WIRTUALIZACJA SCADA

Centralne zarządzanie systemami SCADA w wirtualnym środowisku

Krzysztof Dziambor & Andrzej Soroczyński

Każdy menadżer produkcji chciałby mieć możliwość pełnego przeglądu sytuacji, niezależnie od tego, gdzie się w tej chwili znajduje. Z kolei działania służb utrzymania ruchu i automatyków byłyby szybsze i skuteczniejsze, gdyby interwencja w zakresie systemów SCADA i sterowników PLC była możliwa z dowolnego miejsca w przedsiębiorstwie. Jeżeli do tego dodamy powiadomienia o ważnych zdarzeniach otrzymywane na bieżąco na przenośne urządzenia oraz natychmiastowe samoczynne zastępowanie uszkodzonych elementów systemu przez ich redundantne odpowiedniki, to otrzymamy system nowej generacji, o podwyższonej niezawodności, który usprawnia utrzymanie ruchu oraz ogranicza przestoje wywołane awariami, a co za tym idzie, także koszty utrzymania ruchu.

Artykuł prezentuje wdrożony w polskim przedsiębiorstwie projekt, który spełnia postawione we wstępie wymagania. Celem projektu było uporządkowanie i ujednolicenie wielu różnorodnych, dotychczas odizolowanych aplikacji SCADA i umieszczenie ich w jednorodnym, wspólnym środowisku, spełniającym dodatkowo duże wymagania w zakresie zarządzania bezpieczeństwem informacji oraz przygotowanym do wymiany danych z poziomem nadrzędnym MES/ERP.

> Włożono wiele pracy w implementację założeń dotyczących bezpieczeństwa IT i systemu SCADA w oparciu o filozofię „defence in depth".

W projekcie od samego początku założono ścisłe współdziałanie działów utrzymania ruchu (UR) oraz IT. Pokażemy korzyści wynikające z takiego podejścia oraz wyzwania stojące przed twórcami systemu SCADA oraz pracownikami UR i IT. Połączenie wiedzy i doświadczenia tych działów stworzyło szansę na uzyskanie lepszego i lepiej zarządzanego rozwiązania niż w typowych realizacjach systemów SCADA, prowadzonych bez udziału IT.
Realizację projektu powierzono firmie ASKOM i oparto na systemie SCADA Asix, z wykorzystaniem zalet technologii wirtualizacji oraz zaawansowanych usług sieciowych.
System objął niemal wszystkie procesy produkcyjne w przedsiębiorstwie: 14 dotychczasowych aplikacji, ponad 65 000 zmiennych procesowych, tysiące alarmów, dziesiątki serwerów, stacji operatorskich, terminali produkcyjnych i biurowych.

Defence in depth

Obrona w głąb – taktyka projektowania zabezpieczeń dla systemów informatycznych, która polega na wprowadzeniu wielu niezależnych warstw zabezpieczeń. Taka nadmiarowość znacząco podnosi poziom ochrony ograniczając skutki błędów i ataków.

Przy realizacji tego projektu włożono wiele pracy w implementację głównych założeń dotyczących bezpieczeństwa IT i systemu SCADA w oparciu o filozofię „defence in depth", promowaną przez liderów rynku np. firmę Siemens.

SYNERGIA DZIAŁÓW UR I IT

Zazwyczaj spotykamy się z poważnymi obawami przed ingerencją działu IT w warstwy SCADA i sterowników (PLC). Okazuje się, że te obawy nie są uzasadnione, gdy wszystkie strony są otwarte na nowe rozwiązania. Uzyskane podczas wdrożenia korzyści pokazały, że warto było podjąć to wyzwanie.

