ZESZYTY NAUKOWE
POLITECHNIKI RZESZOWSKIEJ

SCIENTIFIC LETTERS
OF RZESZOW UNIVERSITY OF TECHNOLOGY

NR 296

(e-ISSN 2300-6358)

ELEKTROTECHNIKA

Kwartalnik

tom XXV

zeszyt 36 (nr 2/2017)

lipiec-wrzesień

WYDZIAŁ
ELEKTROTECHNIKI
I INFORMATYKI
POLITECHNIKI RZESZOWSKIEJ

Wydano za zgodą Rektora

p-ISSN 0209-2662
e-ISSN 2300-6358

Wersja drukowana Zeszytu jest wersją pierwotną.

Redakcja czasopisma: Politechnika Rzeszowska, Wydział Elektrotechniki i Informatyki,
ul. W. Pola 2, 35-959 Rzeszów (e-mail: ziemba@prz.edu.pl)
http://oficyna.prz.edu.pl/pl/zeszyty-naukowe/elektrotechnika

Wydawca: Oficyna Wydawnicza Politechniki Rzeszowskiej
al. Powstańców Warszawy 12, 35-959 Rzeszów (e-mail:oficyna@prz.edu.pl)
http://oficyna.prz.edu.pl

Informacje dodatkowe – str. 79

SPIS TREŚCI

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (2/2017), lipiec-wrzesień 2017, s. 5-18

Mariusz GAMRACKI[1]

REJESTRACJE PIORUNOWEGO POLA ELEKTROMAGNETYCZNEGO PRZEZ STACJE SYSTEMU BLITZORTUNG

W pracy opisano możliwości jakie daje system detekcji i lokalizacji Blitzortung pod względem rejestracji przebiegów składowych pola elektromagnetycznego. Początkowe rozdziały opisują podstawy dotyczące działania tego typu systemów, zakresy częstotliwości stosowane przy detekcji wyładowań oraz najczęściej stosowane metody detekcji i lokalizacji wykorzystywane w takich systemach. Dalej opisano działanie systemu detekcji i lokalizacji wyładowań Blitzortung, jego funkcjonalność i rozmieszczenie stacji na świeci. Opisano jak działa system i jakiego typu sygnały są odbierane przez anteny stacji wchodzących w skład systemu. Porównano przebiegi odzwierciedlające składowe magnetyczną i elektryczną pola pochodzącego od wyładowania atmosferycznego. Omówiono parametry numeryczne zastosowane przy detekcji pola przez stacje systemu. Na wybranych przebiegach czasowych pokazano wpływ odległości pomiędzy wyładowaniem atmosferycznym, a stacją detekcji na kształt zarejestrowanych sygnałów pola elektromagnetycznego. Przebiegi porównano także pod względem metody detekcji i rodzaju anten odbierających sygnały pochodzenia piorunowego. W końcowej części pracy opisano możliwości wykorzystania danych z systemu do analizy porównawczej z wynikami symulacyjnymi, z eksperymentów i innych pomiarów.

Słowa kluczowe: wyładowanie atmosferyczne, system detekcji wyładowań, pole elektromagnetyczne, składowe magnetyczna i elektryczna

1. Wprowadzenie

Wyładowanie atmosferyczne jest zjawiskiem unikalnym i niepowtarzalnym i w zasadzie nie występują dwa identyczne wyładowania. Ze względu jednak na pewne wspólne cechy dotyczące kształtu prądów piorunowych można utworzyć grupę modeli, które charakteryzują poszczególne typy wyładowań. Prowadzone już od kilkudziesięciu lat pomiary i rejestracje zjawisk piorunowych doprowadziły do lepszego poznania kształtów składowych pola elektromagnetycznego powstającego podczas wyładowania atmosferycznego. Kształt fali piorunowej, dla każdego typu wyładowania został opisany w międzynarodowych normach, a w ostatnich latach powstała także norma dotycząca burzo-

[1] Mariusz Gamracki, Politechnika Rzeszowska, ul. W. Pola 2, 17-865-1298, mgamrac@prz.edu.pl

wych systemów ostrzegawczych [1]. Są tam dokładnie opisane kolejne fazy prądowe występujące podczas wyładowania atmosferycznego, a także zestawione podstawowe techniki używane podczas detekcji i lokalizacji wyładowań. Systemy detekcji podzielone zostały także na cztery klasy wykrywające poszczególne fazy zjawiska [1].

Spektrum częstotliwościowe pola elektromagnetycznego pochodzącego od wyładowania atmosferycznego jest bardzo szerokie. Zaczynając od ekstremalnie niskich częstotliwości (3Hz – 300Hz), poprzez bardzo niskie (ang. VLF - very low frequencies: 3 kHz – 30 kHz), częstotliwości niskie (ang. LF - low frequencies: 30 kHz – 300 kHz), częstotliwości średnie i wysokie aż do bardzo wysokich (ang. VHF - very high frequencies: 30 MHz – 300 MHz) i częstotliwości gigahercowych [1-3]. Tak bardzo duży zakres częstotliwości wynika ze specyfiki zjawiska, a stosowanie odpowiedniej techniki detekcji i związanym z nią przedziałem częstotliwości, w którym analizuje się sygnały, pozwala na pozyskanie informacji także o typie wyładowania: wyładowania doziemne, wewnątrz- i między-chmurowe, dodatnie i ujemne.

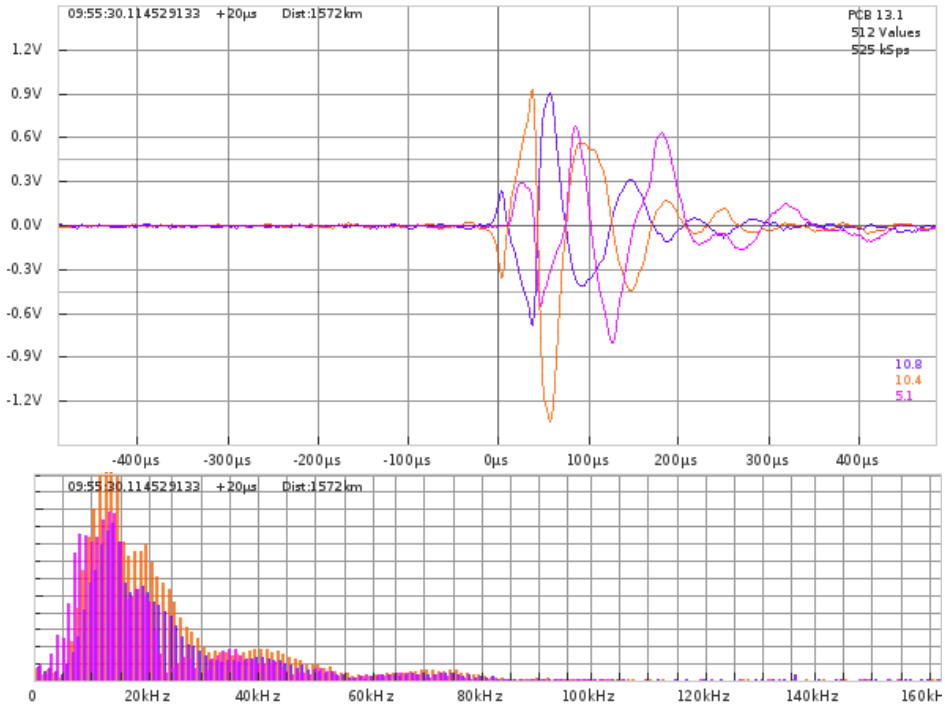
2. Rejestracje wyładowań atmosferycznych przez system Blitzortung

Stosowane obecnie techniki detekcji wyładowań atmosferycznych bazują najczęściej na analizie częstotliwości z zakresów VLF, LF i VHF [1, 2]. Techniki łączące dwa zakresy częstotliwości pozwalają znacznie poszerzyć możliwości detekcji względem metod opartych tylko na jednym zakresie, wymagają jednak zastosowania znacznie bardziej rozbudowanych systemów antenowych niż te stosowane przy analizie w jednym zakresie. Stosowany zakres częstotliwości determinuje zasięg detekcji i możliwość wykrywania określonego typu wyładowań. Największy zasięg detekcji sygnałów mają stacje pracujące na niskich i bardzo niskich częstotliwościach. Ich detekcja sięga nawet tysięcy kilometrów. Pole elektromagnetyczne z zakresów VLF i LF emitowane przez kanał piorunowy jest wyjątkowo silne dla wyładowań głównych doziemnych [2]. System Blitzortung [4] pracuje w zakresach VLF i LF, a zasięg detekcji pojedynczych stacji sięga 10 tyś. km. W wypadku dużego zagęszczenia stacji detekcji na danym obszarze, jak ma to miejsce np. na terenie Europy i USA, nie ma potrzeby wykorzystywania sygnałów zarejestrowanych w odległościach powyżej 5 tyś. km od danej stacji detekcji. Natomiast ze względu na małą ilość stacji, detekcja bez ograniczeń odległości ma miejsce na takich terenach jak Australia, Afryka, państwa dalekiego wschodu (Japonia, Korea Pd.)

Poszczególne stacje wyposażone są w różne typy anten i pracują przy różnych poziomach wzmocnienia w torach kanałów wzmacniaczy. Powoduje to, że rejestrowane sygnały mają różne amplitudy, nawet wtedy gdy wyładowanie zostało zarejestrowane w podobnej odległości od tych stacji. Okazuje się

jednak, że kształty sygnałów z wielu stacji detekcji są do siebie podobne. Różnice mogą występować jedynie w fazie (biegunowości) zarejestrowanych sygnałów ponieważ anteny „magnetyczne” poszczególnych stacji mogą być ustawione przeciwsobnie względem anten innych stacji - przeciwny kierunek nawinięcia uzwojeń lub podłączenia przewodów.

Na rysunku 1 pokazano sygnały zarejestrowane przez anteny stacji Rzeszow-Milocin dla bardzo silnego wyładowania, które miało miejsce w dniu 22 maja 2017 roku na terenie Turcji. Pomimo dużej odległości od miejsca wyładowania stacja zarejestrowała „czyste” sygnały, z małą ilością zakłóceń co widać przed chwilą czasu oznaczoną „0”. Na wykresie czasowym pokazane są trzy przebiegi. Dwa z nich pochodzą od anten składowej magnetycznej (kolory fioletowy i pomarańczowy) natomiast trzeci sygnał (trzeci w legendzie) został zarejestrowany przez antenę składowej elektrycznej (kolor różowy). Wykres poniżej przedstawia widmo częstotliwościowe dla zarejestrowanych sygnałów.

