Robert WÓJTOWICZ, Ryszard KOWALIK, Désiré D. RASOLOMAMPIONONA, Karol KUREK

Politechnika Warszawska, Instytut Elektroenergetyki

doi:10.15199/48.2017.05.02

Koncepcja wirtualizacji usług zabezpieczeniowych w stacjach elektroenergetycznych

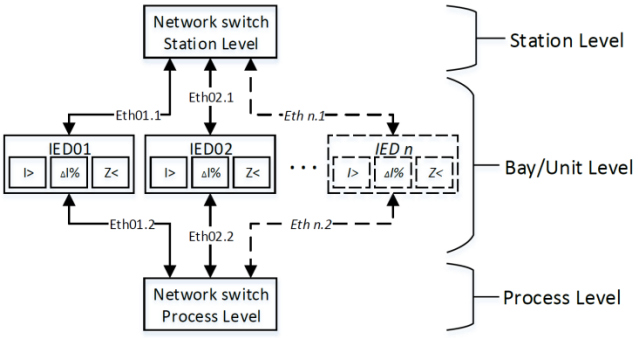
Streszczenie. *Artykuł opisuje koncepcję technologii wirtualizacji, które mogą posłużyć do stworzenia nowej generacji Inteligentnych Urządzeń Elektronicznych (IED). Przegląd koncepcji został oparty o rozwiązania informatyczne stosowane w konwencjonalnych systemach informatycznych. Poddano analizie rozwiązania platform witalizacyjnych firm VMware oraz Microsoft pod kierunkiem wykorzystania w urządzeniach IED.*

Abstract. *The article describes the concept of virtualization technology, which can be used to create a new generation of Intelligent Electronic Devices (IEDs). The presented overview of the concept was based on well-known virtualization concepts used in conventional systems. The VMware and Microsoft platforms are analyzed under their potential application for IEDs virtualization.* ***The concept of virtualization technology, which can be used to create a new generation of Intelligent Electronic Devices***

Słowa kluczowe: Wirtualizacja IED, Wirtualizacja IEC-61850, platforma VMware, Ethernet w IEC-61850, GOOSE, wirtualne maszyny.
Keywords: virtualization IED, virtualization IEC-61850, VMware platform

