

## **System monitorowania obiektów po sieciach LAN/WAN**

### **PALLADION**

System Palladion to nowoczesny system monitorowania obiektów oparty o transmisję danych wykorzystującą infrastrukturę teleinformatyczną Banku (sieć LAN/WAN z protokołem IP v.4), z zapasowym torem transmisji po sieci GSM/GPRS.

Głównym zadaniem systemu jest monitoring lokalnych systemów alarmowych (LSA) podłączonych do systemu poprzez interfejs nadawczy IPS i ich wizualizacja na Terminalach alarmowych. IPSy podłączane są do LSA poprzez 24-wejście równoległe lub RS-232. IPSy komunikują się z serwerem systemu z wykorzystaniem protokołu UDP/IP (Ethernet lub RS-232 z protokołem PPP) przesyłając do niego wszystkie sygnały otrzymane z LSA oraz informacje swoim stanie, w tym stan zasilania i baterii, stanu łącza podstawowego i zapasowego oraz stanie wejść i wyjść równoległych. Serwer otrzymane informacje przetwarza według zdefiniowanych reguł, zapisuje do historii, ustala stany monitorowanych obiektów i przesyła (protokół TCP/IP) w formie zdarzeń na wskazane terminale do obsługi.

Sercem systemu jest serwer pracujący z bazą danych MS SQL, Oracle, DB2.

W systemie przewidziano działanie dwóch równoległe pracujących i współpracujących ze sobą serwerów podstawowego i zapasowego. Normalnie IPS komunikuje się z serwerem podstawowy, lecz w momencie wykrycia jego awarii automatycznie przełącza się na serwer zapasowy. Po powrocie do normalnej pracy serwera podstawowego komunikacja z IPsem przełączana jest z powrotem na ten serwer. Niezależnie od dwóch serwerów IPS obsługuje dwa tory transmisji podstawowy i zapasowy. Torem podstawowy jest łącze Ethernet (UDP/IP) lub zamiennie RS-232 (UDP/IP/PPP), torem zapasowym jest GSM/GPRS. W przypadku awarii toru podstawowego transmisja jest przełączana na tor zapasowy do czasu powrotu łączności poprzez tor podstawowy. Niezależnie od powyższego możliwa jest transmisja tylko jednym z tych torów, tylko podstawowym lub tylko zapasowym. Dla każdego z torów ustala się niezależnie czas kontroli łącza.

Cała transmisja pomiędzy IPsem a serwerem jest zabezpieczona z wykorzystaniem szyfrowania algorytmem DES. Natomiast transmisja pomiędzy serwerem system a terminalami z wykorzystaniem VPN (Virtual Private Network - Wirtualna Sieć Prywatna).

**Interfejs nadawczy IPS** jest to dedykowane urządzenie wykonane na bazie procesora serii MSC51 zawierającego m.in. wewnętrzną pamięć Flash i RAM (zamiast stosowanej zwyczajowo w innych urządzeniach pamięci zewnętrznej) oraz funkcję IAP (In Application Programming) z dodatkową pamięcią Flash o rozmiarze 32 kB, umożliwiającą zdalną aktualizację oprogramowania poprzez sieć IP (Ethernet lub RS-232).

Sterownik IPS wyposażony jest w:

- 24 równoległe wejścia zabezpieczone transoptorowo, z definiowanym indywidualnie dla każdego wejścia trybem pracy (monostabilny / bistabilny) i kodami zdarzeń,
- 8 wyjść sterujących przekaźnikowych,
- standardowe łącze Ethernet (RJ45) z protokołem IP v.4,
- standardowe łącze RS-232 z protokołem PPP/IP v.4,
- 3 dodatkowe łącza RS-232 z przeznaczeniem m.in. do:
  - lokalnego konfigurowania nadajnika,
  - monitorowania stanu urządzeń UPS (przy dostarczeniu przez klienta specyfikacji protokołów komunikacyjnych z tymi urządzeniami),
  - innych zastosowań,
- 1 port RS-485 z przeznaczeniem do komunikacji z urządzeniami i systemami zewnętrznymi,
- 2 wejścia analogowe od 0 do 10V,
- modem GPRS,
- złącze rozszerzeń – pod przyszłe zewnętrzne moduły i urządzenia.