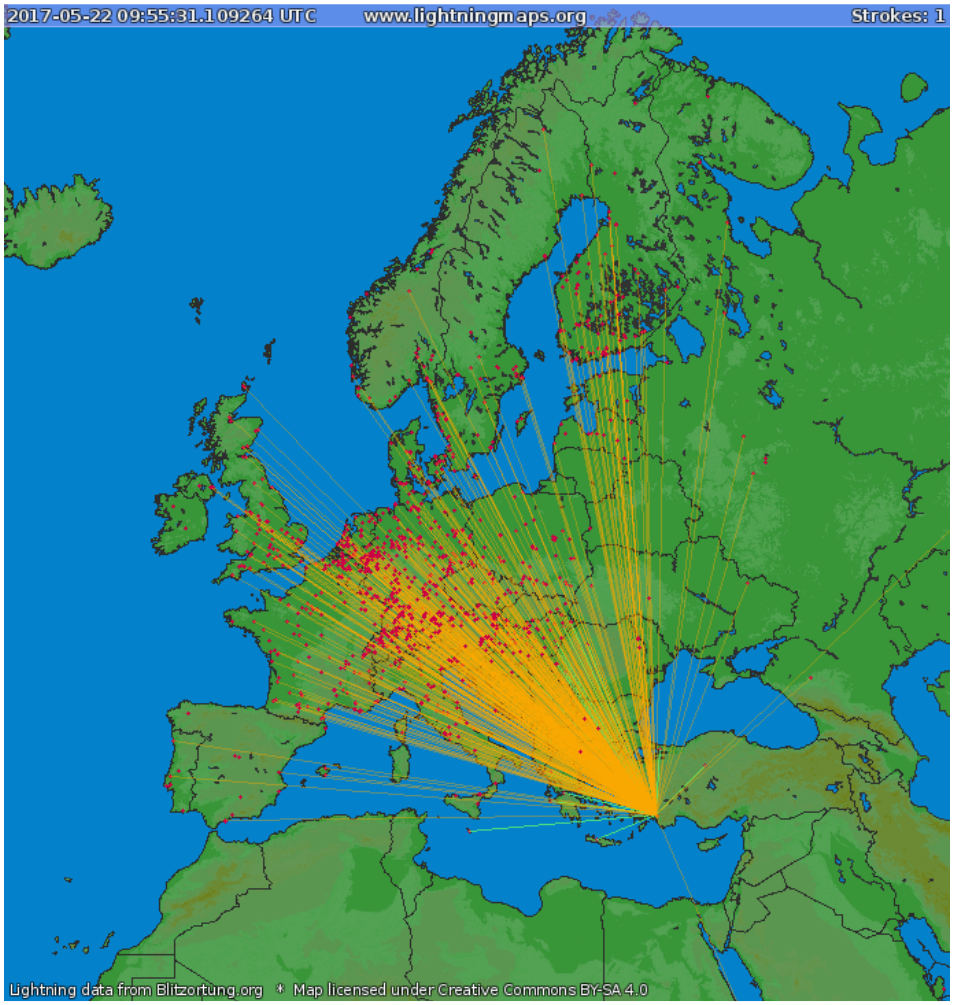


Rys. 1. Sygnały zarejestrowane przez stację Rzeszow-Milocin w Polsce

Fig. 1. Signals recorded by station Rzeszow-Milocin in Poland

Na rysunku 2 pokazano mapę Europy z zaznaczonym miejscem tego wyładowania w pobliżu Turcji, które nastąpiło 22 maja 2017 roku o godzinie

9:55:31 czasu UTC. Czerwone punkty na mapie oznaczają stacje detekcji. Naniesione linie łączą miejsce wyładowania ze stacjami, które zarejestrowały wyładowanie z czego kolorem zielonym oznaczono linie do tych stacji, z których dane posłużyły do wyznaczenia miejsca lokalizacji wyładowania. Zaznaczone wyładowanie zarejestrowało łącznie aż 530 stacji detekcji głównie na terenie Europy. W przypadku dużej liczby stacji, które zarejestrowały wyładowanie do wyznaczenia współrzędnych miejsca wyładowania używane są dane tylko maksymalnie z 24 stacji, przeważnie najbliższych miejsca wyładowania.



Rys. 2. Mapa ukazująca lokalizację wyładowania w pobliżu Turcji w dniu 22 V 2017 roku [4]

Fig. 2. Map showing the location of lightning nearby Turkey on May 22, 2017 [4]

Sygnały rejestrowane przez stacje systemu Blitzortung są odzwierciedleniem składowych pola elektromagnetycznego jakie dociera do stacji. Na wykresach widocznych w kontrolerze i prezentowanych na stronach internetowych systemu oś pionowa jest wyskalowana w woltach i reprezentuje wartości napięć sygnałów, jakie dotarły do kontrolera, a wcześniej wyindukowały się w antenach. Wartości tych napięć zależą od wielu czynników takich jak odległość stacji detekcji od wyładowania, rodzaju wyładowania, wartości prądu pioruna, typu i rodzaju zastosowanych anten ich orientacji oraz aktualnego poziomu wzmocnienia torów wzmacniaczy stacji detekcji jak również zastosowanych dodatkowych filtrów. Dla wyładowań bardzo odległych są to przeważnie ułamki wolta, natomiast dla bardzo bliskich sięgają nawet kilku woltów.

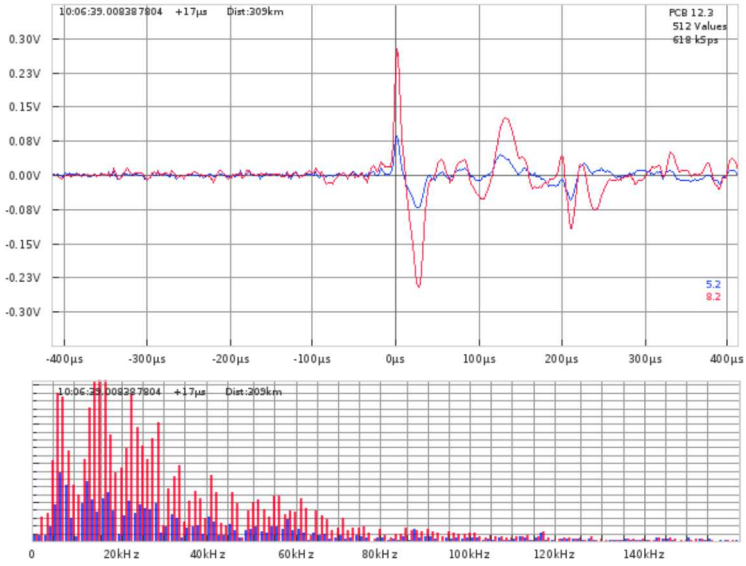
Na wykresach czasowych podane są także parametry dla zarejestrowanych sygnałów takie jak: dokładny czas UTC (z dokładnością do nanosekundy), odległość wyładowania od stacji w kilometrach, wielkości wzmocnień dla dwóch końcowych stopni wzmacniacza (oddzielone kropką) dla kanałów, które zarejestrowały wyładowanie, liczba próbek oraz częstość próbkowania sygnału. Dla systemu RED na wykresach mogą znaleźć się jednocześnie nawet 4 lub 5 zarejestrowanych sygnałów. Dwa pochodzą wtedy od anten rejestrujących składową magnetyczną pola i aż trzy dla składowej elektrycznej. W najnowszej wersji firmware można wyłączyć dowolne kanały i pozostawić np. dwa sygnały z anten składowej magnetycznej i tylko jeden z anteny składowej elektrycznej. Jest to dobre rozwiązanie ponieważ do serwerów wysyłanych jest mniej danych, a jakość detekcji w zasadzie nie zmniejsza się. System w wersji BLUE ma możliwość wysyłania już tylko jednego sygnału z anteny składowej elektrycznej. Wtedy to stacja wysyła maksymalnie 3 lub 4 sygnały, dwa lub trzy z anten składowej magnetycznej i jeden z anteny składowej elektrycznej.

Wzmacniacz składowej elektrycznej pola w wersji RED przepuszcza pojedynczy sygnał pochodzący z anteny „elektrycznej” przez równolegle połączone trzy filtry pasmowe generując w ten sposób trzy przebiegi. Zostało to tak opracowane ponieważ wersja RED była testową wersją dla zastosowanych filtrów dla anteny składowej elektrycznej, spośród których dla wersji BLUE wybrano jeden. Najnowsza wersja systemu BLUE używa tylko jednego kanału dla rejestracji składowej elektrycznej pola. Sygnał przechodzi przez odpowiednio zestawione wzmacniacze i filtry cyfrowe.

Stacje pracujące z systemem RED najczęściej wyposażone są tylko w jeden typ anten: składowej magnetycznej lub składowej elektrycznej, natomiast systemy BLUE mają już przeważnie dwa typy anten. W sytuacji, gdy poziom sygnału jest niski, może się tak zdarzyć, że stacja zarejestruje sygnał tylko z jednej anteny dlatego też najczęściej na wykresach można zaobserwować 1, 2 lub 3 przebiegi. Na wykresach sygnały rysowane są różnymi kolorami, standardowo przypisanymi do poszczególnych kanałów.

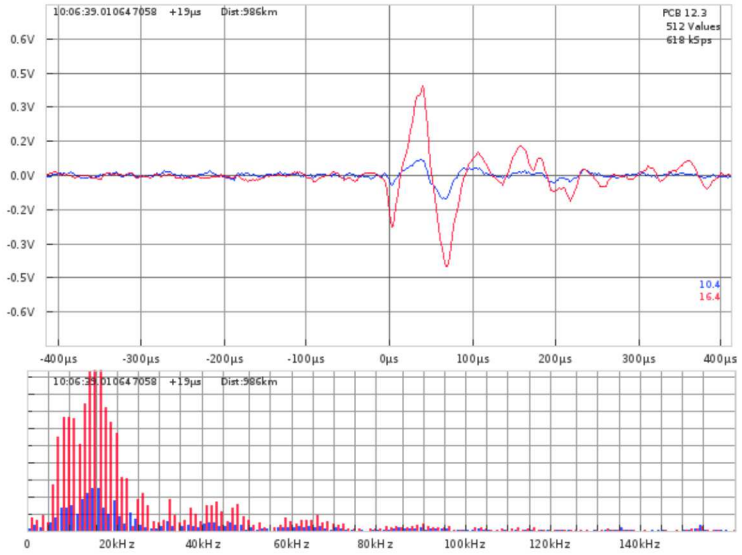
3. Rejestracje piorunowego pola elektromagnetycznego przez system Blitzortung

W tej części pracy przedstawiono przykładowe rejestracje wyładowania, które wystąpiło w pobliżu Grecji w dniu 10 października 2016 roku o godzinie 10:06:39 czasu UTC wykonane przez stacje systemu. Na rysunkach 3-16 przedstawiono rejestracje z wybranych stacji detekcji rozmieszczone na terenie Europy. Poszczególne rysunki przedstawiają przebiegi dla coraz większych odległości pomiędzy wyładowaniem, a stacjami rejestrującymi na rysunkach oznaczone jako „Dist:" i podane w kilometrach. Jak widać na przebiegach moment rejestracji wyładowania umiejscowiony jest na środku osi czasu. Widać wtedy także część przebiegów przed momentem wyładowania. Ma to czasami znaczenie, ponieważ można wtedy zauważyć zjawiska przed głównym wyładowaniem, które mają na tyle małą amplitudę, że nie spowodowałyby wyzwolenia rejestracji przez stacje detekcji. W kontrolerze można zmieniać ustawienia dotyczące zakresu rejestracji w tym także usytuowania punktu zerowego na osi czasu. Standardowa liczba próbek dla przebiegu to 512 i centralne umiejscowienie punktu zerowego. Częstość próbkowania dla takiego ustawienia wynosi 618 kSps (tysięcy próbek na sekundę) co odpowiada czasowi próbkowania 1,6 µs.