Wstęp

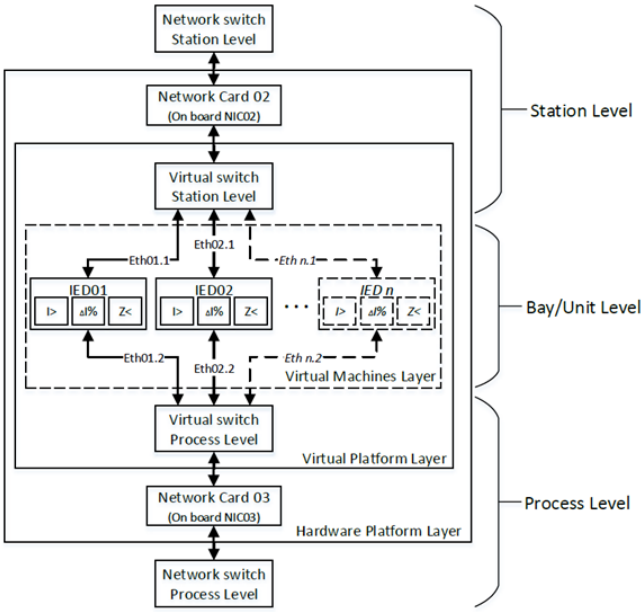
Odkąd technologia mikroprocesorowa oraz nowoczesne technologie cyfrowe weszły do systemów zabezpieczeniowych i kontroli w stacjach elektroenergetycznych, istotne zmiany zaczynają zachodzić lub już zaszły w pracy układów sterowania i zabezpieczeń stacji. Urządzenia IED (ang. *Intelligent Electronic Devices*) stopniowo zastępują tradycyjne przekaźniki zabezpieczeniowe, dotychczas pracujące jako samodzielne urządzenia zabezpieczeniowe. Urządzenia IED mają również kilka wbudowanych, nowych funkcji. Współpracują z licznikami inteligentnymi, sieciowymi przełącznikami sterującymi, starego typu przekaźnikami elektronicznymi, jak i mechanicznymi. Z racji kompleksowości nowych rozwiązań, w przypadku wystąpienia nieprawidłowej pracy urządzenia IED, jak nieudane wyłączenie danego ciągu zasilającego po wystąpieniu zwarcia lub przypadkowe wyłączenie zdrowej linii, konsekwencje mogą być fatalne dla systemu elektroenergetycznego, a nawet doprowadzić do katastrofalnych zdarzeń kaskadowych typu Black-out [1]. Doposażenie urządzeń IED w narzędzia umożliwiające bieżące diagnozowanie własnego stanu byłoby znaczącym dodatkiem w krytycznych miejscach systemu elektroenergetycznego, mogącym usprawnić jego pracę i zmniejszyć prawdopodobieństwo błędnych działań. Automatyka stacyjna, realizowana z wykorzystaniem inteligentnych urządzeń elektronicznych (IED) oraz technologii komunikacyjnych sieci, mogłaby ułatwić skuteczne monitorowanie, lokalną i zdalną kontrolę stacji, zabezpieczeń, bieżące monitorowanie stanu aparatury pierwotnej i wiele innych funkcji, które nie mogły być łatwo realizowane za pomocą konwencjonalnych urządzeń zabezpieczających lub/i sterowania. Aby rozwiązać problemy w wymianie informacji między urządzeniami IED w stacji, ze względu na stosowanie różnych urządzeń IED od różnych producentów, prace normalizacyjne dotyczące komunikacji urządzeń rozpoczęto w Stanach Zjednoczonych i Europie na początku lat 1990. Stowarzyszenia inżynierów IEEE oraz IEC zgodziły się współpracować i stworzyć wspólny standard dla komunikacji w stacjach elektroenergetycznych, o nazwie IEC-61850 [2]. Norma IEC-61850 odwzorowuje usługi i struktury danych w sieci Ethernet. Również zawiera definicję "profilu" protokołów, modele danych, modele abstrakcyjne definiujące usługi oraz wyjaśnienie, jak działa komunikacja między urządzeniami IED [3]. Usługi abstrakcyjne zdefiniowane w IEC-61850 można dopasować do wielu protokołów. Niektóre obecnie stosowane metody odwzorowania są następujące: MMS (ang. *Manufacturing Message Specification*) oraz GOOSE (ang. *Generic Object Oriented Substation Event*). Obsługa wiadomości GOOSE odbywa się w trybie multicast, w związku z tym nie można ich adresować w sieci globalnej WAN (*ang. Wide Area Network),* lecz sama adresacja musi być przeprowadzona jedynie wewnątrz sieci LAN (*ang. Local Area Network*). To niedociągnięcie stwarza problemy, gdy wiadomości muszą być przenoszone między stacjami. Proces wymiany danych odbywa się w sieci Ethernet, gdzie przekazywane są różne typy wiadomości, takich jak konfiguracja systemu, pomiary, dane z bieżącego monitoringu elementów systemu itp. Komunikaty dotyczące tych funkcji nie są czasowo krytyczne, w stosunku do wiadomości GOOSE, jednak ich ruch może mieć wpływ na opóźnienie wiadomości GOOSE. Dodatkowym problemem jest sam ruch w sieci, który okresami może być intensywny [4]. Ze względu na przekazywanie krytycznych lub/i mniej krytycznych wiadomości w tej samej sieci Ethernet, należy zaimplementować mechanizm planowania wymiany pakietów sieci Ethernet. Kilka systemów planowania pakietów, których celem jest kontrola przeciążeń w przełącznikach Ethernet, przedstawiono w [5].



Rys. 1. Uproszczony schemat blokowy tradycyjnej wymiany danych pomiędzy urządzeniami IED Legenda: *Eth - ang. Ethernet/Network Card* - karta sieciowa; ang. *Station Level* - poziom stacji; ang. *Bay/Unit level* - poziom urządzenia; *ang. Process Level* - poziom procesu,

Nowymi koncepcjami, o których coraz częściej się mówi jest technologia wirtualizacji i przetwarzanie w chmurze. Te dwie technologie otworzyły nową przestrzeń badawczą, którą specjaliści od technologii sieciowej zaczęli się interesować. Pomysł wykorzystania wirtualizacji i chmury jako podstawowej infrastruktury systemów

automatyki elektroenergetycznej po raz pierwszy zaprezentowano w artykule o IEC-61850 w "chmurze" [6]. Również autorzy [7] pokazali, jaki potencjał drzemie w rozwiązaniach wirtualnych oraz chmurze. W artykule [8] zespół pod przewodnictwem J.W. Konki przedstawił swoje podejście w sprawie generowania ruchu wartości próbkowanych SV. W tym artykule autorzy [8] przedstawili szczegółowy opis formatu pakietów SV i wynikający ruch podczas wysyłania takich pakietów. Korzyści płynące z wirtualizacji w nowoczesnej automatyce stacyjnej oraz próby przezwyciężenia wyzwań i ograniczeń związanych z wdrażaniem tych systemów w oparciu o aktualnie dostępne technologie opisano szczegółowo w [9].



