in a Data Recovery Centre.

Before closing, there is no substitute for planned and regular maintenance which should also include thermal imaging of critical components, for example, UPS, batteries during discharge, PDUs and switch gear.

ZPAS SA telecom enclosures for the operational service

Electronic communication these days is a way in which a modern society exchanges information. This new way of passing data and news is a result of mass culture and the process of global standardisation. Electronic communication is not an attribute of a society but it's rather an element of an economy based on knowledge and science. It is worth mentioning that the use of electronic communication exceeds industry and economy and goes further to other aspects of life such as culture and areas in which a community exchanges information.

Thinking about electronic communication we come across a problem of a clear definition. One may say there are two ways through which we understand, describe and interpret electronic communication. The first way is a method of exchanging information, mainly in a form of an electronic document. A characteristic of such electronic exchange of information is user's share in the process of communication. The second understanding of the notion lets us consider a communication based on IT technology as electronic communication. In this case it is a most significant goal to safeguard this exchange of information taking advantages of the latest technological achievements. From the point of view of the manufacturer of telecom enclosures it is one of the most important tasks to present a customer with a product of highest quality that will be used as the technical back-up of communication network systems of the operational services.

ZPAS data and telecom enclosures – EMC protected SZBk cabinets

The advent of technological progress, computerisation of police, army and emergency units was the time when ZPAS SA started providing the military with its products, mainly telecom cabinets and structured wiring.

Data cabinets SZB, server cabinets SZB SE, and collocation cabinets DSR, all of them designed for installation of 19" and 21" appliances, are the ones that have a broad application in the military sector. Equally popular with the army are wall boxes with 19" frame, known as SD, SJ, SU. In specific cases 10" SKI wall boxes, used for LAN network installations, are of useful service to the military.

Apart from the mentioned items there is a specific ZPAS product that serves the needs of the armed forces. This is the SZBk cabinet manufactured according to EMC requirements. This kind of enclosure is meant to be installed in rooms along with electromagnetic waves emitting appliances. Two of Polish Institutes, The Wrocław Institute of Telecommunication and Acoustics as well as Warsaw based National Internal Security Agency, confirmed in their independent testing the effective EMC protection in ZPAS SZBk cabinet. An extra guarantee of adherence to quality and technical specifications are ISO 9001 and ISO 14001 certificates that ZPAS SA has been holding for years.

Krzysztof Karwowski
ZPAS SA
kk@zpas.pl

ZPAS-NET products

ZPAS-NET Sp. z o.o. product offer is addressed mainly to IT, energy, central heating and other industry sectors. ZPAS-NET has also implemented several solutions for border guard, border protection military units, fire department, police and prison guards. In 2003 during the Logispol 2003 Fairs, ZPAS-NET has been awarded with the Cup of Pomeranian Military District Commander for "Command Desktop".

ZPAS-NET offer includes products like:

- ✔ elements of structural wiring and telecommunication equipment,
- ✔ outdoor access enclosures,
- ✔ enclosures and NN switches with electrical equipment,
- ✔ dispatcher and steering desktops,
- ✔ synoptic mosaic tables,
- ✔ distributed remote control system ZPAS Control Oversee.

ZPAS-NET solutions enable connection of IT and energy products into one, using the most advanced technology present. All these solutions also provide ability to optimize infrastructure development, helping in electronic communication of energy sector. Unquestionably one of the most important types of all IT solutions are: equipment monitoring tools, and climate control systems. Managing and access control of service personnel for the IT equipment gained whole new meaning in narrow specialization era. The way, security and safety of transmitting and archiving of information are nowadays the most important criteria determining value of IT systems. Innovation, as the way of searching and implementing new technological solutions, is one of the most important factors of competitiveness at global market.

ZPAS Control Oversee distributed remote control system

The system is a complex solution enabling cost effective and reliable remote control network with measurement and management functions. System is scalable and fully independent – works on any hardware, database and software platform. It's architecture enables easy expanding it's possibilities with new equipment detection, new communication technologies, and new visualization elements.

One of the most important parts of the system is a software component used for designing operator panels, with visualization actual and past states, remote control, and configuration of local automation units.