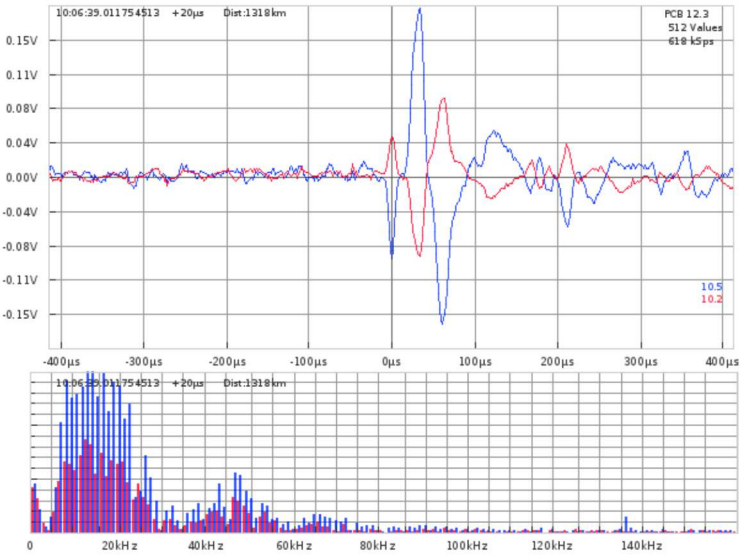
Rys. 3. Sygnały zarejestrowane przez anteny „magnetyczne" stacji Oinoi Viotias w Grecji oraz ich charakterystyki częstotliwościowe

Fig. 3. Signals from station Oinoi Viotias in Greece recorded by the "magnetic" antennas and their frequency characteristics



Rys. 4. Sygnały zarejestrowane przez anteny „magnetyczne” stacji Cluj-Napoca w Rumuni oraz ich charakterystyki częstotliwościowe

Fig. 4. Signals from station Cluj-Napoca in Romania recorded by the "magnetic" antennas and their frequency characteristics



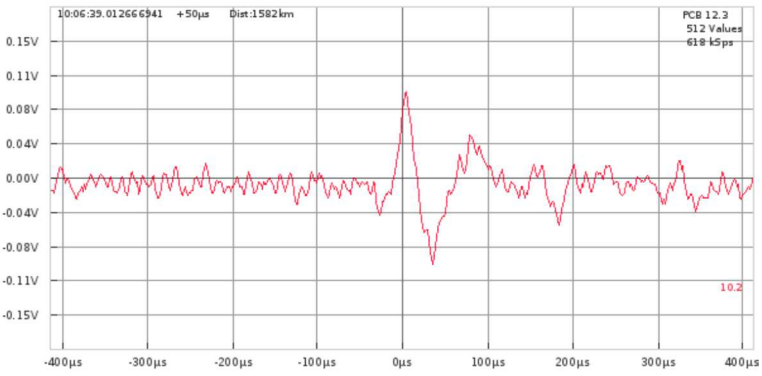
Rys. 5. Sygnały zarejestrowane przez anteny „magnetyczne” stacji Rzeszow-Milocin w Polsce oraz ich charakterystyki częstotliwościowe

Fig. 5. Signals from station Rzeszow-Milocin in Poland recorded by the "magnetic" antennas and their frequency characteristics

Na charakterystykach częstotliwościowych dołączonych do przebiegów na rysunkach 3-5 widać, że widmo sygnału dochodzi do 160 kHz. Ze względu jednak na zastosowane filtry, wysokie częstotliwości są mocno tłumione i użyteczna częstotliwość detekcji sięga ok. 50 kHz. Zagadnienia te mają duże znaczenie ponieważ pomagają we właściwym doborze parametrów numerycznych podczas modelowania matematycznego zjawisk piorunowych [5, 6].

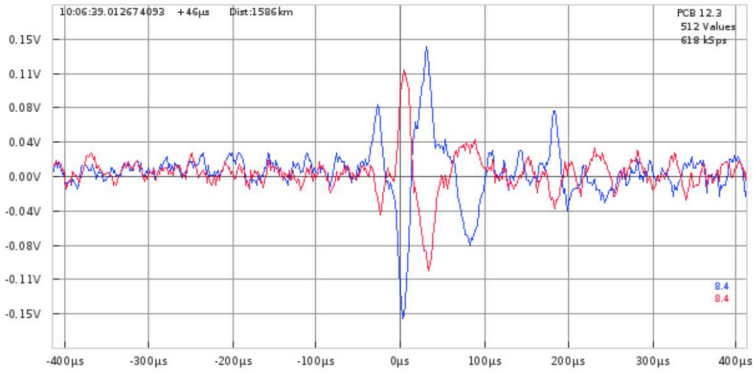
Ponieważ do anten stacji oprócz sygnałów pochodzenia piorunowego docierają także różnego rodzaju zaburzenia, dlatego też na sygnały piorunowe nakładają się powstające zakłócenia. Wielkość tych zakłóceń zależy przeważnie od „zaszumienia" elektromagnetycznego w pobliżu stacji, ale także od całkowitego wzmocnienia w torach wzmacniaczy. Dla silnego sygnału (np. przy bliskim wyładowaniu) ustawione wzmocnienie dla kanałów wzmacniaczy może być małe co skutkuje małym poziomem zakłóceń. Dla słabego sygnału wzmocnienie musi być większe ponieważ stacja nie zarejestrowała by takiego sygnału.

Sygnały pokazane na rysunkach 3 i 4 są mało zaszumione co wynika z niezbyt dużej odległości wyładowania od tych stacji. Pomimo znacznie mniejszej odległości stacji od wyładowania wartość maksymalna sygnału na wykresie z rysunku 3 wynosi 0,28 V i jest mniejsza od wartości max. napięcia na rysunku 4 gdzie wartość ta dochodzi do ok. 0,45 V. Stało się tak, ponieważ wzmocnienie w kanałach (przebiegi czerwone) wzmacniacza stacji rejestrującej sygnał na rysunku 4 wynosi $16 \cdot 4 = 64$ razy, a wzmocnienie sygnału z rysunku 3 tylko $8 \cdot 2 = 16$ razy. Sygnały na rysunku 4 są względnie najmniej zaszumione ze wszystkich tu zamieszczonych choć wartość bezwzględna szumów jest dość duża. Przebiegi na rys. 5 mają podobny poziom zakłóceń jak na rysunkach 3 i 4 jednak ze względu na znacznie mniejszą amplitudę sygnału na rysunku 5, szumy są tu bardziej widoczne. Na rysunkach 6 i 7 można zauważyć, że zakłócenia przed wyładowaniem są na podobnym poziomie i wynoszą średnio ok. ±0,02 V.



Rys. 6. Sygnał zarejestrowany przez antenę „magnetyczną" stacji Lübbenau w Niemczech

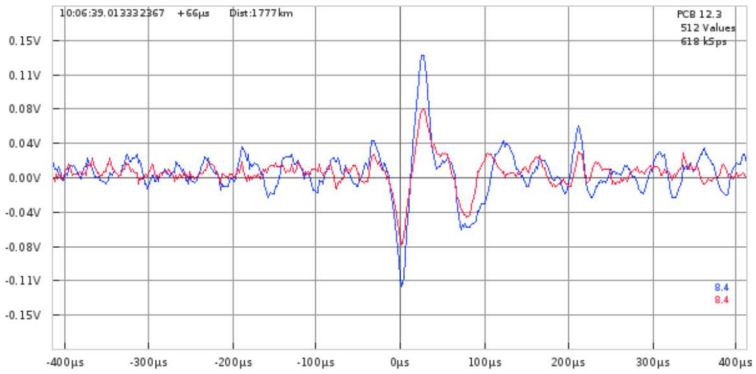
Fig. 6. Signal from station Lübbenau in Deutschland recorded by the "magnetic" antenna



Rys. 7. Sygnały zarejestrowane przez anteny „magnetyczne” stacji Poznan w Polsce

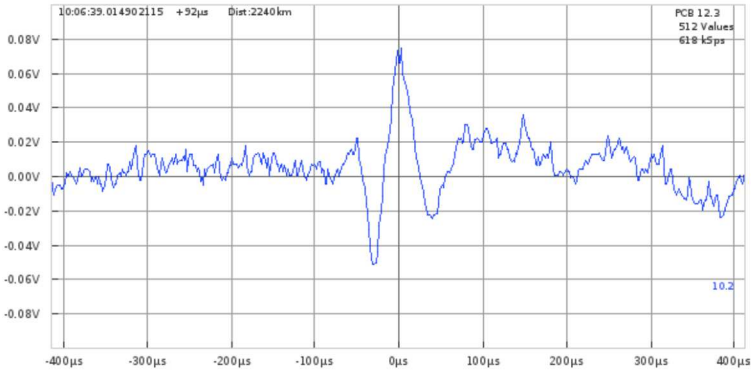
Fig. 7. Signals from station Poznan in Poland recorded by the "magnetic" antennas

Na rysunkach 5 i 7 można zauważyć podobieństwo kształtów przebiegów. Sygnały są trochę przesunięte w czasie, występuje różnica w poziomach zakłóceń, a przebiegi są „odwrócone”. Na rysunkach 8-10 widać duży poziom zakłóceń nakładających się na sygnały piorunowe. Najmniejszą amplitudę sygnału można zaobserwować na rysunku 9. Pomimo tak małej jej wartości sygnał został zarejestrowany ponieważ napięcie sygnału przekroczyło poziom wyzwalania („trigerowania”). Największy względny poziom zakłóceń występuje na przebiegu z rysunku 10. Jest to już skrajny przypadek rejestracji o bardzo małej wartości poznawczej. Stacja rejestrująca jest położona w odległości aż 2917 km od miejsca wyładowania. Największe odległości z jakich zostały zarejestrowane sygnały dochodzą do 10 tysięcy kilometrów. Np. stacja Rzeszów-Miłocin zarejestrowała pojedyncze wyładowania w Brazylii, a także w Afryce południowej.



