Synergia działów IT i automatyków przy wdrażaniu nowego podejścia do systemów SCADA – studium przypadku

Najczęściej stosowanym i typowym rozwiązaniem dla systemów SCADA jest ich ścisłe powiązanie z systemami automatyki pod opieką działu utrzymania ruchu (dalej UR). Rola działu informatyki (dalej IT) zaczyna się dopiero od separacji sieci systemów IT przedsiębiorstwa od sieci systemów SCADA. W tym artykule zaprezentujemy inne podejście, w którym od samego początku realizacji projektu założono ścisłe współdziałanie działów UR i IT, zaczynając już od sterowników. Pokażemy korzyści wynikające z takiego podejścia oraz wyzwania stojące przed twórcami systemu SCADA oraz pracownikami IT.

Krzysztof Dziambor
Andrzej Soroczyński

System zastosowano w polskim przedsiębiorstwie, działającym w ramach dużej międzynarodowej korporacji narzucającej ostre wymagania w zakresie bezpieczeństwa informacji, które sieć i system SCADA muszą spełnić. Realizację powierzono firmie ASKOM, we współpracy z działami UR oraz IT przedsiębiorstwa. Rozwiązanie oparto na systemie Asix.

Postaramy się przedstawić, w jaki sposób system Asix był w stanie dostosować się do wyjątkowo ambitnych planów i zadań w przedsiębiorstwie, a zarazem spełnić wymagania globalnego systemu zarządzania bezpieczeństwem informacji. Pokażemy też, jak wykorzystano zalety technologii wirtualizacji oraz zaawansowane usługi sieciowe.

Synergia działów UR i IT

Połączenie wiedzy i doświadczenia działów UR oraz IT daje szanse na uzyskanie lepszego i lepiej zarządzanego rozwiązania niż w typowych realizacjach systemów SCADA. Zwykle spotykamy się z poważnymi obawami przed ingerencją działu IT w warstwę SCADA i warstwę sterowników (dalej 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, która wykonała odpowiednie zmiany i rozszerzenia. Obecnie tak zmodyfikowany i sprawdzony w praktyce system jest już dla każdego dostępny na rynku w wersji Asix.Evo 8.1.

Opis rozwiązania

Opisywany projekt zakładał uporządkowanie i ujednolicenie wielu różnorodnych, dotychczas odizolowanych aplikacji SCADA przedsiębiorstwa oraz umieszczenie ich w jednorodnym wspólnym środowisku. Dalej pokażemy przyjęte rozwiązania, sposoby ich realizacji i osiągnięte korzyści.

Skala systemu
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. W końcowym rozwiązaniu znalazło się 36 wirtualnych serwerów Asix, 34 sesje terminalowe podstawowe i 14 awaryjnych. Dodatkowo umożliwiono dostęp do wszystkich aplikacji SCADA z przeglądarki internetowej dowolnego terminala korporacji za pośrednictwem sieci LAN lub WAN, jeżeli tylko administrator systemu nada temu terminalowi i osobie z niego korzystającej odpowiednie uprawnienia.

Platforma sprzętowa klastra
Rozwiązanie opiera się na klastrze z systemem wirtualizacji VMware, na którym posadowiono wszystkie kluczowe maszyny systemu.

Klaster wyposażono w 3 hosty 2-procesorowe. Każdy procesor ma 12 rdzeni wykorzystujących technologię Intel HT. Uzyskano w ten sposób 144-wątkowy klaster o podwyższonej niezawodności, w którym nawet przy awarii jednego hosta pozostaje wystarczająco dużo wątków i pamięci do utrzymania ciągłej pracy systemu.

Maszyny wirtualne na klastrze VMware korzystają z wydajnych, nadmiarowych macierzy dyskowych RAID-6 i RAID-10, z interfejsem Fiber Channel.

Dzięki klastrowi uzyskano dwupoziomową redundancję: dla fizycznych serwerów i dla wirtualnych serwerów Asix.

Logiczna struktura systemu
Logiczną strukturę systemu pokazano na rysunku na sąsiedniej stronie.

Wszystkie maszyny w ramach VLAN A (wirtualnej sieci komputerowej) są maszynami wirtualnymi działającymi na klastrze. Znajdują się tam serwery Asix oraz serwery RDS (ang. *Remote Desktop Services* – usługi zdalnego pulpitu) sesji terminalowych Asix.

VLAN B to terminale RDP typu cienki klient, podłączone do sesji Asix na serwerach RDS lub terminale przeglądarkowe.

