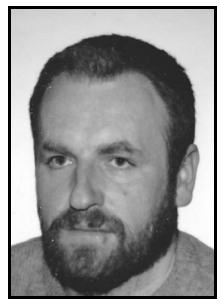
Leszek MAZUR [1], **Michał PORZEZIŃSKI** [2]
[1] DGT Sp. z o.o., ul. Młyńska 7, 83-010 Straszyn
[2] POLITECHNIKA GDAŃSKA, WYDZIAŁ ELEKTROTECHNIKI I AUTOMATYKI, ul. Narutowicza 11/12, 80-233 Gdańsk

Rozproszony system zdalnego nadzoru urządzeń telekomunikacyjnych

Mgr inż. Leszek MAZUR

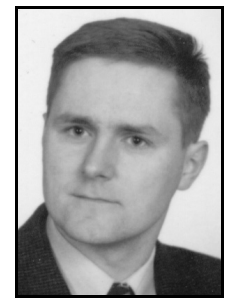
Studiował elektronikę na Politechnice Gdańskiej i uzyskał tytuł magistra inżyniera elektroniki w 1989 roku. W latach 1986-1991 pracował w Instytucie Elektrotechniki, oddział w Gdańsku. Obecnie współpracuje z firmą DGT w Straszynie. Zajmuje się głównie konstruowaniem systemów zarządzania oraz przetwarzania danych bilingowych.



e-mail: leszek@dgt.com.pl

Dr inż. Michał PORZEZIŃSKI

Uzyskał stopień doktora nauk technicznych w 2001 roku na Wydziale Elektrotechniki i Automatyki Politechniki Gdańskiej, gdzie pracuje jako adiunkt w Katedrze Automatyki. Współpracuje również z firmą DGT. Jego zainteresowania naukowe dotyczą zagadnień związanych z projektowaniem komputerowych systemów pomiarowo-sterujących oraz rozproszonych systemów automatyki budynków ze szczególnym uwzględnieniem problemów niezawodności i bezpieczeństwa.



e-mail: mporz@ely.pg.gda.pl

Streszczenie

W artykule przedstawiono rozproszony system nadzoru przygotowany w firmie DGT do zarządzania uszkodzeniami urządzeń pracujących w ogólnopolskiej sieci telekomunikacyjnej. Opracowany od podstaw system wykorzystuje infrastrukturę i mechanizmy komunikacyjne sieci Intranet, pozwala na ciągły nadzór do kilkuset obiektów obejmujących łącznie kilkadziesiąt tysięcy nadzorowanych urządzeń (elementów składowych central i obiektów współpracujących) na terenie całego kraju. Opisano strukturę systemu, jego funkcjonalność, sposób komunikacji oraz mechanizmy bezpieczeństwa i przedstawiono możliwości dalszego rozwoju.

Słowa kluczowe: system nadzoru, monitorowanie uszkodzeń, SCADA.

Distributed system for remote monitoring of telecommunications equipment

Abstract

The paper presents a distributed supervisory system developed in the DGT Company to monitor failures of telecommunications devices in a nationwide telecommunications network. This system, developed from the ground up, allows continuous supervising of tens of thousands of supervised devices (components of telephone exchanges and other objects) throughout the country. Key issues have been resolved through use of the concept of network supervisory agents (Fig. 1), adoption of the hierarchical structure of alarm nodes (Fig. 3) and use of Web servers and Web browsers instead of the traditional SCADA application (Figs. 5 - 7). The system versatility enables developing new agents for supervising the objects of significantly different structure and functionality, without requiring any changes in the pre-existing parts of the system. The experience of several years of the system operation has shown that the developed conception is correct and the DGT supervisory system has been successfully used in several independent installations.

Keywords: supervisory system, failure monitoring, SCADA.