Dział UR wniósł specjalistyczną wiedzę o PLC i SCADA, a dział IT – wiedzę obejmującą sprzęt komputerowy, technologie wirtualizacji, techniki budowy i metody zarządzania siecią oraz bezpieczeństwo systemów informatycznych.
Z kolei system Asix musiał spełnić nowe wymagania, do których na początku nie był przygotowany. Stało się to możliwe, gdyż jest to autorski system firmy ASKOM uczestniczącej we wdrożeniu. Było więc możliwe wykonanie odpowiednich zmian i rozszerzeń. Obecnie tak zmodyfikowany i sprawdzony w praktyce system jest już dla każdego dostępny na rynku w wersji Asix.Evo 8.1.

DEKOMPOZYCJA ZADANIA

Przedsiębiorstwo, które zwróciło się do firmy ASKOM z propozycją projektu, stanęło przed poważną zmianą organizacyjną i technicznym wyzwaniem. Zagadnienie podzielono na 3 podstawowe warstwy:

- **PLC** (w gestii UR) – sprzęt i oprogramowanie PLC,
- **SCADA** (w gestii UR) – instalacja, konfiguracja, aktualizacje i budowa systemów SCADA,
- **IT** (w gestii IT) – interfejsy sieciowe, fizyczne sieci ze switchami, serwery, terminale, ich konfiguracja, zabezpieczenia, zarządzanie i aktualizacja, wirtualizacja, systemy operacyjne, a także monitoring całości infrastruktury komunikacyjnej i serwerowej.

Dla poszczególnych warstw przyjęto założenia wynikające z korporacyjnych wymogów zarządzania bezpieczeństwem informacji oraz koncepcji posadowienia serwerów na klastrze o podwyższonej niezawodności.

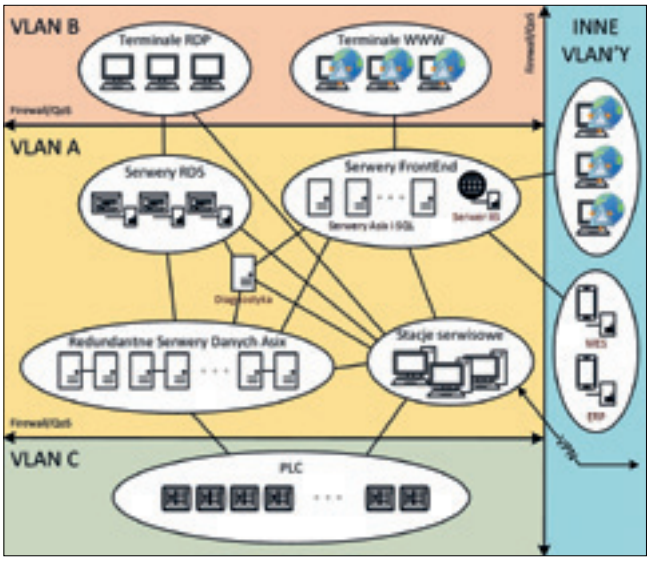
WARSTWA PLC

Wymiana danych PLC-Asix odbywa się poprzez sieć Ethernet i protokół TCP/IP. Dostęp do PLC został ograniczony do wybranych adresów IP, portów i adresów MAC. Dzięki komunikacji TCP/IP, sterowniki mogą być programowane z kilku wyznaczonych wirtualnych stacji z zainstalowanym oprogramowaniem serwisowym PLC, a dostęp do nich przez zdalny pulpit sprawia, że służby utrzymania ruchu mogą wykonywać czynności serwisowe z różnych oddalonych stanowisk.
Centralna diagnostyka zawarta w warstwie SCADA obejmuje także PLC, dzięki czemu odpowiednie służby mają na bieżąco obraz funkcjonowania tej warstwy oraz otrzymują powiadomienia o ewentualnych usterkach.

> Służby utrzymania ruchu mogą wykonywać czynności serwisowe z różnych oddalonych stanowisk.

WARSTWA SCADA

Logiczną strukturę systemu w uproszczeniu pokazano na rysunku 1.