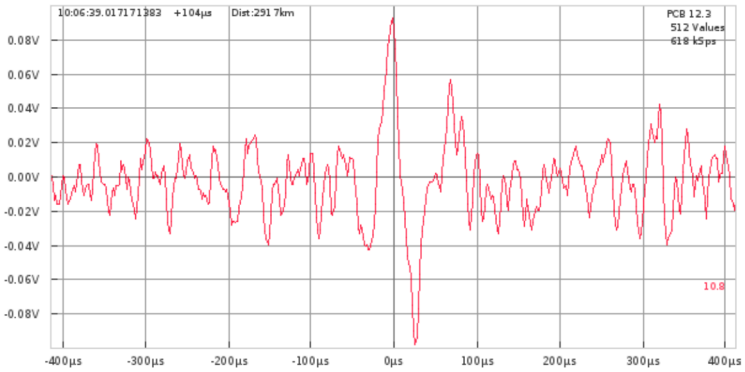
Rys. 8. Sygnały zarejestrowane przez anteny „magnetyczne” stacji Oberhausen w Niemczech

Fig. 8. Signals from station Oberhausen in Deutschland recorded by the "magnetic" antennas



Rys. 9. Sygnał zarejestrowany przez antenę „magnetyczną” stacji Lerum w Szwecji

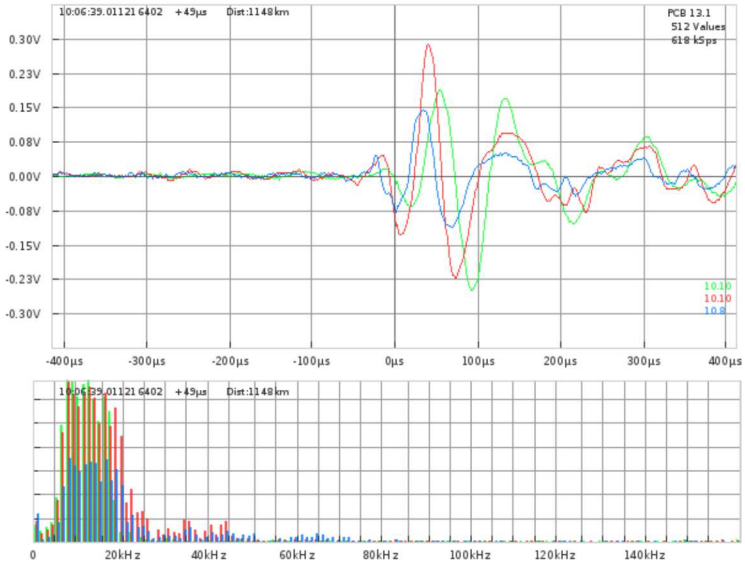
Fig. 9. Signal from station Lerum in Sweden recorded by the "magnetic" antenna



Rys. 10. Sygnał zarejestrowany przez antenę „magnetyczną” stacji Steinkjer w Norwegii

Fig. 10. Signal from station Steinkjer in Norway recorded by the "magnetic" antenna

Na rysunku 11 przedstawiono rejestrację tego samego wyładowania jednak za pomocą anteny rejestrującej składową elektryczną pola. Pomimo dość dużej odległości wyładowania od stacji rejestrującej poziom zakłóceń jest dość mały. Na rysunku widać odmienny kształt przebiegów względem tych z rysunków od 3 do 10. Rejestracja jest ze stacji pracującej z kontrolerem typu RED, który z jednej anteny generuje trzy przebiegi przechodzące przez trzy różne filtry pasmowe. Antena do detekcji składowej elektrycznej musi być umieszczone w lokalizacji o małym „zaszumieniu” elektromagnetycznym, najlepiej za zewnątrz budynku (np. na dachu) lub na wysokim maszcie. Oddalenie anteny od innych urządzeń elektrycznych powoduje, że uzyskiwane z niej sygnały są bardzo mało zaszumione. Systemów pracujących z użyciem anten składowej elektrycznej jest na razie niewiele, większość to systemy z antenami składowej magnetycznej (pętlowe i ferrytowe). W ostatnim roku proporcja ta jednak się zmienia.

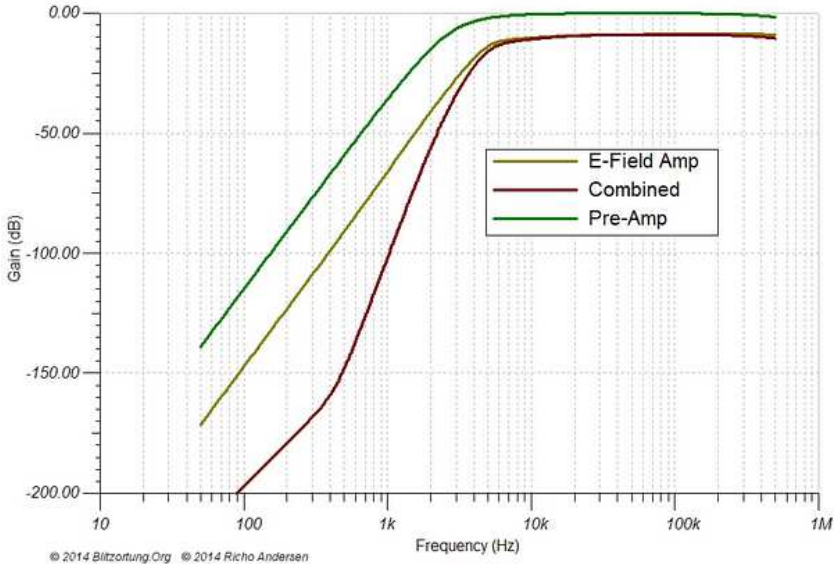


Rys. 11. Sygnały zarejestrowane przez antenę „elektryczną” stacji Monte Penice we Włoszech

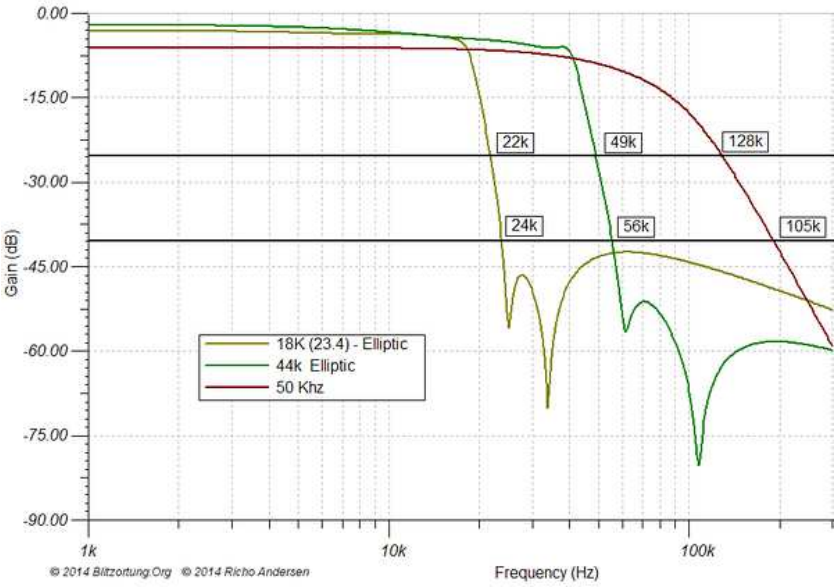
Fig. 11. Signals from station Monte Penice in Italy recorded by the "electric" antenna

Wiele sygnałów rejestrowanych przez stacje systemu, pomimo, że są pochodzenia piorunowego, są odrzucane przez serwery ponieważ nie ma dla nich odpowiedników w sygnałach od wymaganej liczby z innych stacji detekcji. Sytuacja taka występuje bardzo często co powoduje wyraźny wzrost liczby sygnałów, które nie są brane pod uwagę podczas lokalizacji wyładowań. Najwięcej jednak „fałszywych” sygnałów jest pochodzenia lokalnego. Są to różnego rodzaju zakłócenia od urządzeń elektrycznych pracujących w pobliżu. Podobnie dużym problemem są wojskowe stacje nadawcze pracujące na bardzo niskich częstotliwościach, które nawet z odległości kilkudziesięciu czy nawet kilkuset kilometrów mogą powodować poważne zakłócenia.

Na rysunkach 12 i 13 pokazano charakterystyki częstotliwościowe dla torów wzmacniaczy składowej elektrycznej kontrolera w wersji RED. Charakterystyka z rysunku 12 dotyczy dolnego pasma częstotliwościowego. Zamieszczone trzy wykresy dotyczą odpowiednio samego wzmacniacza E-pola (E-Field Amp), samego przedwzmacniacza E-pola (Pre-Amp) i sumy działania całego toru wzmacniaczy składowej elektrycznej pola. Na wykresie można zauważyć, że dolne pasmo przepustowe dla wzmacniaczy zaczyna się od ok. 5 kHz przy czym największe tłumienie wnosi główny wzmacniacz E-pola. Charakterystyka z rysunku 13 pokazuje natomiast tłumienie dla trzech torów wzmacniacza składowej elektrycznej zastosowanego w systemie RED. Główna różnica występuje w górnych częstotliwościach dla poszczególnych torów. Dla wzmocnienia -5dB częstotliwości te wynoszą odpowiednio 18 kHz, 44 kHz i 50 kHz.



Rys. 12. Charakterystyki częstotliwościowe tłumienia wzmacniaczy składowej elektrycznej [4]
Fig. 12. Frequency characteristics of attenuation of electrical component amplifiers [4]



Rys. 13. Górne graniczne częstotliwości trzech torów wzmacniacza składowej elektrycznej [4]
Fig. 13. The upper frequency limit (high-pass filter) of three tracks of electric amplifier [4]

4. Wnioski

Praca jest kontynuacją publikacji [7], gdzie opisano budowę i działanie systemu. Przedstawione przykłady rejestracji pola elektromagnetycznego pokazują możliwości jakie daje system Blitzortung w zastosowaniu do detekcji piorunowego pola elektromagnetycznego. System Blitzortung oprócz swoich podstawowych funkcji związanych z lokalizacją wyładowań umożliwiają wykorzystanie danych z detekcji do analizy czasowej i częstotliwościowej zarejestrowanych sygnałów. Duża ilość rejestracji wymaga jednak odpowiedniej selekcji danych w celu uzyskania przydatnych wyników. Profesjonalne systemy detekcji i lokalizacji wyładowań pracujące na wysokich i bardzo wysokich częstotliwościach (HF, VHF) dają możliwość bardzo dokładnej analizy czasowej przebiegów jednak zasięg detekcji stacji VHF jest nieduży i dochodzi jedynie do kilkudziesięciu kilometrów [1, 2]. System Blitzortung pracując na niskich częstotliwościach nie dostarcza precyzyjnych informacji np. o kształcie przebiegów, ale duży zasięg detekcji pozwala na uzyskanie danych ze stacji rejestrujących położonych w różnych odległościach od miejsca wyładowania. Dodatkową korzyścią dla systemów VLF i LF jest możliwość rejestracji sygnałów w stosunkowo długim czasie, gdyż próbkowanie na poziomie 1-2 ms nie generuje nadmiernej ilości danych. Duża ilość stacji detekcji systemu Blitzortung pozwala uzyskać także dużą liczbę rejestracji dla pojedynczego wyładowania piorunowego i to zarówno dla małych jak i dużych odległości pomiędzy wyładowaniem, a stacja rejestrującą. Uzyskane informacje mogą być wartościowym uzupełnieniem podczas analizy danych z profesjonalnych systemów detekcji [8, 9], danych pomiarowych w układach rzeczywistych [10] jak również przy modelowaniu matematycznym zjawisk propagacji pola elektromagnetycznego [11-13].