1. Wprowadzenie

Podczas eksploatacji urządzeń technicznych bardzo często zachodzi potrzeba monitorowania ich aktualnego stanu i sygnalizowania wystąpienia ewentualnych uszkodzeń. Klasycznym rozwiązaniem systemu nadzoru, stosowanym w przemyśle, jest wykorzystanie gotowego oprogramowania typu SCADA (Supervisory Control and Data Acquisition). Oprogramowanie uruchomione na stacji operatorskiej współpracuje przeważnie ze zbiorem sterowników przemysłowych dostarczających informacje o stanie wybranych punktów pomiarowych nadzorowanego obiektu.

Do zbierania danych wykorzystywana jest najczęściej lokalna przemysłowa sieć komputerowa łącząca sterowniki ze sobą, np. popularna sieć Profibus DP [1]. Często stosowanym elementem jest też serwer OPC, za pośrednictwem którego stacje operatorskie odczytują dane nadzorowanego procesu. Takie rozwiązanie pozwala na ujednolicenie interfejsu komunikacyjnego aplikacji SCADA. Opis zasady działania serwera OPC i aktualnych tendencji rozwojowych tego standardu można znaleźć w m.in. opracowaniach: [2] oraz [3]. Zebrane w ten sposób dane pozwalają na prezentację aktualnego stanu obiektu w postaci graficznej, sygnalizowanie wartości nieprawidłowych, rejestrację historii zdarzeń, a często również na zdalne sterowanie. Struktura nadzorowanego obiektu musi być uwzględniona w oprogramowaniu stacji operatorskiej na etapie jego tworzenia i każda jej późniejsza zmiana pociąga za sobą konieczność zmian w aplikacji SCADA.

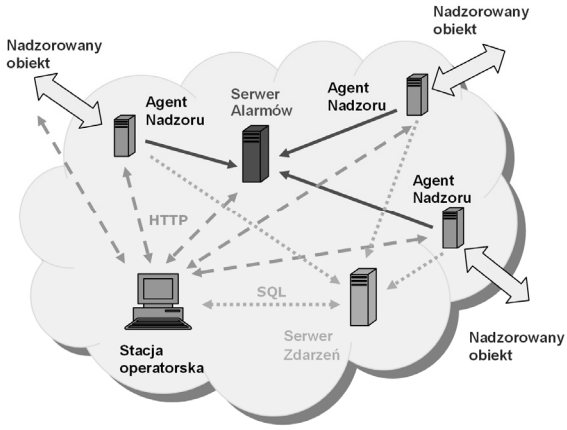
W większości wypadków takie rozwiązanie jest w pełni zadowalające. Istnieją jednak systemy, w przypadku których, typowe rozwiązania przemysłowe mogą być niewystarczające lub zbyt drogie. Przykładem może być zbiór urządzeń telekomunikacyjnych produkowanych przez firmę DGT (jednego z największych krajowych producentów systemów telekomunikacyjnych), obejmujących bardzo różne klasy urządzeń: od systemowych aparatów telefonicznych i bramek telefonii VoIP, po centrale telefoniczne i zintegrowane systemy łączności radiowej. Urządzenia te są rozproszone na terenie całego kraju stanowiąc setki tysięcy potencjalnych punktów alarmowych. Obiekty tego typu charakteryzują się dużą różnorodnością funkcjonalną, niestandardowymi interfejsami oraz częstymi zmianami struktury związanymi z ciągłą rozbudową i modernizacją systemu, co wymagałoby ciągłej aktualizacji typowej aplikacji SCADA. Ponadto, ze względu na duże rozproszenie obiektów pożądane jest, aby dostęp do informacji o aktualnym stanie urządzeń był możliwy z dowolnego komputera włączonego do sieci nadzoru, co znacznie ułatwia nadzór i ewentualny serwis.

Mając na uwadze powyższe wymagania zdecydowano się na opracowanie od podstaw dedykowanego systemu nadzoru. Kluczowe problemy rozwiązano dzięki zastosowaniu koncepcji sieci agentów nadzoru, przyjęciu hierarchicznej struktury punktów alarmowych odzwierciedlających stan nadzorowanych obiektów i wykorzystaniu do ich prezentacji serwerów stron WWW oraz przeglądarki internetowej zamiast klasycznej aplikacji SCADA.