Urządzenie stanowi samodzielną jednostkę, w której skład wchodzi: sterownik, modem GPRS wraz z anteną, zasilacz i akumulator. Nadajnik i zasilacz umieszczone są w jednej wspólnej, zabezpieczonej antysabotażowo obudowie, wykonanej z blachy stalowej, zgodnie z technologią obudów central alarmowych.

Urządzenie zasilane jest zewnętrznym prądem zmiennym 230V / 50Hz oraz posiada przyłącze akumulatora zasilania rezerwowego zapewniającego podtrzymanie zasilania na okres 24 - 72 godzin (zależnie od zastosowanego akumulatora i trybu pracy urządzenia).

Bezpieczeństwo przesyłanych danych pomiędzy Serwerem a IPsem jest zapewnione poprzez zastosowanie szyfrowania tych że danych algorytmem DES z automatyczną wymianą kluczy kryptograficznych sesji.

**Serwer systemu** stanowi komputer klasy serwerowej z zainstalowanym systemem operacyjnym MS Windows 2000 lub 2003 Serwer oraz oprogramowaniem serwera systemu Palladion firmy STEKOP. Serwer bazy danych w typowym rozwiązaniu jest to

MS SQL 2000 Serwer instalowany na tym samym komputerze co oprogramowanie systemu Palladion, jak również instalowany może być na oddzielnym serwerze pracującym na bazie systemu operacyjnego MS Windows 2000/2003 Serwer lub UNIX i jemu pochodne.

Główną rolą serwera jest odbiór, po sieci IP, wszystkich zdarzeń z IPSów i przesłanie, również po sieci IP, wybranych zdarzeń (np. alarmowych i/lub technicznych) do odpowiednich Terminali w celu obsługi przez wyznaczone do tego służby. Do zadań serwer należy również kontrola łączności z IPSami i Terminalami, kontrola załączeń i wyłączeń LSA, rejestracja komunikacji z IPSami i terminalami, rejestracja operacji wykonywanych przez operatorów terminali.

Serwer został zaprojektowany po kątem wysokiej jego stabilności z wykorzystaniem takich mechanizmów jak usługi systemowe MS Windows i wątki. Dostęp do bazy danych realizowany jest z wykorzystaniem technologii ODBC.