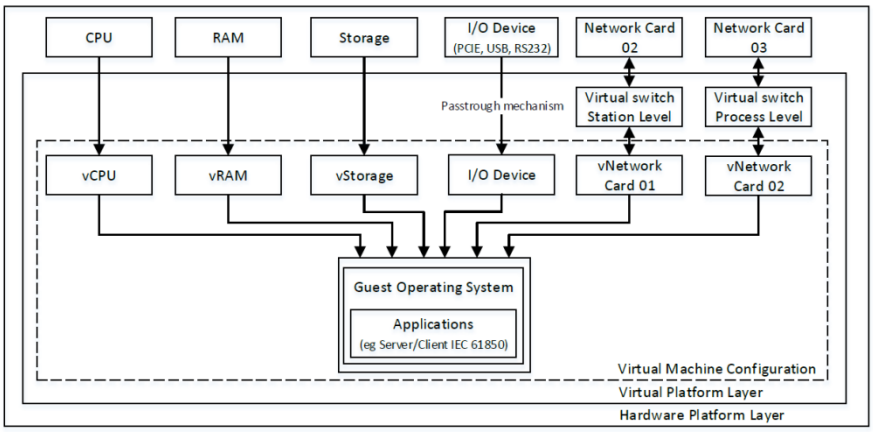
Rys. 2. Uproszczony schemat blokowy koncepcji wirtualnej wymiany danych pomiędzy urządzeniami IED

Niniejszy artykuł zawiera koncepcję wykorzystania wirtualizacji w dziedzinie automatyki zabezpieczeniowej. Przedstawiony jest w fazie koncepcji testowy system obsługi urządzeń zabezpieczeniowych, wykonywany na kilku systemach wirtualnych, modelujący kilka podstawowych zadań, w tym usługę serwerową i kliencką, opartą na normie IEC 61850. Jednym z możliwych testów przeprowadzonych w tym systemie jest wysyłanie i odbieranie pakietów GOOSE za pomocą uruchomienia usług wysyłania/odbierania pakietu na jednym serwerze fizycznym, obsługującym kilka serwerów wirtualnych.

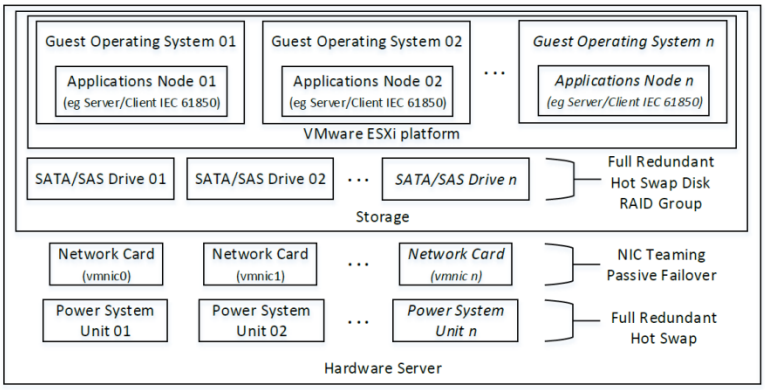
Koncepcja wirtualizacji urządzeń automatyki stacyjnej

Urządzenia IED (ang. Inteligent Electronic Device) w klasycznym ujęciu są rozwiązaniami sprzętowymi, modułami opartymi o systemy wbudowane SoC *(ang. System on a Chip)* z wykorzystaniem różnych wariacji architektury ARM i systemów operacyjnych Unix. Przesyłanie danych w protokole IEC-61850 odbywa się za pomocą sieci LAN wykonanej w standardzie Ethernet. Fizyczną komunikację (wymianę danych) pomiędzy urządzeniami IED zapewnia fizyczny przełącznik sieciowy *(ang. Network switch)*. Należy zaznaczyć, że każda z funkcji I>, ΔI%, Z< ma klika progów zadziałania. W ramach jednego pola pracuje kilka takich urządzeń. Stacja może być złożona z kilku lub kilkudziesięciu pól co daje w sumie liczbę kilkudziesięciu urządzeń IED i wielokrotnie większą liczbę funkcji zabezpieczeniowych, które są na nich uruchomione. Wykorzystany standard komunikacji umożliwia łączenie różnych urządzeń IEC-61850 z serwerami bazującymi na procesorach x86, wykorzystując do tego celu m.in. systemy operacyjne Microsoft Windows oraz różne dystrybucje systemu Linux. W niniejszym artykule została przedstawiona koncepcja wirtualizacji urządzeń IED (rys. 2), a dokładniej działających w nich funkcji. Dzięki takiemu podejściu koszty sprzętowe wynikające z liczby zastosowanych urządzeń do ochrony poszczególnych pól stacji są zoptymalizowane. Dzieje się tak ponieważ jak największa liczba funkcji zabezpieczeniowych i innych usług jest uruchamiana na najmniejszej, ale zapewniającej właściwy poziom bezpieczeństwa liczbie serwerów.