2. Koncepcja systemu

2.1. Struktura systemu

Prezentowany system nadzoru ma charakter rozproszony, co pokazano na rysunku 1. Jest on zbiorem połączonych z sobą aplikacji pełniących role: agentów nadzoru, serwerów alarmów, serwerów zdarzeń oraz aplikacji pomocniczych. Poszczególne programy mogą pracować na jednym lub wielu różnych komputerach, w zależności od potrzeb wynikających z wielkości systemu. Dostęp do danych udostępnianych przez poszczególne aplikacje jest możliwy z dowolnego komputera sieci za pomocą zwykłej przeglądarki internetowej obsługującej protokół HTTP. Dzięki temu nie jest konieczne instalowanie specjalistycznych programów typu SCADA na komputerach stacji operatorskich. Zalety takiego rozwiązania wraz z opisem możliwych do wykorzystania mechanizmów komunikacji zostały opisane w [4].



Rys. 1. Ogólna struktura systemu nadzoru
Fig. 1. Overall structure of the supervisory system

2.2. Kanały komunikacyjne

Elementy systemu nadzoru współpracują ze sobą za pośrednictwem logicznych kanałów komunikacyjnych, w większości przypadków zrealizowanych w o parciu o infrastrukturę sieci Intranet. Do transportu danych wykorzystywany jest najczęściej stos protokołów z rodziny TCP/IP z dobudowaną odpowiednią warstwą aplikacji. Można wyróżnić trzy podstawowe rodzaje kanałów: Kanał obserwacji nadzorowanego urządzenia, kanał przesyłania danych o stanie urządzeń oraz kanał przesyłania informacji o zdarzeniach.

Kanał obserwacji nadzorowanego urządzenia jest lokalnym kanałem komunikacyjnym agenta łączącym go z nadzorowanym obiektem. Kanał ten jest zdeterminowany rodzajem interfejsu nadzorowanego urządzenia. W praktyce wykorzystywane są najczęściej protokoły HDLC, SNMP, RS232, RS485 oraz inne, bazujące na UDP i TCP. Kanał ten umożliwia agentowi gromadzenie informacji o bieżącym stanie nadzorowanego obiektu, a w niektórych przypadkach również sterowanie obiektem poprzez przekazywanie poleceń operatora.

Kanał przesyłania informacji o alarmach łączy agentów nadzoru z serwerami alarmów. Za jego pomocą przekazywane są informacje o bieżącym stanie nadzorowanych przez agenta obiektów w postaci aktualnego poziomu alarmu i listy aktywnych alarmów.

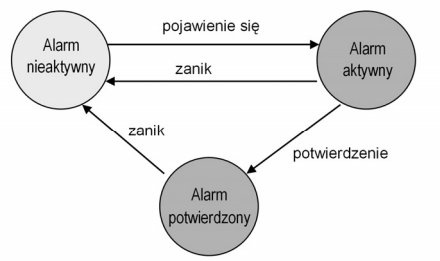
Kanał przesyłania informacji o zdarzeniach pozwala z kolei na rejestrację w serwerze zdarzeń informacji o zmianie stanu alarmów (pojawieniu się, zaniku lub potwierdzeniu) i innych działaniach operatora wraz z odpowiednim znacznikiem daty i czasu wystąpienia zdarzenia. Dane te, tworzące tzw. historię zdarzeń, są w systemie przetwarzane i archiwizowane niezależnie od prezentacji aktualnych (bieżących) alarmów nadzorowanego urządzenia i wynikającego z nich poziomu alarmu.