Z kolei VLAN C zawiera PLC oraz inne urządzenia wymieniające dane procesowe z systemami Asix.
Wirtualne serwery pełnią kilka ról:
1. Serwery danych Asix komunikują się z warstwą PLC, a zgromadzone dane udostępniają innym serwerom i terminalom.
2. Na serwerach RDS działają sesje terminalowe Asix.
3. Serwery pośredniczące typu FrontEnd udostępniają dane terminalom WWW, raportom i systemom MES/ERP (SQL).
4. Na serwerze IIS znajdują się definicje aplikacji WWW.
5. Serwer DIAG pełni funkcje diagnostyczne.
6. Na serwerze plików przechowywane są definicje aplikacji, dokumentacje oraz kopie bezpieczeństwa.

Oprócz tego na klastrze znajdują się maszyny testowe, maszyny z programatorami PLC oraz zarządzające klastrem i backupem.

Operatorzy i mistrzowie korzystają z bezdyskowych terminali podłączonych zdalnym pulpitem do sesji terminalowych Asix na serwerach RDS. Pozostali użytkownicy mogą korzystać z wersji przeglądarkowych WWW aplikacji, czerpiących dane z serwerów pośredniczących.

Dekompozycja zadania

Przedsiębiorstwo, które zwróciło się do firmy ASKOM z propozycją tego interesującego projektu, stanęło przed poważną zmianą organizacyjną i technicznym wyzwaniem.

Zagadnienie podzielono na 3 podstawowe warstwy:
- PLC – w gestii UR, sprzęt i oprogramowanie PLC oraz konfiguracja interfejsu sieciowego,
- SCADA – w gestii UR, instalacja, konfiguracja, aktualizacje i budowa systemów SCADA,
- IT – w gestii IT, interfejsy sieciowe warstwy PLC i SCADA, 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, wybranych portów i adresów MAC.

Dzięki komunikacji TCP/IP sterowniki mogą być programowane z kilku wyznaczonych wirtualnych stacji z zainstalowanym oprogramowaniem serwisowym PLC. Dzięki dostępowi przez zdalny pulpit służby UR mogą wykonywać czynności serwisowe z różnych stanowisk.

Warstwa SCADA
Dla każdej aplikacji zainstalowano dwa redundantne serwery danych (dalej SD). Zapewnia to na poziomie oprogramowania dostępność systemu SCADA w razie awarii jednego z serwerów danych. Możliwa jest też bezprzerwowa aktualizacja systemu operacyjnego, systemu Asix lub aplikacji. W razie kłopotów jest wystarczająco dużo czasu na odtworzenie serwera, gdyż w tym czasie pracuje drugi serwer, a przed instalacją na drugim serwerze – na eliminację przyczyn problemów (np. wadliwej łatki systemowej).

Oddzielono też rolę stacji operatorskiej od roli serwera danych.

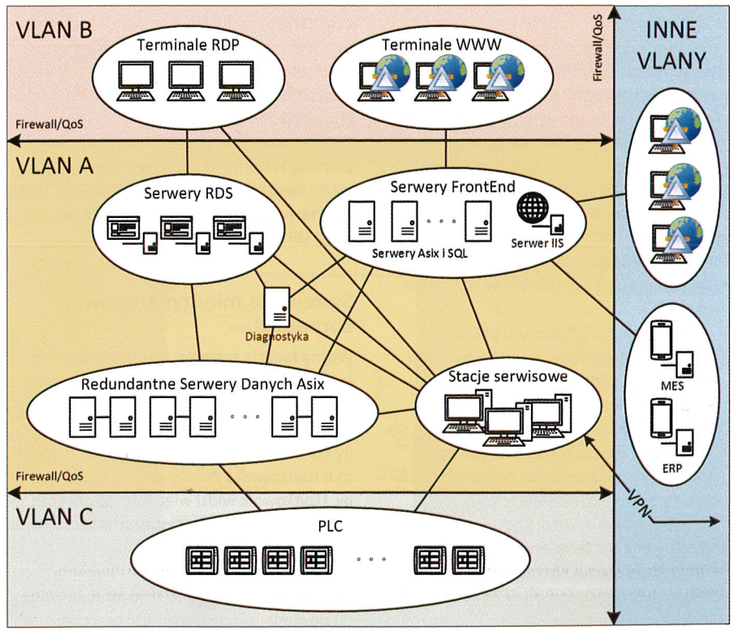
Serwery typu FrontEnd pełnią rolę źródła danych dla usług WWW i innych systemów w przedsiębiorstwie, izolując warstwy sterowania i nadzoru od obciążenia zapytaniami ze strony tych systemów i terminali.