Literatura

[1] PN-EN 50536. Ochrona przed piorunami – burzowy system ostrzegawczy (2011).
[2] Bodzak P.: Detekcja i lokalizacja wyładowań atmosferycznych, Warszawa 2006, http://www.imgw.pl (2017).
[3] Gamracki M.: Modelowanie matematyczne piorunowych zaburzeń elektromagnetycznych w liniach transmisyjnych, praca doktorska, Politechnika Rzeszowska, Wydział Elektrotechniki i Informatyki, 2004.
[4] Egon Wanke, Richo Andersen, Tobias Volgnandt: World-Wide Low-Cost Community-Based Time-of-Arrival Lightning Detection and Lightning Location Network, 2016, http://www.blitzortung.org.
[5] Bajorek J., Gamracki M.: Effectiveness of mathematical modeling of lightning coupling to overhead conductors, International Conference on Lightning Protection, Kraków, 2002, pp. 208-213.
[6] Bajorek J., Gamracki M., Maslowski G.: Effectiveness of FFT-IFFT transformation during calculation of the electrical pulse underground surface, Proc. 28th Int. Conf. on Lightning Protection, Kanazawa, Japan, 2006, pp. 501-506.

[7] Gamracki M.: Budowa i działanie systemu detekcji i lokalizacji wyładowań atmosferycznych Blitzortung, Zeszyty Naukowe Politechniki Rzeszowskiej 296, Elektrotechnika 36, nr 1/2017, s. 27-40, p-ISSN 0209-2662, e-ISSN 2300-6358.
[8] Karnas G., Masłowski G.: Preliminary measurements and analysis of lightning electric field recorded at the observation station in the South-east part of Poland, Przegląd Elektrotechniczny, nr 7/2014, s. 97-99, ISSN 0033-2097.
[9] Karnas G., Masłowski G. Barański P.: Power Spectrum Density Analysis of Intra-Cloud Lightning Discharge Components from Electric Field Recordings in Poland, 33rd International Conference on Lightning Protection, Estoril, Portugal, 2016.
[10] Haddad M.A., Rakov V.A., Cummer S.A.: New measurements of lightning electric field in Florida: Waveform characteristics, interaction with the ionosphere, and peak current estimates, Journal of Geophysical Research, vol. 117, 2012, pp. 1-26.
[11] Gamracki M.: Modelowanie matematyczne propagacji piorunowego zaburzenia elektromagnetycznego nad ziemią, Przegląd Elektrotechniczny, nr 2/2012, s. 23-25, ISSN 0033-2097.
[12] Gamracki M.: Modelowanie propagacji piorunowego zaburzenia elektromagnetycznego nad stratną ziemią, Przegląd Elektrotechniczny, nr 7/2014, s. 171-174, ISSN 0033-2097.
[13] Bajorek J., Gamracki M., Maslowski G.: Modeling of lightning electromagnetic disturbances transmitted into the ground. Proc. XVI International Conference on Electromagnetic Disturbances, Kaunas, Lithuania, 2006, pp. 1132-1137.

REGISTRATION THE LIGHTNING ELECTROMAGNETIC FIELD BY THE STATIONS OF BLITZORTUNG SYSTEM

S u m m a r y

The paper describes the possibilities offered by Blitzortung's detection and location system for recording electromagnetic field components. The initial chapters describe the basics for the operation of such systems, the frequency bands used for lightning detection, and the most common detection and location methods used in such systems. Then describes the operation of Blitzortung detection and location system, its functionality and its location the stations. Describes how the system works and what kind of signals are received by the antenna of the system stations. The magnetic and electric fields from the atmospheric discharge were also compared. The numerical parameters used for field detection by the system stations are discussed. On selected waveforms the effect of the distance between the lightning discharge and the detection station in the shape of the recorded electromagnetic field signals is shown. The waveforms were also compared in terms of the detection method and the type of antennas that received signals of lightning origin. The final part of the paper describes the possibilities of using data from the system for comparative analysis with simulation results, experiments and other measurements.

Keywords: Lightning discharge, lightning detection system, electromagnetic field, magnetic and electrical components

DOI: 10.7862/re.2017.7

Tekst złożono w redakcji: wrzesień 2017
Przyjęto do druku: październik 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (2/2017), lipiec-wrzesień 2017, s. 19-28

Marcin DEREŃ[1]

STANOWISKO SYMULACYJNE DO BADANIA GŁOWIC OPTOELEKTRONICZNYCH

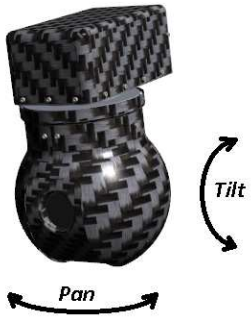
Latające platformy bezzałogowe (UAV) znajdują obecnie coraz więcej zastosowań zarówno militarnych jak i cywilnych. Jednym z częściej wykonywanych zadań jest szeroko rozumiana obserwacja. Podczas jej prowadzenia wykorzystuje się różnego rodzaju sensory, często w postaci głowic optoelektronicznych – kamer umieszczonych w układzie mechatronicznym, umożliwiającym zmianę orientacji sensora (kamery) względem nosiciela. Projektując algorytmy sterowania głowicy optoelektronicznej należy uwzględnić szereg parametrów związanych nie tylko bezpośrednio z konstrukcją tej głowicy, ale również z warunkami jej pracy i możliwościami nosiciela. W artykule przedstawiono podstawowe informacje o głowicach optoelektronicznych, ze szczególnym uwzględnieniem głowicy dwuosiowej, prze-znaczonej do instalacji na pokładzie platformy bezzałogowej. Przedstawiono stanowisko do badań symulacyjnych głowic optoelektronicznych, zrealizowane z wy-korzystaniem pakietu Matlab/Simulink. Umożliwia ono badanie algorytmów sterowania poprzez symulację zachowań nosiciela. Stanowisko umożliwia zadawanie parametrów na podstawie wcześniej zarejestrowanych rzeczywistych lotów platformy bezzałogowej, jak również stosowanie sztucznych, niespotykanych w locie wymuszeń.

Słowa kluczowe: głowica obserwacyjna, gimbal, UAV, stabilizacja,symulacja

1. Głowica optoelektroniczna

Jednym z najczęściej stosowanych rozwiązań wykorzystywanych do zadań szeroko pojętej obserwacji są głowice optoelektroniczne, określane potocznie mianem gimbali. Głowica taka to kamera, lub zestaw kilku kamer umieszczonych na mechanicznej platformie umożliwiającej obrót sensora względem podstawy. Głowice projektuje się przyjmując odpowiednie założenia, co do ich przyszłego wykorzystania, uwzględniając również możliwości nosiciela (platformy bezzałogowej). Należy uwzględnić nie tylko gabaryty platformy (wpływające na wielkość głowicy, a tym samym możliwości zastosowania sensorów) ale również jej zdolności manewrowe, a nawet rodzaje planowanych misji.

[1] Marcin Dereń, Eurotech sp. z o.o. 39-300 Mielec, ul. Strefowa 3, m.deren@eurotech.com.pl



Rys. 1. Kierunki obrotów dwuosiowej głowicy obserwacyjnej
Fig. 1. Rotation directions of two-axis gimbal

Jednym z podstawowych rozwiązań są głowice z dwiema osiami obrotu (rys. 1): w osi azymutu (nazywanej *pan*) oraz osi elewacji (nazywanej *tilt*) z przynajmniej jedną kamerą z możliwością przybliżania obrazu (*zoom*). Rozwiązanie takie jest stosunkowo prostym a jednocześnie uniwersalnym, zapewniającym szerokie spektrum możliwych realizacji działań. Większość oferowanych układów sterowania dla platform bezzałogowych przewiduje w swej transmisji sterowanie przynajmniej tymi trzema wielkościami. Dotyczy to również standardów militarnych [1].

2. Sterowanie i podstawowe tryby pracy głowicy dwuosiowej

2.1. Sterowanie głowicą optoelektroniczną

Sterowanie głowicą optoelektroniczną możemy rozpatrywać na dwóch poziomach.

Na poziomie niższym mówimy o sterowaniu poszczególnymi napędami, z uwzględnieniem dynamiki silników oraz zastosowanych przekładni. Rozpatrujemy wtedy głowicę jako zespół napędów, lub nawet serwomechanizmów zdolnych zapewnić odpowiedni ruch w wybranych osiach głowicy. Zapewnić należy odpowiednie sygnały sterujące, zależne od zastosowanych silników (np. PWM, dla silników DC, odpowiednia częstotliwość kroków dla silników krokowych), oraz pożądanych parametrów pracy – najczęściej uzyskania odpowiednich prędkości kątowych, lub dokładności pozycji danej osi.

Na poziomie wyższym nie zajmujemy się sterowaniem silnikami a sterowaniem wektora LOS (Line of Sight) – wektora kierunku „patrzenia" głowicy. Tu, w zależności od rodzaju sterowania, istotna staje się orientacja sensora względem podstawy (nosiciela) oraz względem nieruchomego układu związanego z ziemią. Na tym poziomie wypracowywane są wartości zadawane sterowań dla poziomu niższego, tak by utrzymać, lub uzyskać odpowiednie ukieru-

kowanie wektora LOS. Można tu rozpatrywać różne tryby pracy głowic (punkt 2.2)

Równolegle do tych dwóch poziomów sterowania możemy wyróżnić również sterowanie zainstalowanym sensorem, które wpływa pośrednio na parametry algorytmów sterowania (np. poprzez modyfikację prędkości obrotowych głowicy, w zależności od aktualnego powiększenia/przybliżenia kamery).

2.2. Tryby pracy

Z punktu widzenia operatora, platforma UAV i głowica optoelektroniczna stanowią zespół urządzeń będących narzędziem pracy. Należy pamiętać, że lot platformy wykonywany jest w ściśle określonym celu i (w przypadku zadań szeroko pojętej obserwacji) operator nie zajmuje się pilotażem a uzyskaniem określonych danych z obserwowanego obrazu. Operator obserwuje obraz przekazywany z głowicy i na jego podstawie steruje obrotami osi, tak by osiągnąć zamierzony cel (np. ciągła obserwacja danego obiektu). Operator staje się w ten sposób elementem pętli sterowania głowicy.

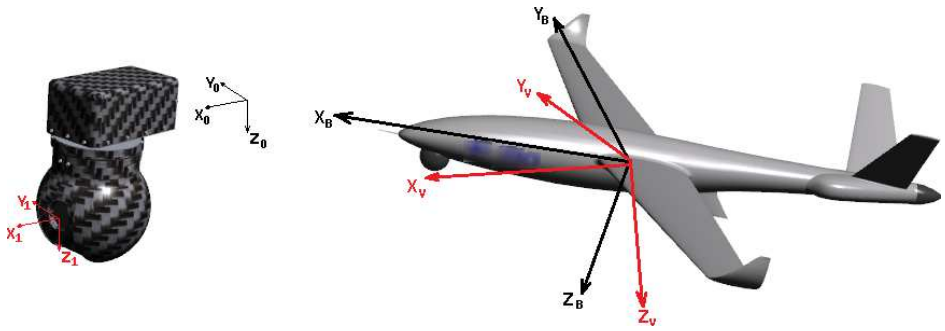
Tryby pracy głowic są dostosowane do specyfiki realizowania misji, stąd dostępne na rynku głowice zapewniają minimum 2 tryby pracy: tryb prędkościowy ze stabilizacją żyroskopową, oraz tryb pozycyjny. Należy zauważyć, że różni producenci udostępniają również inne tryby pracy (np. geopointing, czyli kierowanie wektora LOS w kierunku określonych współrzędnych geograficznych), jednak dwa wymienione powyżej tryby są najpowszechniejsze i bez nich niemożliwa byłaby realizacja wielu misji obserwacyjnych.