2.3. Agent nadzoru

Agent nadzoru jest podstawowym elementem funkcjonalnym systemu. Jego główną rolą jest odczytywanie danych z nadzorowanych obiektów, ich analiza oraz dynamiczne generowanie stron WWW prezentujących, w postaci graficznej, strukturę i stan nadzorowanych obiektów. Pośrednikiem w przekazywaniu stron WWW jest serwer HTTP komputera, na którym agent jest zainstalowany, a prezentowana informacja jest dostępna dla operatorów systemu nadzoru z poziomu zwykłej przeglądarki internetowej. Oprócz tego Agent przekazuje informacje o stanie alarmów nadzorowanych obiektów do serwerów alarmowych i rejestruje zdarzenia alarmowe w serwerze zdarzeń za pośrednictwem opisanych wcześniej kanałów komunikacyjnych.

Struktura nadzorowanego urządzenia jest reprezentowana w postaci hierarchicznego zbioru wewnętrznych obiektów agenta, zwanych węzłami. Każdy węzeł posiada jednoznacznie identyfikujący go adres i nazwę. Węzeł jest również widziany przez stację operatorską jako strona WWW. Hierarchiczna struktura węzłów odpowiada najczęściej strukturze nadzorowanych urządzeń i odzwierciedla strukturę adresową poszczególnych węzłów. Przykładowo, centrala telefoniczna składa się z modułów, te z kolei składają się z sekcji, a każda sekcja zawiera pewną liczbę procesorów, z których każdy może być źródłem kilkunastu różnych alarmów. Drzewiastą strukturę można stosować również do obiektów, których struktura adresowa jest z natury płaska np. do systemowych aparatów telefonicznych VoIP. Można wówczas grupować obiekty według pewnych kryteriów np. lokalizacji geograficznej (miasto, instytucja, budynek) lub lokalizacji sieciowej (sieć, podsieć) itp.

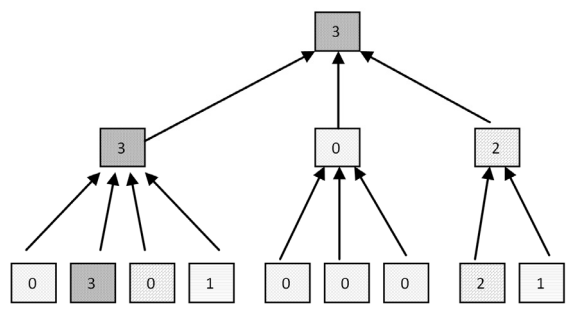
Każdy węzeł może być punktem alarmowym. Punkt alarmowy posiada predefiniowany zbiór alarmów, które mogą zaistnieć. Alarm jest sygnalizacją nieprawidłowego stanu obiektu i cechuje się poziomem (bardzo pilny, pilny, niepilny) oraz opisem pozwalającym zidentyfikować jego źródło. Dane te są określane podczas konfiguracji systemu i mogą być modyfikowane przez uprawnionego operatora. W trakcie pracy systemu alarm może dynamicznie zmieniać swój stan z nieaktywnego na aktywny i odwrotnie. Alarm aktywny charakteryzuje się ponadto dodatkowym stanem, sygnalizującym fakt potwierdzenia alarmu przez operatora (rys. 2).



Rys. 2. Diagram stanów pojedynczego alarmu
Fig. 2. Diagram of the single alarm states

Nadzorowane obiekty mogą dostarczać agentowi gotowych informacji o stanach alarmowych uzyskiwanych na drodze autodiagnostyki (alarmy wewnętrzne nadzorowanego obiektu). Możliwe jest również analizowanie innych informacji o stanie nadzorowanego obiektu (np. aktualnych wartości napięć, prądów czy temperatury) i podejmowanie decyzji o zaistnieniu alarmu przez samego agenta.

Przyjmuje się, że poziom alarmu punktu alarmowego jest najwyższym poziomem aktywnego alarmu związanego z tym punktem. Ponadto, mając na uwadze drzewiastą strukturę węzłów, wprowadzono zasadę, że poziom alarmu danego węzła jest najwyższym poziomem alarmu węzłów mu podlegających (rys. 3).