Operatorzy i mistrzowie korzystają z bezdyskowych terminali podłączonych zdalnym pulpitem do sesji terminalowych Asix na serwerach RDS. Takie rozwiązanie obniża koszty licencji i sprzętu. Sprawia też, że bezpośredni dostęp do samych serwerów Asix mają tylko uprawnione służby.

Potrojenie serwerów RDS zapewnia dostęp do aplikacji także w razie awarii jednego z nich. Również awaria sprzętowa terminala nie zatrzymuje procesu produkcyjnego, gdyż system nadal działa, a operator może przyłączyć się do tej samej sesji Asix z innego terminala. Wymiana urządzenia zajmuje nie więcej niż 15 minut.

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 przeglądarkowych aplikacji, czerpiących dane z serwerów pośredniczących. Klient WWW ma możliwość jedynie odczytu (techniczne sterowanie byłoby możliwe, ale zostało zablokowane). Kompresja komunikacji systemu Asix umożliwia wydajną pracę także na łączach WAN i VPN.



Uwierzytelnianie użytkowników systemu Asix zostało zintegrowane z domeną przedsiębiorstwa i z bazą Microsoft Active Directory. Krok ten gwarantuje pełną zgodność z polityką złożoności i terminowej zmiany haseł użytkowników, czasu i miejsc logowania oraz centralne zarządzanie użytkownikami. W systemie Asix zdefiniowano prosty i czytelny zestaw ról o określonych uprawnieniach. Administratorom udostępniono raport obrazujący aktualną strukturę i uprawnienia użytkowników.

Interfejs graficzny wszystkich aplikacji został ujednolicony, a dla każdej z aplikacji przygotowano wersję dwujęzyczną: polsko-angielską, która umożliwia posługiwanie się aplikacjami w międzynarodowej korporacji.

Warstwa IT

Węzły sieciowe wyposażono w kilka źródeł zasilania sygnałem sieciowym przez instalację dwóch lub więcej kabli światłowodowych biegnących do węzła z fizycznie różnych kierunków i punktów dystrybucyjnych.

Zasilanie elektryczne punktów sieciowych podłączono z dwóch różnych podstacji oraz wyposażono w centralnie monitorowane zasilanie awaryjne (UPS).

Od strony sieci komputerowej zapewniono bezpieczny fizyczny i logiczny dostęp do interfejsów sieciowych, blokujący nieuprawnione osoby lub sprzęt nienależący do przedsiębiorstwa.

W celu spełnienia wymogów bezpieczeństwa informacji dokonano podziału logicznego sieci (segmentacji). Na potrzeby systemu SCADA wygenerowano 3 dedykowane wirtualne sieci komputerowe (VLAN):
VLAN A – dla serwerów aplikacyjnych i stacji serwisowych,
VLAN B – dla terminali bezdyskowych
VLAN C – dla PLC oraz innych urządzeń przemysłowych.

Cała komunikacja pomiędzy ww. VLAN-ami oraz pozostałymi segmentami sieci przedsiębiorstwa została ograniczona do ruchu sieciowego niezbędnego do prawidłowego funkcjonowania całości systemu Asix i usług infrastruktury IT.

W związku z tym, że ruch sieciowy w systemach Asix, a szczególnie ruch sieciowy pomiędzy PLC i SD, jest specyficzny i wymaga odpowiednich parametrów, dział IT opracował indywidualne polityki zarządzania ruchem sieciowym (priorytetyzację/QoS) dla systemu Asix.

Wirtualizacja, odpowiednie wyskalowanie parametrów klastra, monitoring IT, procedury postępowania na wypadek awarii i redundancja wirtualnych serwerów pozwalają nawet na awarię 66% fizycznych serwerów klastra i 50% serwerów wirtualnych systemu Asix, bez istotnego wpływu na funkcjonowanie całości systemu.

Fizyczne oddalenie serwerów od miejsca procesu produkcyjnego i umieszczenie ich w dedykowanych serwerowniach IT, spełniających właściwe im regulacje i standardy, znacząco podniosło bezawaryjność systemu SCADA, ale również bezpieczeństwo danych w razie kłopotów z samym procesem produkcyjnym (pożar, zalanie etc.).

W całej instalacji zablokowano możliwość użycia portów USB w celu eliminacji wymiany danych na pamięciach przenośnych, redukując w ten sposób ryzyko zarażenia wirusami lub nieautoryzowanego wyprowadzania danych z przedsiębiorstwa.

Wymiana plików np. ze wsparciem technicznym inżynierów ASKOM następuje przez ich wielopoziomowe sprawdzenie systemami antywirusowymi i dedykowany do tego celu kanał VPN w ramach zdalnego dostępu do przedsiębiorstwa.