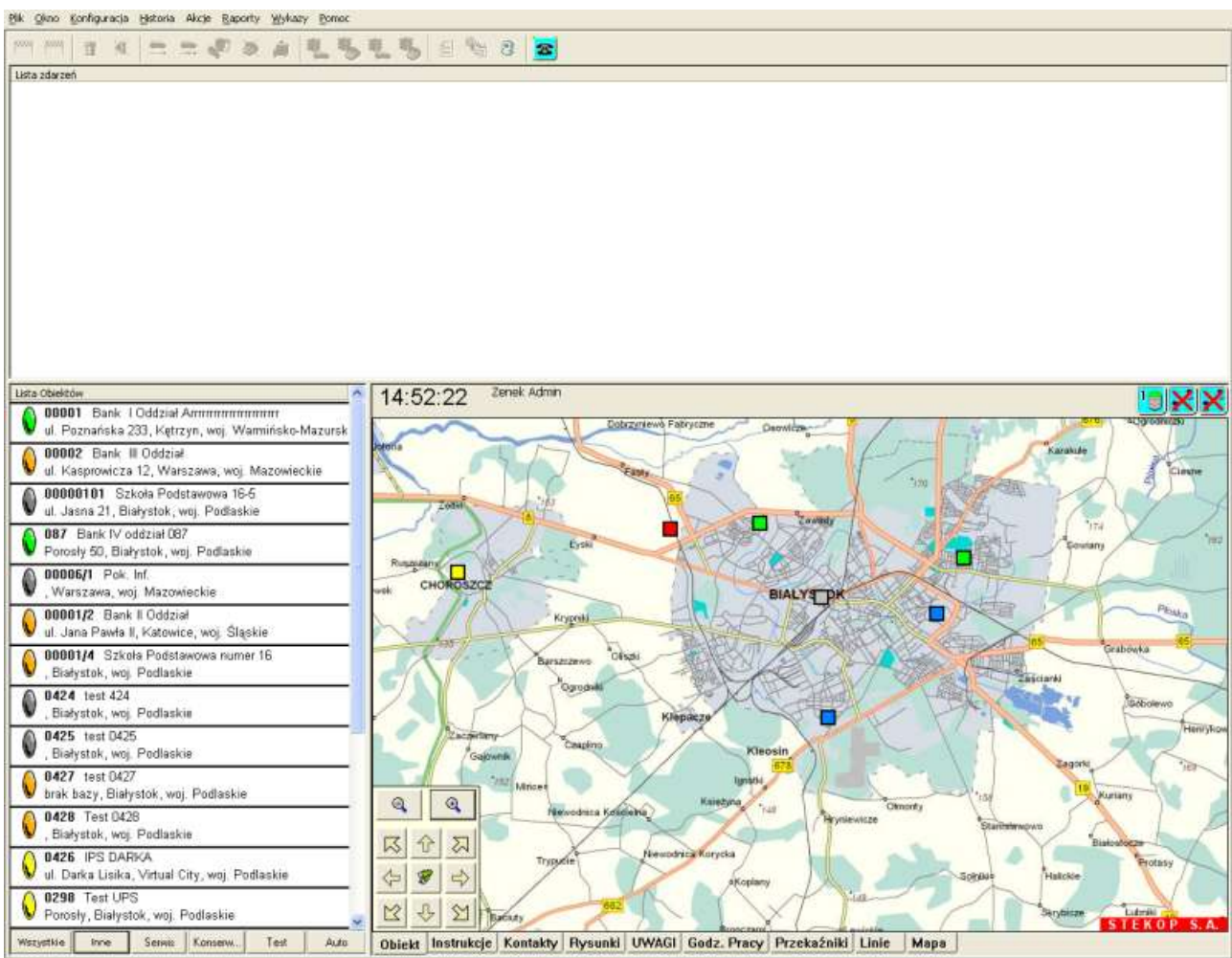
**Terminal alarmowy** stanowi komputer klasy PC z zainstalowanym systemem operacyjnym MS Windows 2000/XP Professional i oprogramowaniem Terminala systemu Palladion.

Główną rolą Terminala alarmowego jest prezentacja, w sposób czytelny i prosty (różne typy zdarzeń oznaczane są dodatkowo oddzielnymi kolorami definiowanymi w systemie), otrzymywanych od serwera systemu zgłoszeń wraz ze wszystkimi niezbędnymi danymi do obsługi tegoż zdarzenia przez operatora oraz wspomaganie pracy operatora poprzez automatyzację często powtarzanych czynności tj. wybieranie numeru telefonu do obiektu. Na terminalu przeprowadzana jest rejestracja rozmów telefonicznych operatora – zarówno wychodzących jaki i przychodzących. Rozmowy prowadzone są przez zestaw słuchawkowy z mikrofonem.

Operator w celu rozpoczęcia pracy musi wykonać procedurę logowania do systemu poprzez podanie nazwy użytkownika i odpowiedniego mu hasła. Wszystkie czynności wykonane przez operatora, tj. przeprowadzone rozmowy wraz z rej. treści rozmowy, skasowanie zdarzenia i inne, rejestrowane są w historii zdarzeń systemu.

System umożliwia definiowanie własnych szablonów raportów i zestawień, które można wyświetlać i drukować operator z poziomu Terminala po wcześniejszym nadaniu mu odpowiednich uprawnień.