Rys. 3. Propagacja poziomu alarmu w hierarchicznej strukturze węzłów
Fig. 3. Propagation of the alarm level in the hierarchical structure of nodes

2.4. Pozostałe elementy systemu

Oprócz agentów ważnymi elementami systemu są również aplikacje pełniące rolę serwerów alarmów, serwerów zdarzeń oraz koncentratorów danych.

Serwer alarmów jest obiektem najwyższym w hierarchii wszystkich punktów alarmowych. Odwzorowuje on stan wszystkich podległych sobie agentów oraz listę alarmów aktywnych w nadzorowanym podsystemie. Strona WWW generowana przez serwer alarmów stanowi dla operatora punkt wyjścia w drodze do wybranego punktu alarmowego, dzięki mechanizmowi odnośników automatycznie przekierowujących przeglądarkę do wybranego agenta lub jego punktu alarmowego. Strona ta, podobnie jak w przypadku agenta jest generowana dynamicznie i publikowana za pośrednictwem standardowego serwera HTTP.

Serwer zdarzeń pełni rolę bazy danych, w której zapisywane są wszystkie zdarzenia związane z alarmami i ich obsługą. rejestrowane są m.in. data i czas zdarzenia, rodzaj zdarzenia (pojawienie się alarmu, potwierdzenie alarmu, zanik alarmu) oraz dane identyfikujące agenta i punkt alarmowy będący źródłem zdarzenia. Dane te mogą być przeglądane, przetwarzane i analizowane za pomocą dodatkowych narzędzi programowych generujących zapytania w języku SQL.

Rolą koncentratora jest zmniejszenie liczby otwartych połączeń logicznych pomiędzy serwerem alarmów, a podległymi mu agentami. Utrzymuje on logiczne połączenia z wybraną grupą agentów i przekazuje otrzymywane dane do serwera za pomocą pojedynczego kanału logicznego. Koncentrator ponadto może przekazywać otrzymywane dane do kilku wskazanych serwerów, co pozwala na dublowanie serwerów i tworzenie struktur redundantnych. Takie rozwiązanie zapewnia niezawodność i skalowalność systemu umożliwiając obsługę zarówno małych, kilkuagentowych systemów, jak i systemów liczących setki agentów nadzoru.

3. Niezawodność i bezpieczeństwo

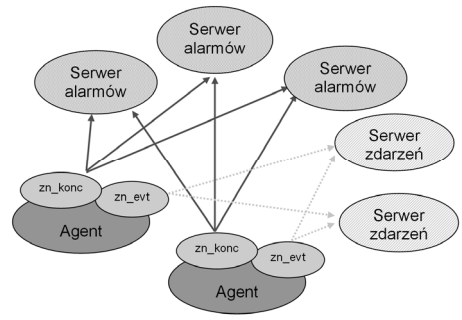
Głównym założeniem projektu systemu było zapewnienie jego jak największej niezawodności. W trakcie projektowania uwzględniono możliwość występowania zarówno błędów systematycznych wprowadzonych na etapie opracowywania oprogramowania, jak i błędów przypadkowych, wynikających z zakłóceń oddziałujących na eksploatowany system.

Zredukowanie liczby błędów systematycznych osiągnięto poprzez: modularyzację polegająca na dekompozycji systemu na mniejsze elementy funkcjonalne, zastosowanie mechanizmu logowania zdarzeń informujących o nieprawidłowościach w pracy systemu oraz odpowiednie zarządzanie cyklem wytwarzania oprogramowania. Duże znaczenie w uzyskaniu wymaganej jakości oprogramowania ma również przeprowadzany zgodnie z zasadami sztuki inżynierskiej [5] proces testowania oprogramowania oraz system rejestrowania błędów zgłaszanych przez użytkowników.