Tryb pozycyjny jest wykorzystywany rzadziej. W trybie tym operator zadaje ustawienie kątów głowicy na określone wartości i wektor LOS jest utrzymywany jako stały względem nosiciela. Tryb ten najczęściej wykorzystuje się podczas lotu w trybie widoku pilota (ang. PilotView). Polega ona na prowadzeniu obserwacji w kierunku lotu platformy, wykorzystywanego podczas startów i lądowań, w sytuacjach awaryjnych, lub podczas lotu ręcznego (pod pełną kontrolą operatora).

Tryb sterowania prędkościowego ze stabilizacją wykorzystywany jest znacznie częściej niż tryb pozycyjny. W trybie tym operator zadaje kierunki i prędkości obrotu głowicy, nie zważając na pozycję kamery, a jedynie na obserwowany obraz, tak by wektor LOS cały czas skierowany był na obserwowany obiekt. Na uzyskiwane prędkości kątowe głowicy wpływ ma nie tylko operator (poprzez wychylenie manipulatora), ale również – co zapewnia człon stabilizacji – prędkości kątowe nosiciela, oraz zoom sensora. W przypadku prędkości kątowych nosiciela chodzi o wyeliminowanie ich wpływu (przeciwdziałanie obrotom), zaś w przypadku zoom, chodzi o odpowiednie zmniejszenie prędkości kątowych w ruchu głowicy dla dużych przybliżeń.

3. Wektor LOS

Wektor LOS jako kierunek patrzenia kamery określany jest w układzie współrzędnych związanym z ziemią. Wpływ na niego ma zarówno zmiana kątów osi głowicy (pan i tilt), jak i orientacja nosiciela.



Rys. 2.Układy współrzędnych do wyznaczenia wektora LOS dla głowicy i nosiciela.
Fig. 2. Coordinate systems for determining gimball and carrier LOS vector

Przyjmijmy układy współrzędnych jak na rys 2. Układ XYZ_1 związany jest z kamerą, natomiast XYZ_0 z podstawą, tym wypadku z nosicielem. Takie rozmieszczenie układów współrzędnych jest związane ze sposobem montażu. Głowica jest montowana na spodzie nosiciela, co nie jest jedynym możliwym rozwiązaniem. Macierz obrotu układu XYZ_1 względem układu XYZ_0 (po uwzględnieniu obrotu wokół dwóch osi: Pan (P) i Tilt (T)) jest równa:

$$R_{GO} = \begin{bmatrix} cosPcosT & sinPcosT & -sinT \\ -sinP & cosP & 0 \\ cosPsinT & sinPsinT & cosT \end{bmatrix} \tag{1}$$

Wektor obserwacji kamery w układzie XYZ_0 można wyznaczyć jako:

$$\vec{L} = \begin{bmatrix} x \\ y \\ z \end{bmatrix} = R_{GO}^{T} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} cosPcosT \\ sinPcosT \\ -sinT \end{bmatrix} \tag{2}$$

Przyjmując, że głowica jest na platformie zamontowana tak, że kierunek osi X_0 wskazuje dziób samolotu, zaś kierunek osi Y_0 prawe skrzydło wektor $L=[1,0,0]^T$ oznacza orientację osi optycznej kamery w kierunku zgodnym z kierunkiem lotu, $L=[0,1,0]^T$ oznacza obserwację na prawe skrzydło, zaś $L=[0,0,1]^T$ oznacza kierunek patrzenia w dół platformy.

Macierz obrotu dla nosiciela (wyznaczająca orientację układu XYZ_B w układzie związanym z ziemią XYZ_V) jest równa [2]:

$$R_{BV} = \begin{bmatrix} c\Psi c\Theta & -s\Psi c\Theta & s\Theta \\ s\Phi c\Psi s\Theta + c\Phi s\Psi & c\Phi c\Psi - s\Phi s\Psi s\Theta & -s\Phi c\Theta \\ s\Phi s\Psi - c\Phi c\Psi s\Theta & c\Phi s\Psi s\Theta + s\Phi c\Psi & c\Phi c\Theta \end{bmatrix} \tag{3}$$

gdzie:

$$c\Phi = cos(\Phi), s\Phi = sin(\Phi),$$
$$c\Theta = cos(\Theta), s = sin(\Theta),$$
$$c\Psi = cos(\Psi), s\Psi = sin(\Psi)$$

to cosinusy i sinusy kątów Eulera odpowiednio przechylenie, pochylenie i odchylenie platformy UAV, (kolejne obroty wokół osi *x*, *y*, *z)*. Na podstawie równań 1-3 wektor LOS wyrażony w układzie związanym z ziemią ma postać:

$$\overrightarrow{LOS} = \begin{bmatrix} r_x \\ r_y \\ r_z \end{bmatrix} = (R_{GO}R_{BV})^T \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \tag{4}$$

co daje kolejne współrzędne wektora:

$$r_x = \Big(c(\Psi)c(\Theta)c(P) + \big(s(\Phi)c(\Psi)s(\Theta) - c(\Phi)s(\Psi)\big)s(P)\Big)c(T) - \big(s(\Phi)s(\Psi) + c(\Phi)s(\Psi)s(\Theta)\big)s(T) \tag{5.1}$$

$$r_y = \Big(s(\Psi)c(\Theta)c(P) + \big(s(\Phi)s(\Psi)s(\Theta) + c(\Phi)c(\Psi)\big)s(P)\Big)c(T) - \big(c(\Phi)s(\Psi)s(\Theta) - s(\Phi)c(\Psi)\big)s(T) \tag{5.2}$$

$$r_z = \big(s(\Phi)c(\Theta)s(P) - s(\Theta)c(P)\big)c(T) - c(\Phi)c(\Theta)s(T) \tag{5.3}$$

Współrzędne te uwzględniają obrót głowicy oraz nosiciela, i są wyrażone w układzie związanym z ziemią. Ich określenie umożliwia weryfikację modelu oraz algorytmów stabilizacji głowicy. Dla stabilizacji głowicy musi zostać wypracowane takie sterowanie, aby wektor LOS pozostał stały podczas zmiany orientacji nosiciela.

4. Stanowisko symulacyjne do badań Hardware in the Loop

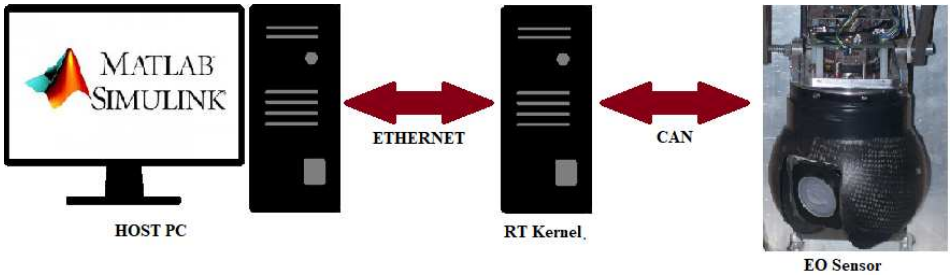
Skutecznym testem dla opracowanej głowicy i algorytmów sterowania jest jej montaż na platformie docelowej i wykonanie lotu z profilem misji zbliżonym do przewidywanego. Niestety, podejście takie jest kosztowne i kłopotliwe (zwłaszcza w przypadku większych UAV). Innym sposobem testowania jest budowa modelu matematycznego i symulacja zachowań głowicy. Budowa dokładnego modelu dynamiki nie jest jednak zadaniem trywialnym, a dokładna symulacja wymaga również modelu symulacyjnego platformy i prowadzonej misji. Możliwym jest również zainstalowanie głowicy na stole obrotowym, lub ramieniu robota [3] by w ten sposób wymusić przyspieszenia i prędkości kątowe. Niejako pośrednim sposobem testowania algorytmów sterowania jest wykonanie stanowiska HIL (ang. hardware in the loop). Na takim stanowisku oprogramowanie sterujące jest uruchamiane na docelowej platformie sprzętowej, z symulowaniem modelu sterowanego procesu. Stanowiska HIL pozwalają sprawdzić reakcje rzeczywistego układu sterowania w symulowanym otoczeniu, co wpływa na ich szerokie stosowanie w technice lotniczej [4], jako tańszą alternatywę dla wykonywania badań w locie.

4.1. xPC Target (Simulink Real-Time)

Pakiet Matlab/Simulink zawiera oprogramowanie Simulink Real-Time [5] (we wcześniejszych wersjach, w tym w wersji wykorzystywanej przez autora, udostępnianego jako xPC Target). Środowisko to pozwala na implementację algorytmu lub modelu symulacyjnego w środowisku Simulink na komputerze (hoście), po czym jego wykonanie na dedykowanym komputerze docelowym (xPC Target) z fizycznie dołączonymi elementami systemu. Umożliwia to przygotowanie symulacji, przeprowadzenie testów hardware in the loop, a także szybkie prototypowanie algorytmów. Komunikacja pomiędzy komputerem-hostem, a komputerem docelowym odbywa się poprzez interfejs ethernetowy, umożliwiając nie tylko programowanie układu xPC Target, ale również podgląd i wizualizację parametrów na komputerze host.

4.2. Stanowisko testowe

Wykorzystywane stanowisko (przedstawione schematycznie na rys. 3) składa się z komputera klasy PC z oprogramowaniem Matlab/Simulink, komputera PC (pracującego jako xPC target), głowicy optoelektronicznej (z własnym mikrokontrolerem sterującym) oraz opcjonalnego rejestratora CAN [6].



Rys. 3. Schemat ogólny stanowiska testowego
Fig. 3. General scheme of the test stand

Komputer PC pełni rolę hosta. xPC target w prezentowanym rozwiązaniu jest komputerem umożliwiającym przeprowadzenie symulacji opracowanych algorytmów w czasie rzeczywistym z uwzględnieniem odpowiedzi fizycznego obiektu sterowania. Nie jest planowany jako docelowa platforma sterująca, ale jako główne narzędzie do przeprowadzenia symulacji i doboru algorytmów. Komunikacja pomiędzy hostem a xPC odbywa się poprzez interfejs ethernet, natomiast pomiędzy xPC, a głowicą optoelektroniczną poprzez interfejs CAN. Całość komunikacji poprzez interfejs CAN jest dodatkowo rejestrowana do późniejszej analizy offline. Taka budowa stanowiska umożliwia badanie algorytmów na obu poziomach sterowania głowicą, przy czym nie narzuca docelowego rozwiązania sprzętowego dla głowicy optoelektronicznej. Dodatkowo możliwe jest przeprowadzenie symulacji z udziałem innych komponentów połączonych do wspólnej magistrali CAN, np. w celu sprawdzenia ich wzajemnej interakcji. Algorytmy opracowywane są na komputerze PC (host), po czym wgrywane i wykonywane na komputerze xPC target, do którego trafiają również dane z głowicy. Umożliwia to nie tylko sprawdzenie działania projektowanych algorytmów, ale również porównanie posiadanego/opracowanego modelu symulacyjnego z rzeczywistym obiektem.