Położenie obiektów stałych (budynków) jak i ruchomych (pojazdy i ludzie) prezentowane jest na mapach cyfrowych za pomocą definiowalnych symboli graficznych przedstawiających stan monitorowanego obiektu (alarm, uszkodzenie, stan łączności, załączenie, wyłączenie i inne) oraz jego typ (bank, muzeum, hurtownia, sklep i inne zdefiniowane przez użytkownika typy).



Rys. 1. Okno główne aplikacji Terminala alarmowego

Terminal działa jako element systemu typu Command&Control pozwalający w sposób zcentralizowany i przejrzysty kontrolować i kierować poczynaniami podległych służb. Możliwe to jest poprzez połączenie funkcjonalności następujących elementów systemu w jeden spójny system:

1. Mapy cyfrowe – prezentacja stanu i położenia zarówno chronionych obiektów jak również pojazdów i ludzi (system lokalizacji GPS) w kontekście prezentowanego zdarzenia alarmowego.
2. Komunikacja telefoniczna, fax i SMS z podległymi służbami ochrony na obiekcie oraz załogami interwencyjnymi pozwalająca na koordynację i wspólne ich działanie.
3. Powiadamianie poprzez fax, SMS i/lub pocztę elektroniczną służb tj. Policja, Straż Pożarna i inne.
4. Zdalny dostęp do systemu CCTV obiektu w celu weryfikacji wizyjnej bieżącego stanu zagrożonych obszarów monitorowanego obiektu. Podgląd bieżącego obrazu z kamer oraz dostęp do archiwalnych nagrań.

5. Zintegrowane środowisko prezentacji zdarzeń (lista zdarzeń), bieżącego stanu obiektu (wykaz obiektów, ikony na mapach cyfrowych), danych niezbędnych do obsługi tj. kontakty (dane osoby i numer telefonu), instrukcje postępowania, rysunki obiektu.
6. Łatwo dostępne funkcje komunikacji (telefon, fax, SMS i poczta elektroniczna) ze służbami lokalnymi na obiekcie i załogami interwencyjnymi oraz innymi służbami tj. Policja, Straż pożarna i inne w kontekście obsługiwanego zdarzenia.

Bezpieczeństwo przesyłanych danych pomiędzy Serwerem a Terminalem jest zapewnione poprzez zastosowanie protokołu VPN.

**Terminal administracyjny** stanowi komputer klasy PC z zainstalowanym systemem operacyjnym MS Windows 2000/XP Professional i oprogramowaniem Terminala systemu Palladion.

Główną rolą Terminala administracyjnego konfiguracja zdalna i lokalna oraz administracja poszczególnymi elementami systemu, tj. nadajnik IPS, terminal alarmowy i serwer systemu. Posiada on również funkcjonalność terminala alarmowego dzięki czemu możliwa jest na nim obsługa zgłoszeń technicznych tj. awarie i uszkodzenia.

Bezpieczeństwo przesyłanych danych pomiędzy Serwerem a Terminalem jest zapewnione poprzez zastosowanie protokołu VPN.

**Dedykowane terminale** monitorujące stan innych podsystemów zintegrowanych z systemem Palladion, np. podsystem monitorowania stanu pracy urządzeń UPS.