Najczęstszymi błędami przypadkowymi występującymi w systemie są: błędy komunikacji (przekłamanie danych lub całkowita utrata łączności), uszkodzenia sprzętu oraz nieprawidłowe działanie aplikacji składowych. Przekłamanie danych jest w większości przypadków wykrywane już na poziomie warstwy łącza danych lub transportowej na podstawie sumy kontrolnej. Brak łączności jest wykrywany przez system nadzoru w oparciu o mechanizm okresowego odpytywania lub mechanizm cyklicznego powiadamiania. Pierwszy sposób stosowany jest najczęściej w kanałach obserwacji nadzorowanego urządzenia i jest łączony z mechanizmem odpytywania o stan nadzorowanego urządzenia. Odpowiedź jest jednocześnie dowodem poprawnego działania kanału komunikacyjnego. Drugi sposób zakłada cykliczne przesyłanie meldunku do odbiorcy. Odmierzany jest czas od chwili odebrania ostatniej wiadomości. Przekroczenie określonej wartości czasu powoduje zgłoszenie błędu. W przedstawianym systemie nadzoru błąd braku komunikacji jest sygnalizowany jako alarm.

Dodatkowym mechanizmem jest system monitorowania aplikacji będących składnikami systemu. Każda z aplikacji w chwili wykrycia krytycznego błędu kończy swoje działanie. Specjalna aplikacja monitorująca wykrywa ten fakt i ponownie uruchamia brakujący proces. Aplikacja monitorująca jest uruchamiana i monitorowana przez inną aplikację należącą do listy aplikacji monitorowanych. Tym samym zakończenie pracy, przez którąkolwiek z nich może być wykryte i naprawione.

Wprowadzenie w systemie procesów będących multiplekserami/demultiplekserami wiadomości pozwala na swobodne kształtowanie redundantnej struktury systemu dostosowanej do potrzeb instalacji końcowej. Poniżej przedstawiony jest prosty przykład struktury systemu z potrójnym serwerem alarmów i zdublowanym serwerem zdarzeń (rys. 4).



Rys. 4. Przykład redundantnej struktury systemu nadzoru
Fig. 4. An example of the supervisory system redundant structure

Ważnym elementem systemu są również mechanizmy kontroli dostępu do zasobów. Są one wbudowane w oprogramowanie systemu i dotyczą każdego odwołania do jakiejkolwiek wywoływanej strony HTML. Autoryzacja użytkowników odbywa się w oparciu o mechanizmy systemu operacyjnego i serwera HTTP. Administrator ma możliwość definiowania grup użytkowników, które mogą być odpowiednikiem jednej z 14 możliwych grup, dla której definiowane są zasady dostępu. Definicja obejmuje dostęp do strony oraz wykonanie akcji na obiekcie, którego stan jest prezentowany. Możliwe jest też wprowadzenie użytkownika do jednej z grup śledzonych – wtedy pełna historia jego operacji będzie pamiętana.

4. Rozwój systemu i przykładowe instalacje

Większość aplikacji systemu nadzoru została napisana w języku C++ i działa na platformie Windows (NT, 2000, XP, 2003 Server, 2008 Server). We fragmentach związanych z obsługą stron WWW wykorzystano również język Java oraz Java Script. Od momentu powstania system podlega ciągłemu rozwojowi, polegającemu głównie na tworzeniu nowych agentów nadzorujących kolejne typy urządzeń telekomunikacyjnych. Zestawienie agentów nadzoru opracowanych w ciągu ostatnich lat zawarto w tabeli 1.