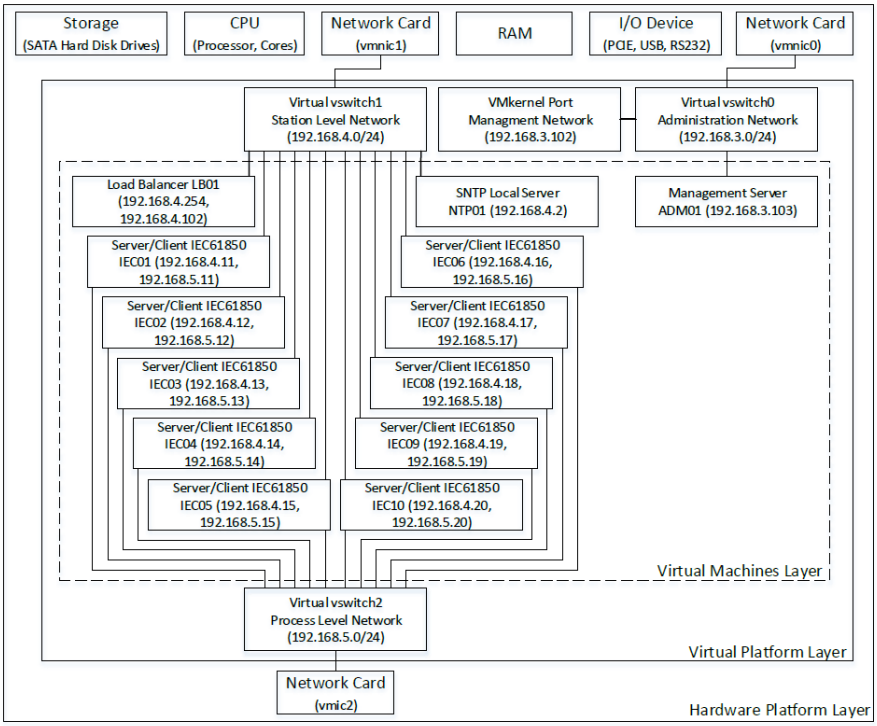
Wirtualizacja w tym przypadku polega na uruchomieniu wirtualnego systemu operacyjnego – warstwa wirtualnej maszyny *(ang. Virtual Machine Layer)* na dedykowanej platformie wirtualizacyjnej *(ang. Virtual Platform Layer),* która jest zainstalowana na fizycznym serwerze – warstwa sprzętowa *(ang. Hardware Platform Layer),* oraz uruchomienie oprogramowania pełniącego funkcje urządzenia IED. Komunikacja pomiędzy urządzeniami IED jest możliwa wewnętrznie dzięki wirtualnemu przełącznikowi *(ang. Virtual switch),* karcie fizycznej serwera *(ang. Network Card)* oraz fizycznego przełącznika *(ang. Network switch),* który pełni funkcję komunikacji z zewnętrznymi urządzeniami IED nie podlegającymi wirtualizacji. Współczesne serwery oparte o architekturę procesorów x86 posiadają bardzo dużą moc obliczeniową, często nie spożytkowaną gdy wykorzystuje się pojedynczy system operacyjny. Według firmy VMware przeciętne obciążenie zasobów nie przekracza 15%.



Rys. 3. Schemat blokowy, budowy logicznej serwera wirtualnego, przydzielanie zasobów sprzętowych



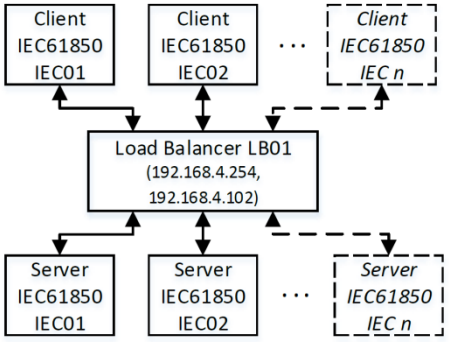
Rys. 4. Schemat obrazujący możliwości redundancji rozwiązania programowego i sprzętowego.



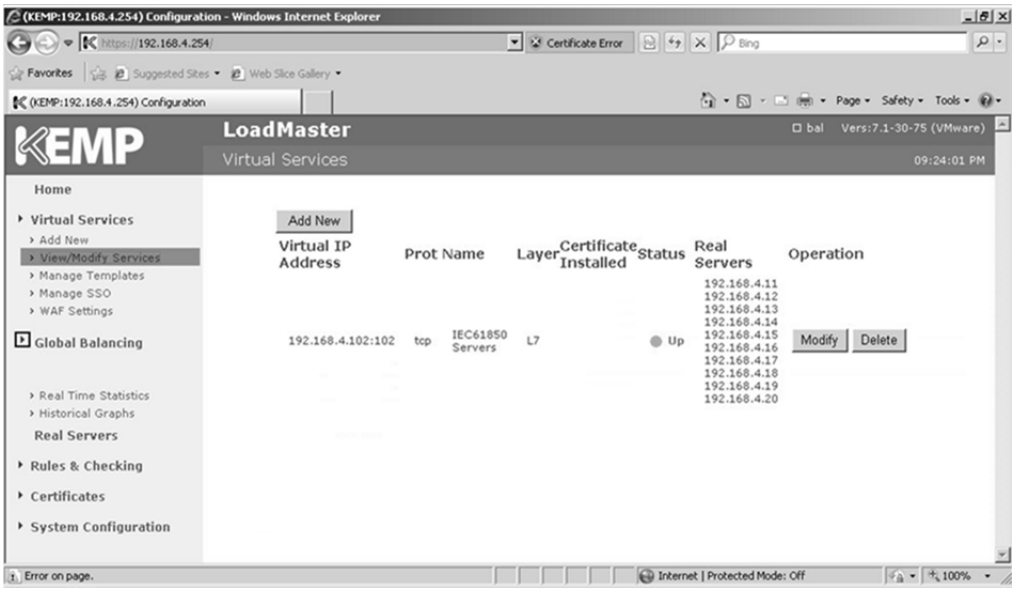
Rys. 5. Schemat blokowy planowanego środowiska laboratoryjnego oraz przeznaczenie serwerów wirtualnych. Zaznaczono połączenia sieciowe pomiędzy serwerami