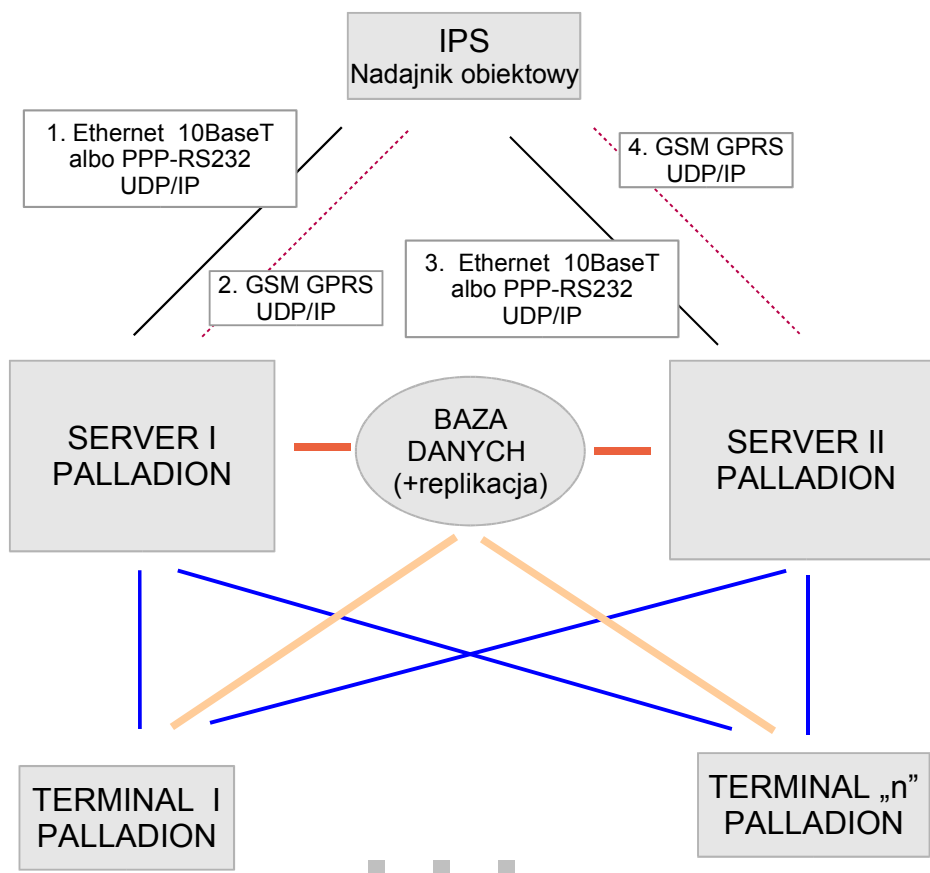
Bezpieczeństwo przesyłanych danych pomiędzy Serwerem a Terminalem jest zapewnione poprzez zastosowanie protokołu VPN.

## Najważniejsze realizacje

1. System monitorowania bezpieczeństwa obiektów oraz stanu pracy zasilania rezerwowego w ING Bank Śląski S.A. (ok. 400 obiektów)
2. System monitorowania bezpieczeństwa obiektów w Kredyt Bank S.A. (ok. 400 obiektów)