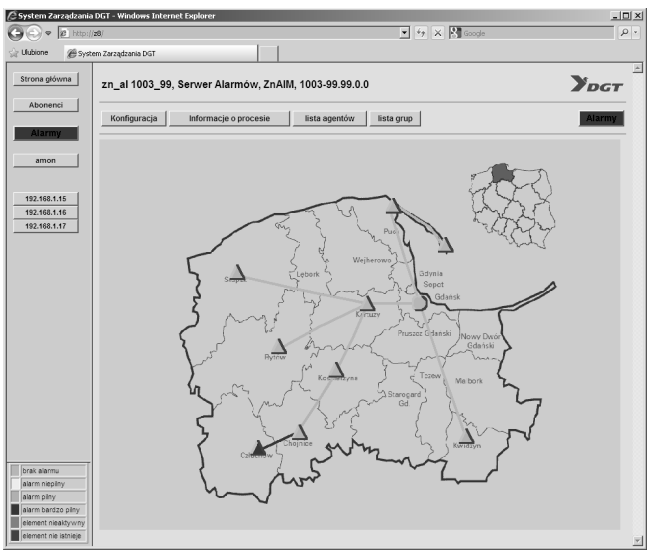
Najważniejszą instalacją systemu jest sieć zarządzania urządzeniami DGT zainstalowanymi w TP (Telekomunikacja Polska). Obejmuje ona sto kilkadziesiąt obiektów telekomunikacyjnych (central telefonicznych, systemów dostępu abonenckiego oraz dynamicznych przetworników sygnalizacji wraz z osprzętem sieciowym), zainstalowanych u operatora. Pozostałe instalacje systemu nadzoru obejmują, między innymi: sieci central innych operatorów, urządzenia systemu dostępu abonenckiego (SDA) oraz System zintegrowanej łączności radiowej (MCS). Ważną instalacją jest również sieć zarządzania centralami produkcji DGT w wojsku, gdzie możliwość rozproszenia systemu oraz szybka zmiana jego konfiguracji ma bardzo istotne znaczenie.

Przykładowy widok okna serwera alarmów systemu pokazano na rysunku 5. Kolor obiektów odzwierciedla aktualny poziom alarmu. Kliknięcie w obiekt powoduje, zgodnie z przyjętą koncepcją, przekierowanie przeglądarki do strony WWW prezentowanej przez wybranego agenta (rys. 6) oraz umożliwia, na tej samej

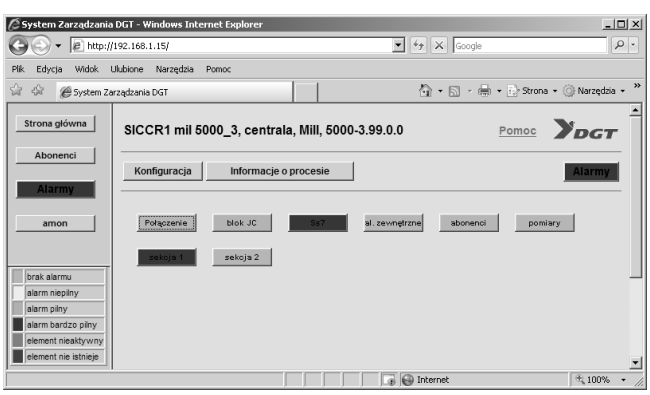
zasadzie, dalsze zagłębianie się w strukturę nadzorowanych obiektów.

Tab. 1. Zestawienie dotychczas opracowanych agentów
Tab. 1. Summary of the agents already developed

Nazwa	Opis
Środowisko systemu nadzoru	
ZN_AL	Serwer alarmów
ZN_EVA, ZN_EVT	Procesy zapisu zdarzeń
ZN_WDOG, ZN_AMON, ZN_MUSE	Programy nadzoru zasobów i obsługi innych procesów
ZN_WAN	Agent nadzoru nad routerami i połączeniami sieciowymi,
Podsystem nadzoru nad obiektami	
ZN_MIL	Agent nadzoru central DGT typu MCS
ZN_SDA	Agent nadzoru nad obiektami Systemu Dostępu Abonenckiego
ZN_MCS	Agent nadzoru nad zintegrowanym systemem łączności radiowej
ZN_ATK, ZN_AST, ZN_CRR, ZN_EXP	Programy agentów nadzoru nad urządzeniami DGT (telefony systemowe, terminale kablowe, rejestratory rozmów itp.)
Podsystem zarządzania konfiguracją	
ZN_MKBD, ZN_CFG, ZN_CFGSPL	Programy agentów do zarządzania konfiguracją central
Podsystem przetwarzania bilingu	
traLin, traNs, traK, traWers	Programy agentów do zarządzania bilingiem