Rys 1. logiczna struktura systemu SCADA

Wszystkie serwery umieszczono w maszynach wirtualnych na niezawodnym klastrze. Dla każdej aplikacji zainstalowano dwa redundantne serwery danych (SD). Dzięki temu zapewniono dostępność systemu SCADA także w razie awarii lub planowego wyłączenia jednego z SD. W razie wystąpienia problemów (np. wadliwej łatki systemowej lub SCADA) mamy wystarczająco dużo czasu na odtworzenie serwera, gdyż w tym czasie pracuje drugi serwer, a przed instalacją na drugim serwerze – na eliminację przyczyn problemów. Oddzielono też rolę stacji operatorskiej od roli serwera danych. Dzięki temu bezpośredni dostęp do samych serwerów Asix mają tylko uprawnione służby.
Operatorzy i mistrzowie korzystają z bezdyskowych terminali podłączonych zdalnym pulpitem do sesji terminalowych Asix na wirtualnych serwerach RDS (Remote Desktop Services). Takie rozwiązanie obniża koszty licencji i sprzętu. Potrojenie serwerów RDS zapewnia dostęp do aplikacji także w razie awarii jednego z nich.

Awaria sprzętowa terminala również nie zatrzymuje proce su produkcyjnego, gdyż system nadal działa, a operator może przyłączyć się do tej samej sesji Asix z innego terminala. Wy miana urządzenia, jeśli konieczna, zajmuje nie więcej niż 15 mi nut. Terminale pozwalają na równoczesne podłączenie do wielu sesji zdalnych i ich łatwe przełączanie. Dlatego każdy terminal znakomicie nadaje się także do prowadzenia prac serwisowych, włączając w to programowanie PLC i SCADA.
Pozostali użytkownicy mogą korzystać z wersji przeglądarko wych aplikacji, czerpiących dane z serwerów pośredniczących. Webowy klient ma możliwość jedynie odczytu, a sterowanie celowo zablokowano. Kompresja komunikacji systemu Asix umożliwia wydajną pracę także na łączach WAN i VPN.
Dostępem do aplikacji SCADA na serwerach, a także do-po szczególnych terminali, zarządza administrator systemu. Uwie rzytelnianie użytkowników systemu Asix zostało zintegrowane z domeną przedsiębiorstwa i z bazą Microsoft Active Directory. Krok ten gwarantuje pełną zgodność z polityką złożoności i ter minowej zmiany haseł użytkowników, czasu i miejsc logowania oraz centralne zarządzanie użytkownikami. W systemie Asix zdefiniowano prosty i czytelny zestaw ról o określonych upraw nieniach. Administratorom udostępniono raport obrazujący aktualną strukturę i uprawnienia użytkowników.
Interfejs graficzny wszystkich aplikacji został ujednolicony, a dla każdej z nich przygotowano wersję dwujęzyczną: pol sko-angielską, która umożliwia posługiwanie się aplikacjami w międzynarodowej korporacji.

WARSTWA IT

Wszystkie wirtualne maszyny umieszczono na 3-hostowym klastrze. Odpowiednie wyskalowanie parametrów klastra, mo nitoring IT, procedury postępowania na wypadek awarii i re dundancja wirtualnych serwerów sprawiają, że nawet awaria 66 proc. fizycznych serwerów klastra i 50 proc. serwerów-wir tualnych systemu Asix, nie wpływa istotnie na funkcjonowanie całości systemu.
Kable światłowodowe do węzłów sieciowych doprowadzono z innych węzłów w sposób redundantny, aby sygnał sieciowy mógł do nich dotrzeć przynajmniej z 2 różnych kierunków. Podwojono też źródła zasilania elektrycznego punktów siecio wych oraz wyposażono je w zasilacze UPS z kartami do zdalne go zarządzania i monitoringu.
Fizyczne oddalenie serwerów od miejsca procesu produk cyjnego i umieszczenie ich w dedykowanych serwerowniach IT spełniających właściwe im regulacje i standardy, znaczą