Istotne jest też to, że system Asix prawidłowo współpracuje z popularnymi systemami antywirusowymi i backupowymi, co umożliwiło użycie oprogramowania typowo stosowanego do tych celów w ramach przedsiębiorstwa.

Całe rozwiązanie otrzymało swój własny, wielopoziomowy system backupów, oparty na klasycznych rozwiązaniach IT obejmujących:
- backup maszyn wirtualnych w trakcie ich pracy,
- backup określonych danych plikowych poprzez dedykowanego agenta backupu (dodatkowe skrypty weryfikują ich kompletność, a wyniki weryfikacji wysyłają e-mailem do wskazanych osób),
- regularną replikację kopii danych oraz przeniesienie na taśmach do innych obszarów na terenie przedsiębiorstwa.

Przygotowano też bezpieczną i wiarygodną infrastrukturę sieciowych serwerów czasu, synchronizujących czas PLC, SCADA oraz infrastruktury wirtualnej.

Monitoring i diagnostyka

Wszystkie elementy infrastruktury są nadzorowane przez centralny system monitoringu IT. W razie przekroczenia zadanych wartości granicznych lub braku odpowiedzi ze strony urządzenia, natychmiast są powiadamiane odpowiednie służby. Dodatkowo system monitoringu jest zintegrowany z globalnym systemem analizy trendów systemów IT i pozwala w szybki sposób wychwycić zachowania systemu niezgodne z typowymi, np. wzrost obciążenia CPU lub zajętości pamięci czy dużą ilość prób logowania do domeny. System analizy behawioralnej powiadamia wtedy o nietypowym zachowaniu elementów składowych infrastruktury IT i pozostawia do decyzji administratora dalsze działanie.

W systemie Asix stworzono także własną aplikację diagnostyki (dalej DIAG). Monitoruje ona funkcjonowanie samych systemów Asix, sygnalizuje anomalie w ich działaniu lub problemy w komunikacji z PLC. Aktualny stan jest widoczny na aplikacji WWW, udostępnionej służbom UR i IT. Dodatkowo Asix ma system powiadamiania, który w razie wykrycia awarii lub anomalii, 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.

Dodatkowo moduł DIAG został zintegrowany z ww. centralnym systemem monitoringu zasobów IT, który również powiadamia o ewentualnych problemach z samym modułem DIAG.

Obydwa systemy monitoringu umożliwiają ciągły centralny nadzór nad aplikacjami i niemal natychmiastową reakcję odpowiednich służb UR i IT na sytuacje awaryjne.

System dla międzynarodowej korporacji

Ważną funkcją 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.

Podsumowanie

Opisane rozwiązanie nie tylko wymaga współpracy UR z IT, ale także systemu SCADA spełniającego szereg wymagań, także tych nietypowych. Podsumujmy je:
- możliwość wirtualizacji serwerów i klientów SCADA,
- pełna redundancja serwerów danych,
- zdolność do pracy wielu różnych sesji SCADA na jednym serwerze RDS,
- możliwość pracy w wersji przeglądarkowej,
- system zabezpieczeń i zarządzania użytkownikami zintegrowany z usługą Active Directory,
- dobrze udokumentowany zestaw portów sieciowych i protokołów komunikacyjnych,
- wbudowany system backupu kluczowych danych,
- kompresja połączeń WAN i VPN między terminalami a serwerami,
- odporność na instalację bieżących łatek systemowych,
- wielojęzyczność aplikacji i praca w różnych strefach czasowych,
- monitoring, procedury postępowania na wypadek awarii i szczegółowa, aktualna dokumentacja.

Współpraca służb UR oraz IT przedsiębiorstwa z zespołem wdrożeniowym firmy ASKOM, a także z zespołem twórców systemu Asix, doprowadziła do powstania systemu spełniającego zarówno wysokie wymagania stawiane przez system zarządzania bezpieczeństwem informacji już na poziomie SCADA, a nawet PLC, jak i wymagania stawiane przez tradycyjnych użytkowników systemów SCADA, czyli operatorów, służby UR i kadrę zarządzającą.

Jak widać na przytoczonym przykładzie, możemy zacytować staropolskie przysłowie: „zgoda buduje, niezgoda rujnuje". Głęboka integracja i wola współpracy pomiędzy działami UR oraz IT pozwoliła nie tylko zoptymalizować procesy SCADA, ale również zaoszczędzić sporo pieniędzy na inwestycjach, podnieść jakość i dostępność systemu Asix na wyższy poziom, ułatwić czynności serwisowe pracownikom, a także zachować wysoką transparentność i czytelność funkcjonowania systemu.

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

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