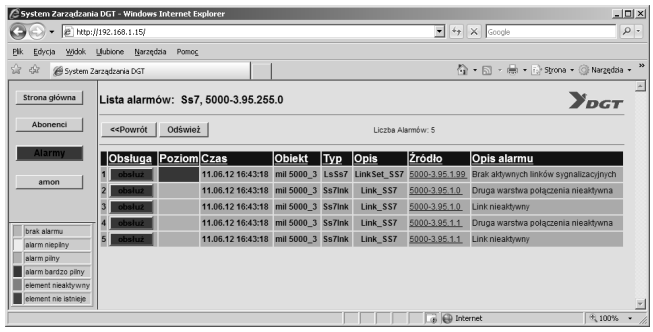


Rys. 5. Przykładowy widok okna serwera alarmów
Fig. 5. A sample view of the alarm server window



Rys. 6. Przykładowy widok okna agenta systemu nadzoru
Fig. 6. A sample view of the supervisory agent window

Na każdym z poziomów możliwy jest także dostęp do listy aktywnych alarmów (rys. 7) przypisanych do danego węzła oraz węzłów położonych niżej w hierarchii.



Rys. 7. Przykładowy widok okna listy aktywnych alarmów
Fig. 7. A sample view of the active alarm list window

5. Podsumowanie

Doświadczenia kilku lat eksploatacji systemu pokazały, że przyjęta koncepcja w pełni się sprawdziła. System nadzoru DGT jest z powodzeniem eksploatowany w kilku niezależnych instalacjach obejmując swoim zasięgiem kilkadziesiąt tysięcy nadzorowanych urządzeń.

Jedną z największych zalet systemu jest jego uniwersalność. Dzięki niej możliwe było opracowywanie kolejnych agentów obejmujących nadzorem obiekty znacząco różniące się między sobą strukturą i funkcjonalnością, bez konieczności zmian we wcześniej istniejących częściach systemu.

Wykorzystanie infrastruktury sieci Intranet i zastosowanie przeglądarki internetowej zamiast dedykowanej graficznej aplikacji SCADA umożliwia łatwe poruszanie się po zasobach informacyjnych systemu nadzoru, łącznie z prezentowaniem stron generowanych przez same nadzorowane urządzenia.

Uniwersalność systemu pozwala na wykorzystanie go do nadzoru praktycznie dowolnego obiektu. Wymaga to jedynie opracowania odpowiedniego agenta odwzorowującego strukturę nadzorowanego obiektu i przetwarzającego udostępniane przez obiekt sygnały. W najbliższym czasie na Wydziale Elektrotechniki i Automatyki Politechniki Gdańskiej planowane są prace nad zintegrowaniem prezentowanego systemu nadzoru z otwartymi systemami automatyki budynków. Wiąże się to z koniecznością opracowania odpowiednich agentów i metod niezawodnego odczytu danych z obiektów, podczas gdy pozostałe komponenty systemu mogą być wykorzystane bez większych zmian.

6. Literatura

[1] Solnik W., Zajda Z.: Komputerowe sieci przemysłowe Profibus DP i MPI. Oficyna Wydawnicza Politechniki Wrocławskiej, 2007.
[2] Berge J.: Software for Automation: Architecture, Integration, and Security, ISA, 2005.
[3] Lange J., Iwanitz F., Burke T.J.: OPC From Data Acces to Unified Architecture, VDE VERLAG GMBH, 2010.
[4] Mazur L., Porzeziński M.: Remote Monitoring and Control of Technical System Using Internet Network Technology, Proceedings of the IEEE International Conference on Technologies for Homeland Security and Safety TEHOSS 2005, s. 407-412, Gdansk 2005.
[5] Górski J. i inni: Inżynieria oprogramowania w projekcie informatycznym, Mikom, 2000.

otrzymano / received: 03.05.2011
przyjęto do druku / accepted: 06.06.2011 *artykuł recenzowany*