Dodatkowym problemem wielu aplikacji jest to, że używają jedynie jednego lub dwóch rdzeni fizycznego procesora. W dobie wielordzeniowości najlepszym sposobem byłoby uruchomienie wielu systemów operacyjnych i przypisaniu rdzeni procesorów osobno w zależności od potrzeb oprogramowania. Wiele programów umożliwia uruchomienie jedynie jednej sesji aplikacji przez pojedynczy system operacyjny. W przypadku wirtualizacji problem jest rozwiązywalny poprzez postawienie kolejnej instancji systemu operacyjnego gościa w ramach jednego serwera fizycznego. Wirtualizacja serwerów umożliwia wykorzystanie w pełni potencjału zasobów serwera poprzez umożliwienie przypisania zasobów warstwy sprzętowej serwera do pojedynczych serwerów wirtualnych (rys. 3). Każdy serwer wirtualny posiada własną konfigurację *(ang. Virtual Machine Configuration)*, która składa się z przydzielonych zasobów serwera rzeczywistego – platformy sprzętowej *(ang. Hardware Platform Layer),* takich jak procesor CPU *(ang. Central Processing Unit*), ilość pamięci RAM *(ang. Random Access Memory)*, dysku twardego *(ang. Storage),* opcjonalnych urządzeń wejścia/wyjścia (I/O Device) oraz wirtualnej karty sieciowej *(ang. Network Card).* Zasoby sprzętowe są dynamicznie przydzielane maszynie wirtualnej, na której jest zainstalowany system operacyjny gościa *(ang. Guest Operating Systems)* i dedykowane oprogramowanie wspierające wymianę danych zgodnie z IEC-61850 *(ang. Applications)*. W efekcie na jednym fizycznym serwerze w zależności o zasobów sprzętowych możemy uruchomić kilka lub kilkadziesiąt serwerów wirtualnych obsługujących wiele aplikacji i łączyć je np. w klastry obliczeniowe. Każdy serwer wirtualny może też skorzystać z urządzeń wejścia/wyjścia, takich jak karty zbierania danych na PCI/PCI-E, USB oraz RS223. Inną ważną cechą przy tworzeniu środowiska laboratoryjnego jest wysoka elastyczność zarządzania wirtualnymi serwerami. Utworzenie kolejnych serwerów z przygotowanego szablonu zajmuje bardzo mało czasu i jest bardzo proste w użytkowaniu. Wirtualna maszyna składa się z 2 plików – pliku konfiguracji vmx oraz pliku dysku twardego vmdk. Gdy symulacje wymagają dużej ilości węzłów-serwerów wirtualizacja przynosi pełną automatyzację przy tworzeniu i utrzymaniu takiego środowiska.