## Schemat A

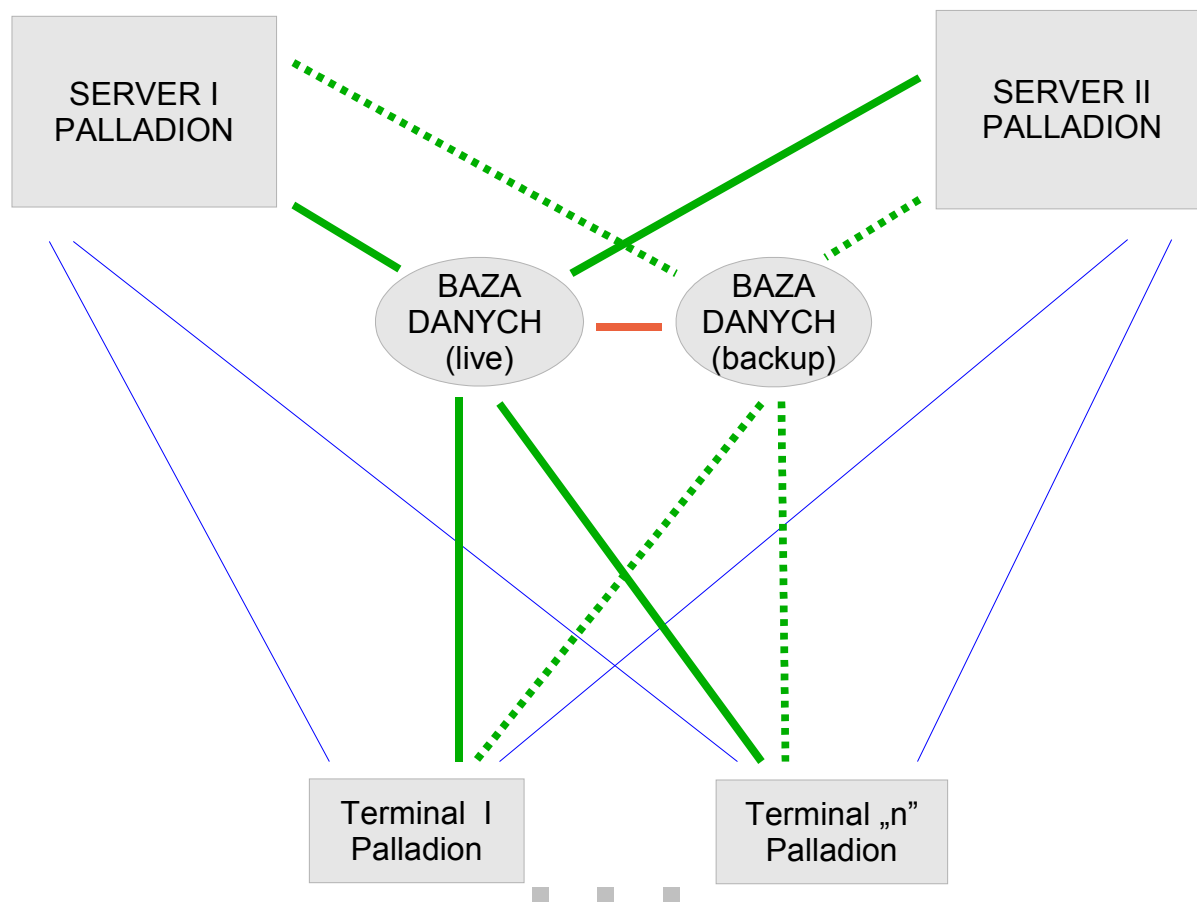
### Ogólny schemat połączeń sieciowych systemu PALLADION







- Połączenie VPN Terminal Palladion <-> Serwer Palladion (wszystkie stanowiska terminali Palladion powinny mieć zestawione połączenie VPN z dwoma serwerami Palladion)
- Połączenie Terminal Palladion <-> Baza danych (np. z wykorzystaniem mechanizmu mocnego szyfrowania danych dostarczonego przez sterowniki ODBC SQL Server)
- Połączenie Serwer Palladion <-> Baza danych (np. z wykorzystaniem mechanizmu mocnego szyfrowania danych dostarczonego przez sterowniki ODBC SQL Server)
- Połączenie Serwer Palladion <-> Urządzenie końcowe IPS – tor podstawowy, szyfrowanie DES
- Połączenie Serwer Palladion <-> Urządzenie końcowe IPS – tor zapasowy, szyfrowanie DES

## Schemat B

### Połączenia sieciowe systemu PALLADION z bazą danych (przykład połączenia z bazą MS SQL)



-  Połączenie (opcja VPN) Terminal Palladion <-> Serwer Palladion (wszystkie stanowiska terminali Palladion z dwoma serwerami Palladion) protokół TCP/IP porty 4096...4115.
-  Replikacja baz danych.
-  Połączenie Baza danych <-> Terminale / Serwer Palladion protokół TCP /IP port: 2937 (domyślny port SQLServer)
-  Połączenie Baza danych <-> Terminale / Serwer Palladion protokół TCP /IP port: 2937 (domyślny port SQLServer)  
Połączenie jest zestawiane tylko w przypadku gdy jest nie dostępna podstawowa baza danych.