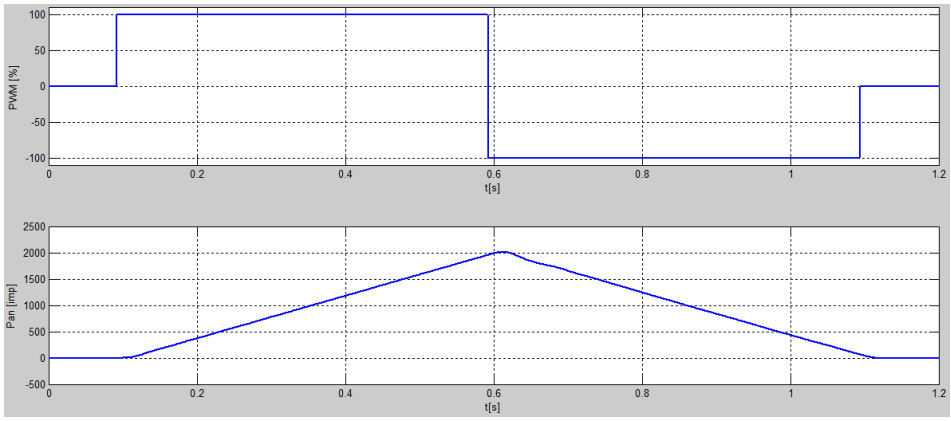
4.3. Wybrane realizacje

W przypadku sterowania niższego poziomu na komputerze PC opracowane zostały algorytmy sterowania napędami. Wartości zadawane są ustawiane przez operatora za pośrednictwem interfejsu CAN. Trafiają one na wejście regulatorów realizowanych w komputerze xPC target. Wyjścia z regulatorów (również poprzez magistralę CAN) trafiają do głowicy optoelektronicznej gdzie mikrokontroler wystawia zadane sygnały sterujące (wyznaczone w xPC Target), oraz dokonuje odczytu aktualnej pozycji, a także prędkości osi głowicy. Wartości te trafiają do xPC (ponownie przez magistralę CAN) tworząc pętlę sprzężenia zwrotnego. Mikrokontroler w głowicy pełnił w tym przypadku jedynie rolę

układu pomiarowego oraz generujacego zadany sygnał PWM do sterowania pracą silników. Na tym poziomie możliwe jest przeprowadzenie identyfikacji poszczególnych osi jako obiektów sterowania, dobór algorytmów sterowania napędami oraz ich parametrów. Dzięki zastosowaniu do tego stanowiska z oprogramowaniem Matlab/simulink możliwe było szybkie przetestowanie różnych regulatorów, z różnymi parametrami działania. Umożliwia to również budowę modelu zachowania napędów głowicy poddanych różnym wymuszeniom. Dobrane w ten sposób regulatory zostały następnie zaimplementowane w języku C i posłużyły do zaprogramowania mikrokontrolerów sterujących napędami głowicy. Na rysunku 4 przedstawiono wynik jednej z prób identyfikacji parametrów dynamicznych osi Pan. Wykres 1 przedstawia zadawane wymuszenia w postaci wypełnienia PWM (przy czym ujemna wartość oznacza zmianę kierunku obrotów). Wykres 2 przedstawia odpowiedź głowicy w postaci kąta obrotu osi Pan wyrażonej w impulsach enkodera (jako wartości mierzonej bezpośrednio).

W przypadku sterowania wyższego poziomu, w układzie HIL jak poprzednio, możliwe jest przetestowanie algorytmów stabilizacji. W tym wypadku komputer xPC target służył do symulacji zachowania nosiciela. Dla podstawowych algorytmów stabilizacji sygnałami wejściowymi są orientacja przestrzenna (Φ,Θ,Ψ) oraz prędkości kątowe nosiciela (P, Q, R), a sygnałami wyjściowymi odpowiedź głowicy w postaci zmiany kątów *pan* oraz *tilt*, co umożliwia określenie wektora LOS, oraz określenie dokładności algorytmu. Dzięki zastosowaniu HIL możemy zadać wymuszenia nie występujące w rzeczywistym locie, w celu sprawdzenia poprawności działania stabilizacji w pojedynczej osi, co ułatwia zaobserwowanie działania algorytmu. W kolejnych etapach testowania łatwo można dodać niezerowe wartości prędkości w pozostałych osiach i badanie poprawności zachowania algorytmów stabilizacji. Należy zauważyć, że dzięki symulacji możliwe jest podanie wymuszeń niezakłóconych, jak i obarczonych szumem. Wreszcie możliwe jest również podanie na wejście wcześniej zarejestrowanych parametrów rzeczywistego lotu i sprawdzenie działania głowicy, oraz porównania rzeczywistych odpowiedzi z opracowanym modelem.

Należy zaznaczyć, że stanowisko symuluje dla głowicy jej sensory prędkości kątowych i przyspieszeń, zatem wymaga poprawnego przygotowania danych, z uwzględnieniem wpływu zmiany orientacji nosiciela.



Rys. 4. Fragment przebiegów uzyskanych w trakcie prób identyfikacji osi Pan
Fig. 4. Fragment of the waveforms obtained during the Pan axis identification test

5. Podsumowanie

Zaprezentowane stanowisko do badań głowic optoelektronicznych jest pośrednim rozwiązaniem w badaniu, pomiędzy próbami w locie a przeprowadzeniem wyłącznie symulacji opartej na modelu matematycznym głowicy. W przypadku dostępu do oprogramowania *Matlab/simulink real time* umożliwia przeprowadzenie szeregu symulacji zarówno dla sztucznych jak i rzeczywiście występujących wymuszeń. Wadą rozwiązania jest niemożliwość sprawdzenia rzeczywistych czujników prędkości kątowych i przyspieszeń, jednak dla sprawdzenia poprawności działania algorytmów nie stanowi to powodu do dyskwalifikacji.

Literatura

[1] STANAG 4586, STANDARD INTERFACES OF UAV CONTROL SYSTEM (UCS) FOR NATO UAV INTEROPERABILITY.
[2] Bociek S., Gruszecki J.: Układy sterowania automatycznego samolotem. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 1999.
[3] Machowski B., Panasiuk K.: Wykorzystanie robota przemysłowego do badania układu stabilizacji głowicy śledzącej, Mechanik, nr 7/2011, s. 521-526.
[4] Chudy P., Dittrich P., Vlk J., Rzucidlo P., HW in-the-loop simulation of light aircraft's autopilot, AIAA Modeling and Simulation Technologies (MST) Conference, August 19-22, Boston, MA, 2013.
[5] https://www.mathworks.com/products/simulink-real-time.html (dostęp 15.08.2017).
[6] Dereń M.: A miniature on-board data recorder for unmanned platform, ZN PRz Mechanika, 87, 2015, s. 17-22.

TEST STAND FOR ELECTRO-OPTICAL GIMBAL SIMULATION TEST

S u m m a r y

Unmanned aerial vehicles (UAV) function in a growing number both military and civil applications. One of commonly undertaken tasks is an observation in its broadest sense. The observation involves using different kinds of sensors which often take form of electro-optical gimbals i.e. cameras placed in a mechatronic system which enables change of camera orientation toward a carrier. Developing control algorithms for the electro–optical gimbals as well as for the cameras, one should consider a number of parameters connected not only with the construction of the gimbal but also with its work conditions, especially including the capabilities of the carrier. The article presents the elementary information on the electro-optical gimbal, with special emphasis on a two axis gimbal dedicated to installing on board UAV. The designed and realized test stand for electro–optical gimbals simulation tests,which have been perfomed with the use of Matlab/Simulink, is also described in the article. The test stand allows testing the control algorithms via simulation of carrier behavior. It also enables parameterization on the basis of recorded UAV real flights as well as using forced set values not existing during real flights.

Keywords: electro-optical systems, gimbal, UAV, stabilization, simulation

DOI: 10.7862/re.2017.8

Tekst złożono w redakcji: wrzesień 2017
Przyjęto do druku: październik 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (2/2017), lipiec-wrzesień 2017, s. 29-39

Mateusz MUCHA [1]

PROTOTYPOWY SYSTEM ROZPOZNAWANIA TABLIC REJESTRACYJNYCH Z WYKORZYSTANIEM SIECI NEURONOWYCH

W artykule przedstawiono prototypowy system rozpoznawania tablic rejestracyjnych oparty o urządzenie Raspberry PI 2, zaprojektowany jako niskobudżetowa alternatywa dla komercyjnych rozwiązań. Praca opisuje poszczególne komponenty sprzętowe, aplikację sterującą rozpoznawaniem tekstu oraz przeprowadzone badania, pokazujące poprawność odczytu. Opisany został zastosowany algorytm, a także samo rozpoznawanie tekstu oparte o sztuczne sieci neuronowe.

Słowa kluczowe: OCR, OpenCV, Python, Raspberry PI 2, Sieci neuronowe

1. Wprowadzenie

Obecnie wiele uwagi przykłada się do kontroli wjazdu. Powstają obiekty o zamkniętym dostępie, takie jak osiedla mieszkaniowe, do których dostęp ma jedynie wybrana grupa pojazdów. Ograniczeniem dostępu zazwyczaj jest brama wjazdowa lub szlaban. Sterowanie nimi przez jedną osobę nie jest kłopotliwe, jednak w przypadku wielu osób może być już problemem. Można zastosować urządzenie, które w sposób automatyczny rozpozna pojazd za pomocą jego identyfikatora, którym jest tablica rejestracyjna, a następnie – w przypadku posiadania odpowiednich uprawnień – udzieli mu dostępu.

Prototypowy system rozpoznawania tablic rejestracyjnych jest propozycją takiego urządzenia. Może ono rozpoznać tablicę rejestracyjną na podstawie wykonanego zdjęcia, a dzięki wbudowanej bazie danych zezwolić, na wjazd pojazdu lub go odmówić.

Prototypowe rozwiązanie zostało zaimplementowane na platformie sprzętowej Raspberry Pi 2 wyposażonej w procesor ARM Cortex-A7 CPU z czterema rdzeniami taktowanymi częstotliwością 900 MHz [1]. Pozwala to na wykonywanie zaawansowanych obliczeń. Urządzenie ma do dyspozycji 1GB pamięci RAM. Dane przechowywane są na karcie micro SD, której minimalna prędkość zapisu wynosi 10 MB/s. Za część programową odpowiada system Linux.

[1] Mateusz Mucha, Krasne 10A, 36-007 Krasne, tel. 501252243, mateusz.mucha@wp.pl

Do urządzenia została podłączona kamera o rozdzielczości 5MPx, która w momencie wykrycia tablicy rejestracyjnej, robi jej zdjęcie [2]. Obecność pojazdów przed urządzeniem identyfikuje czujnik ultradźwiękowy HC-SR04, którego zadaniem jest stwierdzenie czy przed kamerą znajduje się tablica, czy też nie. Jest również możliwa detekcja za pomocą samej kamery, jednak w takim przypadku obciążenie urządzenia Raspberry Pi 2 staje się dużo większe. Spada wydajność przetwarzania danych. Urządzenie posiada także kartę sieciową, za pomocą której możliwa jest komunikacja w celu dodania lub usunięcia tablicy rejestracyjnej. Potencjalny użytkownik informowany jest o aktualnym stanie systemu za pomocą wbudowanych diod LED. Ostatnim elementem układu jest przekaźnik, który otwiera lub zamyka element końcowy jakim jest brama wjazdowa lub szlaban.