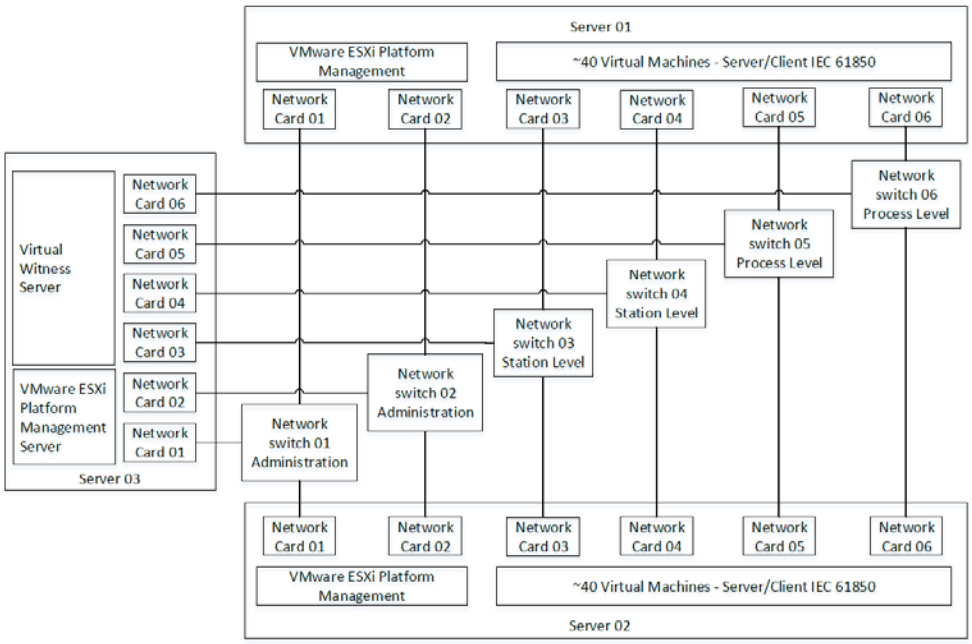
Niniejszy artykuł przedstawia dwie koncepcje systemu ograniczonego do dwóch platform wirtualizacyjnych: VMware ESXi v6 oraz Microsoft Windows Server 2012 R2 z usługą Hyper-V. Wykonane testy pozwoliły na wybór platformy wirtualizacyjnej VMware ESXi v6, która w lepiej wykorzystuje zasoby sprzętowe takie jak RAM (dynamiczne przydzielanie) i CPU oraz pobiera mniej zasobów sprzętowych niż Windows 2012 R2 z usługą Hyper-V. Ważną funkcją platformy wirtualizacyjnej jest bezpośrednia obsługa urządzeń wejścia/wyjścia oraz magistrali PCI/PCI-E serwera, której usługa Hyper-V nie posiada (możliwe jest jedynie przechwytywanie dysków przenośnych USB). Należy zaznaczyć, że platforma VMware ma również większy zakres konfiguracji wirtualnych maszyn niż produkt firmy Microsoft. W podstawowej konfiguracji VMware jest bezpłatny do celów naukowych jak i komercyjnych, natomiast w przypadku wykorzystania Hyper-V należy zakupić licencję na Microsoft Windows 2012 R2, który jest platformą komercyjną.



Rys 6. Uproszczony schemat komunikacji client <> load balancer <> serwer



Rys. 7. Widok panelu administracyjnego oprogramowania Free Load Balancera firmy KEMP



Rys. 8. Schemat blokowy teoretycznej konfiguracji środowiska docelowego, zapewniającej redundancję na poziomie serwerów wirtualnych i rzeczywistych

Redundancja sprzętowa serwerów x86

Nowoczesne serwery fizyczne mogą mieć sprzętową redundancję (rys. 4) m.in. takich podzespołów jak: zasilacze, dyski twarde (grupy RAID *ang. Redundant Array of Independent Disks - Nadmiarowa macierz niezależnych dysków*), karty sieciowe (grupowanie połączeń). Wirtualizacja daje swobodę, oddzielenie warstwy sprzętowej od programowej, każdy wirtualny serwer może być bezpiecznie przeniesiony na inny serwer fizyczny o zmienionej konfiguracji sprzętowej (jedynym warunkiem jest posiadanie CPU tego samego producenta). W przypadku awarii tradycyjne urządzenie IED należy wymienić, w przypadku urządzenia wirtualnego przy uszkodzeniu oprogramowania procedura sprowadza się do odtworzenia wirtualnego serwera.

Wirtualizacja sieci oraz budowanie wysokiej dostępności HA (ang. *High Availability*)

Platforma wirtualizacyjna VMware ESXi v6 zapewnia podejście kompleksowe nie tylko do zasobów sprzętowych serwera, udostępnia także uruchomienie wirtualizowanej sieci, która jest odwzorowaniem sieci fizycznej. Sieci wirtualne oferują te same funkcje i mogą zapewnić wysoką dostępność w ramach wirtualnej infrastruktury.

Środowisko koncepcyjne pokazane w formie blokowej na rys. 5 oraz odwzorowanie na platformie wirtulizacyjnej VMware ESXi v6 zostało podzielone na trzy części (podsieci):

- vswitch0 i sieć Administration;
- vswitch1 i sieć Station Level;
- vswitch2 i sieć Process Level.