> Nawet awaria 66 proc. fizycznych serwerów klastra i 50 proc. serwerów wirtualnych systemu Asix, nie wpływa istotnie na funkcjonowanie całości.

co podniosło bezawaryjność systemu SCADA, ale również bezpieczeństwo danych w razie kłopotów z samym procesem produkcyjnym (pożar, zalanie, etc.). Fakt, że wszystkie fizyczne i wirtualne maszyny znalazły się w serwerowniach i są moni torowane przy pomocy dedykowanych narzędzi na poziomie infrastruktury IT oraz SCADA, znacznie skraca czas wykrycia ewentualnej awarii i reakcji służb UR i IT.
Sieć zabezpieczono blokując fizyczny i logiczny dostęp nieupraw nionych osób lub sprzętu oraz ograniczając ruch sieciowy do nie zbędnego dla prawidłowego funkcjonowania całości systemu Asix i usług infrastruktury IT. Zablokowano też możliwość użycia portów USB. Zredukowano w ten sposób ryzyko zarażenia wiru sami lub nieautoryzowanego wyprowadzania danych z przed siębiorstwa. Wymiana plików następuje poprzez ich wielopozio mowe sprawdzenie systemami antywirusowymi i dedykowany do tego celu kanał VPN w ramach zdalnego dostępu. Istotne jest też to, że system Asix prawidłowo współpracuje z popularnymi systemami antywirusowymi i backupowymi, co umożliwiło uży cie typowego oprogramowania stosowanego do tych celów. Całe rozwiązanie otrzymało swój własny, wielopoziomowy system backupów oparty o klasyczne rozwiązania IT.

MONITORING I DIAGNOSTYKA

Wszystkie elementy infrastruktury są nadzorowane przez cen tralny system monitoringu IT. W razie przekroczenia zadanych wartości granicznych lub braku odpowiedzi ze strony urządze nia, natychmiast są powiadamiane odpowiednie służby. Dodat kowo system monitoringu jest zintegrowany z globalnym system mem analizy trendów systemów IT i pozwala w szybki sposób wychwycić zachowania systemu niezgodne z typowymi. Ad ministrator jest o tym fakcie powiadamiany, a dalsze działania zależą od jego decyzji.
W systemie Asix stworzono także aplikację diagnostyki (DIAG), która monitoruje funkcjonowanie samych systemów Asix, sy gnalizuje anomalie w ich działaniu lub problemy w komuni kacji z PLC. Aktualny stan jest widoczny na aplikacji WWW, udostępnionej służbom UR i IT. Dodatkowo Asix posiada system powiadamiania, który w razie wykrycia awarii lub ano

> Asix stał się kolejnym elementem składowym w przedsiębiorstwie, zgodnym z filozofią czwartej rewolucji przemysłowej (Industry 4.0).

malii, oprócz klasycznych komunikatów ekranowych, generuje komunikaty e-mail/SMS dla przypisanych do danego zdarzenia odbiorców. Komunikaty rozszerzono o alerty informujące o najbardziej niebezpiecznych zdarzeniach w samych aplikacjach i obiektach technologicznych.
Obydwa systemy monitoringu umożliwiają ciągły centralny nadzór nad aplikacjami i niemal natychmiastową reakcję odpowiednich służb UR i IT na sytuacje awaryjne.
Publikacja aplikacji na stronach intranetowych oraz rozsyłanie powiadomień o zdarzeniach systemowych sprawia, że kadra zarządzająca może mieć stały bezpośredni wgląd w sytuację w zakresie PLC i SCADA przedsiębiorstwa.

INTEGRACJA Z SYSTEMAMI NADRZĘDNYMI MES/ERP

Systemy SCADA znalazły się w tym samym środowisku i pod opieką tych samych służb, co systemy nadrzędne MES/ERP. Pozostaje to nie bez znaczenia dla sprawnego funkcjonowania dwustronnej wymiany danych z tymi systemami, ułatwia tworzenie spójnej, dobrze zabezpieczonej struktury oraz sprawną diagnostykę i serwis.