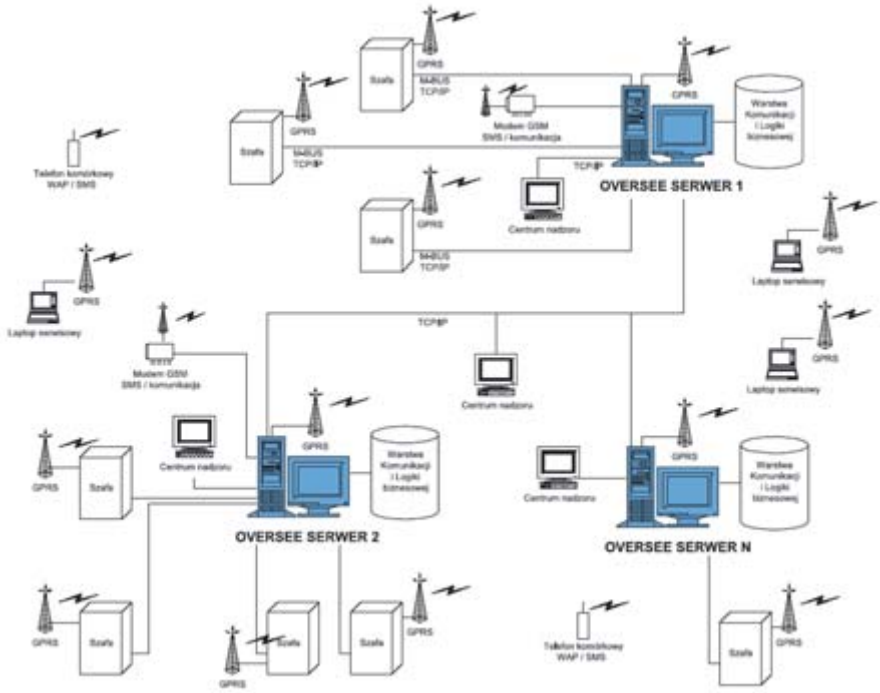
Central part of the system is distributed control network based on modern software technologies, i.e. J2EE and JMX. This part contains 3 layers: communication, business logic and presentation.

The communication layer has a module structure, where particular modules designed for specific operating system and equipment are managing communication between the hardware and business logic layer. Connecting new equipment requires design of a specific communication module, dedicated to this equipment, but it does not require any changes in business logic and presentation layers. Basic task of business logic layer is to manage data gathered by communication layer, process it, optimize and send to the presentation layer, as well as steering the equipment of communication layer with commands from presentation layer. Very important part of this layer, from the view of system security, provide mechanisms of replication and data archiving, access and privileges control, registering and exception event service.

Presentation layer enables client applications, Internet browsers and mobile equipment (PDAs, mobile phones) to use data provided by business logic layer. It is possible to access object information, no matter where it is, from any allowed location. System archives information on objects and provides mechanisms to review them. Multiserver architecture and connection optimization processes provide fast and reliable system, able to work even during computer hardware failure or power supply failure. ZPAS Control Oversee system has been awarded with a Cup of XVI International Communication Fairs 2005 for the best polish product of exhibition.

Control, steering and management equipment system with fully programmable driver

ZPAS Control Oversee System is a digital automation system provides possibility to build effective, cheap and reliable measurement and management networks. It is designed for professional integrated building and industrial sites management systems. It is excellent in handling heating and air condition systems, producing and



distributing water, gas and electricity systems and in access control and alerting systems.

Use of standard M-Bus interface between central unit and customized object modules enabled to create a distributed architecture with simple scalability system.

M-Bus as international standard of transmitting data from billing equipment provides possibility of gathering information with ease by cost effective interfaces, from any type and structure of network. Ease of building the network and possibility to power it's elements with the network itself significantly reduces costs of the network.

In the software layer, system offers unique way of archiving data that creates object distributed database. Each central unit with sufficient memory stores all the data. Then with the use of simple and cost effective visualization system the data is presented to users and saved on a hard drive of operator's computer. Additionally the system works with any SCADA visualization packages.

Simple, fast and cost effective casing of the system elements is possible with the use of standard enclosures for electric equipment of low voltage.