Pierwsza cześć służy do zarządzania po sieci LAN infrastrukturą wirtualną (fizyczna karta sieciowa vmnic0), dzięki niej można dostać się do konsoli vSphere Client, SSH (*ang. Secure Shell*), oraz do dodatkowego serwera administracyjnego. Druga i trzecia część służy do komunikacji pomiędzy maszynami wirtualnymi oraz posiada dodatkowe połączenia na zewnątrz dla fizycznych urządzeń IED (fizyczna karta sieciowa vmnic1 oraz vmnic2). Dzięki segmentacji sieci (sieć Station Level oraz Process Level) można eksperymentować na wydzielonej grupie serwerów nie obciążając sieci administracyjnej. Ważne jest, aby w domyślnej konfiguracji przełącznika ustawić przepuszczanie wszystkich VLAN'ów (*ang. Virtual Local Area Network*), aby móc odbierać i wysyłać pakiety od wybranych aplikacji. Sieć o nazwie *Station* odpowiada logicznie komunikacji w IEC-61850 poziomowi stacji (centrum SSiN stacji, stanowisko prowadzenia ruchu, połączenia do centrów nadzoru, serwery SCADA, HMI, centralne urządzenia synchronizujące czas), natomiast sieć o nazwie *Process Level* odpowiada poziomowi procesu (zdalne I/O, czujniki, włączniki, wyłączniki, przekładniki). Do dyspozycji w konfiguracji wirtualnego serwera w wersji 11 dla systemów Windows 7 oraz Windows 2012 R2 są do wyboru karty sieciowe: emulator Intel PRO 1000 MT oraz natywną VMXNET3. Dodatkowym plusem korzystania z wirtualnych interfejsów sieciowych jest ich wysoka wydajność ponieważ zgodnie z specyfikacją pozwalają na przesyłanie danych z szybkością do 10 Gbitów. Dostęp do wirtualnych serwerów jest możliwy poprzez konsolę vSphere Client, która sięga bezpośrednio do platformy wirtualizacyjnej oraz zdalny pulpit. Nowoczesne systemy informatyczne są tak budowane by zapewnić wysoką dostępność oferowanych usług. Mechanizmy z jakich korzystają aplikacje można spróbować zaimplementować do oprogramowania obsługującego protokół IEC-61850. Aktualnie urządzenia IED nie posiadają takich mechanizmów i nie ma możliwości budowania redundancji na poziomie aplikacji. Sytuacja się zmienia, gdy wykona się wirtualizowanie urządzeń IED. W celu zapewnienia redundancji i równomiernego rozłożenia ruchu przy komunikacji zorientowanej połączeniowo klient/serwer np. do wysyłania raportów, rejestracji, zmiany nastawień itp. można użyć programu Load Balancera. Jego zadaniem jest równomierne rozłożenie ruchu np. do jednakowych serwerów (redundancja) od warstwy 4 do 7 modelu OSI (rys. 6). Zastosowany mechanizm jest prosty i polega na nawiązywaniu sesji pomiędzy klientem IEC-61850 a serwerem IEC-61850 poprzez program Load Balancer. Klient IEC-61850 łączy się pośrednio przez Load Balancer, który odpowiednim algorytmem przydziela sesję do serwera IEC-61850. Każda kolejna sesja jest przydzielana do następnego serwera IEC-61850, rozrzucając ruch równomiernie pomiędzy wirtualne maszyny. Podczas awarii serwera wirtualnego, *Load Balancer*, każdą kolejną lub aktualną sesję przekieruje do kolejnego serwera, minimalizując utratę danych. Na potrzeby koncepcji został skonfigurowany *Free Load Balancer* firmy KEMP (rys. 7).

Aby ruch przepływał w obie strony pomiędzy klientem a serwerem, brama sieciowa serwerów musi być ustawiona na wirtualny adres IP *Load Balancer*a. Klient łączy się do wirtualnego adresu IP *Load Balancer*a, brama IP klienta pozostaje dowolna w obrębie danej podsieci. W konfiguracji Load Balancera należy zwrócić uwagę na *„Idle Connection Timeout"* dla sesji i ustawić duży czas. Nawiązana sesja klient-serwer po odczytaniu danych nie jest aktywna dla Load Balancera, po przekroczeniu czasu parametru *„Idle Connection Timeout"* sesja zostanie rozłączona. Innym wyjściem z opisanej sytuacji jest cykliczne odpytywanie serwera tzw. „Heart Beat", tym samym podtrzymując sesję. Jest to naturalne zachowanie Load Balncera w celu zamykania nie aktywnych sesji. W przypadku komunikacji bezpołączeniowej urządzenia IED używają multicastów mac (warstwa 2-3 modelu OSI), w tym wypadku nie ma możliwości pośredniego balansowania ruchu za pomocą Load Balancera. Staje się problematyczna sytuacja, gdy trzeba stworzyć redundancję klienta lub serwera, w przypadku gdy grupa multicastowa odbierze pakiet danych, to zduplikowane (redundancja) funkcyjne serwery mogą wysłać podwójnie informację zwrotną, a taka sytuacja nie jest zawsze pożądana. Pozostaje dla powyższego przypadku rozpatrzyć implementację mechanizmu klastra trybu failover, w konfiguracji active-passive. Jeśli jeden lub kilka węzłów (serwerów klastrowanych) ulegnie awarii, pozostałe węzły rozpoczną udostępnianie usługi w ramach procesu nazywanego trybem failover.

Koncepcyjna konfiguracja zakłada (rys. 8) klaster dwuwęzłowy składający się z dwóch serwerów fizycznych (Server 01 i Server 02), każdy z nich będzie posiadał 50% aktywnych wirtualnych serwerów i 50 % pasywnych. Serwer 03 służy do zarządzania infrastrukturą wirtualną *(*ang. *Management Server)* oraz czuwaniem nad poprawną pracą trybu failover – serwer świadek *(*ang. *Witness Server).* Jego zadaniem jest cykliczne odpytywanie usług serwerów wirtualnych umieszczonych na serwerze 01 i serwerze 02. W przypadku gdy zostanie przekroczony zdefiniowany czas nieodstępności całego serwera wirtualnego lub jego usług zadaniem serwera świadka będzie wskazanie działającej kopii. Koncepcja sprowadza się do wyłączenia wirtualnej karty sieciowej, niedziałającej w pełni maszyny wirtualnej i włączenie karty sieciowej kopii pasywnej tego serwera znajdującej się na serwerze 01 lub 02. Docelowa konfiguracja ma posiadać pełną redundancję sprzętowa (serwery 1-2) oraz redundancję połączeń i urządzeń sieciowych. Rzeczywiste karty sieciowe będą pracowały grupami (*ang. Teaming*). Dzięki wbudowanemu w platformę VMware mechanizmowi NIC Teaming, fizyczne