SYSTEM DLA MIĘDZYNARODOWEJ KORPORACJI

Ważną funkcjonalnością systemu Asix jest pełna wielojęzyczność interfejsu użytkownika przełączana w czasie rzeczywistym, w trakcie pracy programu. Ponadto czas jest przechowywany i przekazywany w konwencji UTC, a dopiero u użytkownika zamieniany na czas lokalny. Użytkownik widzi więc historię zdarzeń w systemie w swojej własnej strefie czasowej i w swoim języku. W dzisiejszych przedsiębiorstwach, ze względu na globalizację i mobilność pracowników i kadry zarządzającej, są to bardzo użyteczne cechy.

Industry 4.0

Pierwsza rewolucja przemysłowa wprowadziła maszyny parowe i produkcję seryjną, druga -elektryczność, trzecia – sterowniki PLC, a czwarta wprowadzi spójne, bezpieczne i centralnie zarządzane środowisko IT, które połączy systemy produkcyjne (MRP/ERP/MES/SCADA), sprzedaży, marketingowe, technologiczne (PLM) oraz fizyczne obiekty dotychczas nie zarządzane (dzięki IIoT/IoT), a także roboty, dając możliwość funkcjonowania przedsiębiorstw w zupełnie nowym, wielowymiarowym środowisku oraz szybkiej elastycznej adaptacji do dynamicznie zmieniającej się sytuacji rynkowej i wymagań klienta.

PODSUMOWANIE

Opisane rozwiązanie nie tylko wymaga współpracy UR z IT, ale także systemu SCADA spełniającego szereg wymagań, tak że tych nietypowych, m.in.: możliwość wirtualizacji serwerów i klientów SCADA, ich redundancja, praca w wersji przeglądarkowej, wbudowany system backupu kluczowych danych, odporność na instalację bieżących łatek systemowych, wielojęzyczność aplikacji, praca w różnych strefach czasowych, monitoring i procedury postępowania na wypadek awarii, system zabezpieczeń i zarządzania użytkownikami zintegrowany z usługą Active Directory, czy szczegółowa, stale aktualizowana dokumentacja w wersji elektronicznej.
Współpraca służb UR oraz IT przedsiębiorstwa z zespołem wdrożeniowym firmy ASKOM, a także z zespołem twórców Asix, doprowadziła do powstania systemu spełniającego wysokie wymagania stawiane przez system zarządzania bezpieczeństwem informacji, już na poziomie SCADA, a nawet PLC, jak i wymagania stawiane przez tradycyjnych użytkowników systemów SCADA (operatorów, służby UR i kadrę zarządzającą). Centralne zarządzanie i diagnostyka znacznie ułatwiły i podniosły skuteczność czynności serwisowych pracowników. Funkcjonowanie systemu stało się transparentne i czytelne. Nie bez znaczenia jest też ułatwiona integracja SCADA z systemami nadrzędnymi MES/ERP.
Dzięki opisanym rozwiązaniom, korzyści w obszarach funkcjonalności, niezawodności oraz łatwości eksploatacji i utrzymania ruchu udało się osiągnąć przy umiarkowanych kosztach realizacji. Co istotne, w zaprezentowanej wersji, system Asix stał się kolejnym elementem składowym w przedsiębiorstwie, zgodnym z filozofią funkcjonowania nowoczesnych fabryk, budowanych i pracujących w oparciu o założenia czwartej rewolucji przemysłowej (Industry 4.0).

ASKOM Spółka z o.o.
ul. Józefa Sowińskiego 13, 44-100 Gliwice
tel.: +48 32 30 18 100, e-mail: biuro@askom.com.pl
www.askom.com.pl | www.asix.com.pl

Artykuł dedykujemy naszemu nieodżałowanemu koledze śp. Januszowi Mierzwie, który był autorem koncepcji przedstawionego rozwiązania.