Climate control and measurement network system based on 1-Wire

ZPAS-NET decided to implement new solution based on 1-Wire technology, because of it's flexibility. To build 1-Wire network you need only to connect sensor with transducer and add a signal wire. In a minimum version it is a single 2-wire cable to provide power and data transmission. It is possible to connect many object in a slave mode to one master bus interface. Every slave object has a unique 64-bit address which can be easily found even in a large network. 1-Wire type component network can be attached with a single communication interface directly to a PC or a driver. It is possible to build even large and complicated networks in this technology without any network concentrators. If there is a necessity of dividing the network into subnets, there are 1-Wire hubs to help. Due to wide range of components, it's accessibility and low price, the 1-Wire technology is often used in server room, telecommunication enclosures monitoring as well as in building an intelligent building. The most important advantages of this technology is reliability and ability to work in co-operation with ZPAS Control Oversee System.

Supplementation to 1-Wire network is an interface to connect it to ZPAS Control Oversee distributed system. It helps to monitor the conditions in even very large networks with a cost effective solutions.

Roman Głaz
ZPAS-NET sp. z o.o.

PKI – cure to all evil or information security

The continuous development of the IT leads to revolutionary changes in the use of information. E-document is becoming more and more common and replaces its paper predecessor all the way long from recording the information, sending and receiving through archiving and storing for a long time. The increasing number of documents being electronically processed and their transmission over public and dedicated connections results in the growth of e-crime. Recently, users have experienced the significantly higher number of attempts to hack at information systems and steal data. Unfortunately, such attempts happen to be successful and one of Polish banks lost around one million Polish zloties in this way. Consequences of such a loss does not only affect economic issues, but social ones as well – they may as well undermine bank's trustworthiness or even result in the bankruptcy.

On the other hand, how can you estimate the value of the data stolen from systems operated by the police, army, border guard or other so called uniformed forces?

Attempts to steal the information from the above systems are undoubtedly connected with espionage or terrorist actions, and their consequences are more political than economic or social only. It is therefore extremely important to apply tools relevant to potential hazards that provide the highest security for the processed data.

The public key infrastructure – PKI is a special feature among solutions that provide the data security. The PKI-based systems combine document protection (e-signature, encryption), room access control (authorization management and authorization application monitoring) and validation and authentication systems (applications, databases, servers).

Unizeto Technologies SA is an outstanding supplier of complete PKI solutions. The co-operation of the company with partners and customers may cover such areas as IT system security audits, supply of hardware and software, implementation, integration and service on standard or dedicated solutions and training schemes.

In cases where economic aspects matter and security requirements allow for – systems can work on Unizeto servers (outsourcing) or dedicated solutions be developed by a customer with Unizeto support.

Take advantage of 40-year market experience, 10 years of activities in the field of encryption technologies, 7-year experience of providing e-signature related certification services and more than 200 highly qualified staff at your disposal. Moreover, the successful completion of a number of largest PKI projects in Poland, references given by satisfied customers (incl. the so called uniformed forces) make Unizeto Technologies SA a trustworthy partner.

Unizeto Technologies offers three main groups of software solutions:

- ✔ server software,
- ✔ customized applications,
- ✔ programming tools for implementing PKI functionality in other systems.

All procedures regarding processes that take place within Unizeto Technologies comply with ISO 9001:2000 and AQAP 2110. The company has been audited to check for the compliance with WebTrust criteria for certification authorities providing e-signature and time stamp related services.

Licenses:

- ✔ license granted by the Ministry of Interior and Administration for manufacture of and trade in products and technologies of military or police use,
- ✔ license for economic activities in the field of property security in form of technical protection.

Since December 2004 Unizeto Technologies SA has had a NCAGE – NATO Commercial and Government Entity Code)

Jacek Wojtala
Deputy Director
Uniformem Services
Unizeto Technologies SA
www.unizeto.pl; www.certum.pl

www.unizeto.pl

UNIZETO TECHNOLOGIES SA

Producer and integrator of IT solutions

E-signature and Access Control

Unizeto Technologies SA

- producer, supplier and integrator of systems to develop public key infrastructure and applications to support use of e-signature

CERTUM
General Certification Authority

- qualified certificates
- non-qualified certificates
- time stamping

Access Control Systems

using cryptographic smart cards

- single logging on information systems
- for work stations
- for rooms
- Working Time Registration systems

Unizeto Technologies SA is licensed by the Ministry of Interior and Administration:
- for manufacture of and trade in products and technologies of military or police use,
- for economic activities in the field of property security in form of technical protection.

www.certum.pl

UNIZETO CERTUM

POWSZECHNE CENTRUM CERTYFIKACJI