karty sieciowe będą mogły dzielić obciążenie ruchu między sieciami fizycznymi i wirtualnymi wśród niektórych lub wszystkich urządzeń, jak również powinny zapewnić pasywny failover w przypadku awarii sprzętu lub awarii sieci.

Podsumowanie

Koncepcja oraz analiza zagadnienia wirtualizacji, pozwalają wysnuć tezę, że rozwiązania informatyczne stosowane obecnie w branży IT są możliwe do zaimplementowania w układach zabezpieczeń stacji elektroenergetycznych i realizując funkcje zabezpieczeń wszystkich pól, zapewniają podobny lub większy poziom niezawodności jak rozwiązania klasyczne składające się z dziesiątek niezależnych urządzeń zabezpieczeniowych IED.

Kolejnymi krokami, które będą realizowane w ramach sprawdzania przedstawionej powyżej koncepcji są: budowa fizyczna środowiska testowego oraz przeprowadzenie badań pozwalających na weryfikację funkcjonalności oraz działania urządzeń IED jako wirtualnych systemów z oprogramowaniem symulacyjnym.

***Autorzy**: mgr inż. Robert Wójtowicz, Politechnika Warszawska, Instytut Elektroenergetyki, ul. Koszykowa 75, Gmach Mechaniki, 00-662 Warszawa, e-mail: Robert.Wojtowicz@pw.edu.pl;*
dr inż. Ryszard Kowalik, Politechnika Warszawska, Instytut Elektroenergetyki, ul. Koszykowa 75, Gmach Mechaniki, 00-662 Warszawa, e-mail: Ryszard.Kowalik@ien.pw.edu.pl;
prof. nzw. dr hab. inż. Désiré Rasolomampionona, Politechnika Warszawska, Instytut Elektroenergetyki, ul. Koszykowa 75, Gmach Mechaniki, 00-662 Warszawa, E-mail: draso@pw.edu.pl;
mgr inż. Karol Kurek, Politechnika Warszawska, Instytut Elektroenergetyki, ul. Koszykowa 75, Gmach Mechaniki, 00-662 Warszawa, e-mail: karol.kurek@ien.pw.edu.pl.

LITERATURA

[1] Bertsch, J. et al., “Experiences with and perspectives of the system for wide area monitoring of power systems,” CIGRE/IEEE PES International Symposium, Quality and Security of Electric Power Delivery Systems, 8- 10 Oct. pp.5-9, 2003.
[2] U.-K. Premaratne, J. Samarabandu, T.-S. Sidhu, R. Beresh, and J.-C. Tan, “An Intrusion Detection System for IEC61850 Automated Substations,” IEEE Trans. Power Del., vol. 25, no. 4, pp. 2376-2383, Oct. 2010.
[3] B. Su, J. Fan, Y. Xu, “Application Summary of IEC61850 in Power System Protection voltage phasor oscillation at the relaying point,” 17th Conference of the Electric Power Supply Industry (CEPSI 2008), Macau SAR, Oct 27- Oct 31.
[4] T. S. Sidhu, M. G. Kanabar, P. P. Parikh, “Implementation Issues with IEC 61850 Based Substation Automation Systems,” in Proc. National Power Systems Conference (NPSC), IIT Bombay, Dec. 2008.
[5] B. Kasztenny, J. Whatley, E. A. Urden, J. Burger, D. Finney, M. Adamiak, “A Practical Application Primer For Protection Engineer,” Presented at 60th annual Georgia Tech Protective Relaying conference, May 2006
[6] Ferreira, R. D. F. et al. Cloud IEC 61850. PAC World Conference 2013, Dublin, Ireland. June 2013.
[7] Thiago Berticelli Lo; Marcos Fonseca Mendes; Hugo A. Larangeira Samaniego; Rômulo Silva de Oliveira, Cloud IEC 61850: Architecture and Integration of Electrical Automation Systems 2014 Brazilian Symposium on Computing Systems Engineering.
[8] J. W. Konka, C. M. Arthur, F. J. Garcia, R.C. Atkinson "Traffic generation of IEC-61850 sampled values", Pages 43-48, Smart Grid Modeling and Simulation (SGMS), 2011 IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS).
[9] S. Dayabhai, P. Diamandis "The role of virtualization in a smart-grid enabled substation automation system", Quadnet Computer Systems, Protection, Automation & Control World Africa Conference 2015, South Africa