2. Komponenty sprzętowe

Urządzenie Raspberry Pi 2 jako platforma sprzętowa, posiada własne komponenty takie jak karta sieciowa lub port obsługi kart micro SD. Zapewnia również możliwość rozszerzenia funkcjonalności o kolejne podzespoły dzięki wbudowanym portom.

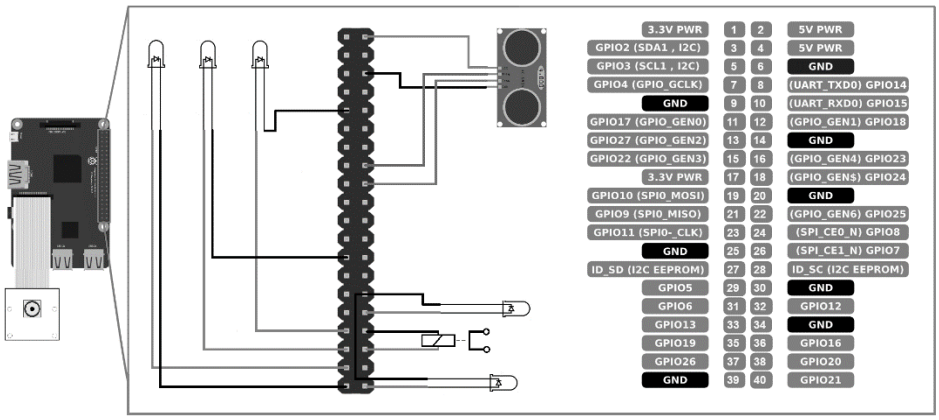
2.1. Schemat podłączenia

Zewnętrzne komponenty zostały podłączone do urządzenia Raspberry Pi 2 bezpośrednio za pomocą portów wejścia/wyjścia GPIO (*General Purpose Input/Output*). Rysunek 1 przedstawia wykorzystanie portów wejścia oraz wyjścia. Na schemacie nie uwzględniono rezystorów zabezpieczających Raspberry Pi 2 przed przeciążeniem.

Do urządzenia podłączono następujące komponenty:

- kamerę,
- czujnik zbliżeniowy,
- 3 diody sygnalizacyjne,
- 2 diody oświetlające otoczenie,
- przekaźnik.

Czujnik zbliżeniowy odpowiada za detekcję pojazdu przed bramą wjazdową. Kamera tworzy obraz tablicy rejestracyjnej, po czym przekazuje go do analizy. Trzy diody sygnalizacyjne informują o stanie urządzenia. Dwie diody doświetlające służą do oświetlenia analizowanej tablicy w nocy. Przekaźnik jest końcowym efektem wykonawczym otwierającym bramę wjazdową.



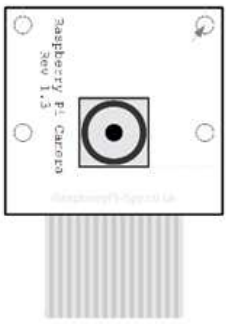
Rys. 1.Schemat podłączenia poszczególnych komponentów

Fig. 1. Diagram presenting connections between components

2.2. Kamera

Kamera wykorzystywana w prototypowym rozwiązaniu jest pierwszą wersją przeznaczoną dla urządzenia Raspberry Pi. Do urządzenia podłączona jest za pomocą dedykowanego portu. Kamera ma niewielkie rozmiary (25×24×9 mm) i waży zaledwie 3g. Matryca do przetwarzania obrazu jest wyposażona w sensor *OmniVision OV5647* o rozdzielczości 5 MPx. Maksymalna rozdzielczość, z jaką można zrobić zdjęcie, to 2592×1944 pikseli. Dzięki sprzętowemu wsparciu formatu h.264, możliwe jest także nagrywanie filmów w następujących rozdzielczościach:

- Full HD1080, przy zachowaniu 30 klatek na sekundę,
- HD720 przy 60 klatkach na sekundę,
- SD 640×480 przy maksymalnej prędkości 90 klatek na sekundę [3].

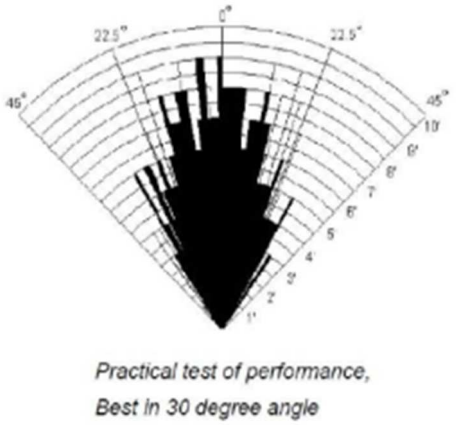


Rys. 2. Schemat kamery [2]

Fig. 2. Scheme of the camera [2]

2.3. Czujnik HC-04

Do odczytu odległości zastosowano czujnik ultradźwiękowy HC-SR04. Czujnik charakteryzuje się wysoką dokładnością (0,3 cm) oraz szerokim 30-stopniowym kątem pracy. Odległość mierzona mieści się w przedziale od 2 cm do 400 cm. Poza tym przedziałem urządzenie również odczytuje odległość, jednak pomiar jest niedokładny i podatny na zakłócenia. Czujnik jest zasilany napięciem 5V, pochodzącym bezpośrednio z Raspberry Pi 2. Odległość od przeszkody jest mierzona na podstawie prędkości dźwięku oraz czasu w jakim dana fala akustyczna zostanie wysłana z czujnika oraz do niego wróci. Obszar pracy przedstawia rys. 3 [4].



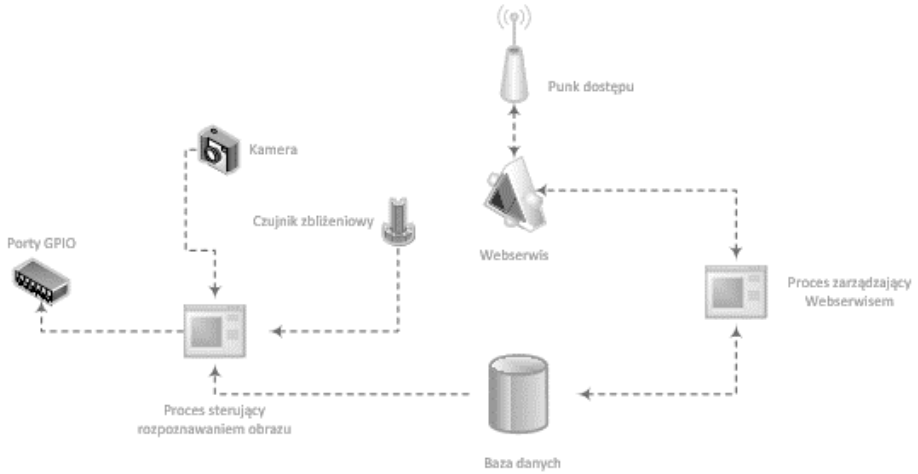
Rys. 3. Obszar pracy czujnika [4]

Fig. 3. Work area of the sensor [4]

3. Struktura programowa

Urządzenie do zarządzania danymi posługuje się zaimplementowaną usługą sieciową (z ang. *web service*). Za jej pośrednictwem możliwe jest odczytywanie informacji o tablicach rejestracyjnych oraz dodawanie nowych tablic lub ich usuwanie. *WebSerwis* jest obsługiwany przez proces uruchamiany podczas startu urządzenia. Proces posiada bezpośredni dostęp do bazy danych, w której zapisuje dane lub je odczytuje. Usługa sieciowa wykorzystuje format *XML* (z ang. *Extensible Markup Language*). Zastosowaną bazą danych jest *PostgreSQL* [5].

Do zadań procesu uruchamianego podczas startu urządzenia należy również detekcja obrazu oraz sterowanie wszystkimi portami wejścia/wyjścia. Zarządza on pracą aparatu oraz czujnika zbliżeniowego. Przepływ danych w projekcie prezentuje rys. 4.



Rys. 4. Schemat przepływu informacji.

Fig. 4. Model of information flow.

4. Algorytm

Proces główny rozpoznaje tablice poprzez wykonanie szeregu kroków, przedstawionych na Rys. 5.

Pierwszym krokiem jest wczytanie konfiguracji, w tym ustawień diod kontrolnych, portów oraz wczytanie zakresu odległości. Operacje te wykonywane są podczas startu procesu. Urządzenie zgłasza gotowość poprzez zaświecenie diody LED1.

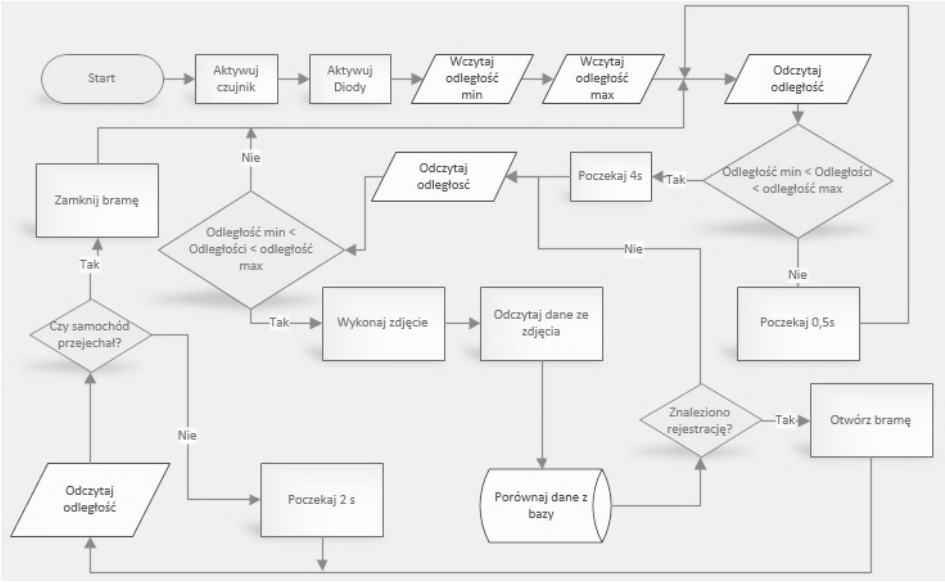
Następnie urządzenie odczytuje odległość z czujnika zbliżeniowego i sprawdza, czy pojazd znajduje się w odpowiednim miejscu. Przedział jest definiowany przez odległość minimalną i odległość maksymalną. Jeżeli w odpowiednim miejscu od czujnika znajduje się samochód, zostaje zaświecona dioda LED2. Aplikacja czeka 4 sekundy w celu stwierdzenia, czy samochód dalej znajduje się przed urządzeniem. Jeżeli nie, to następuje powrót do pierwszej detekcji odległości.

Jeżeli wykryto samochód, to ponownie odczytywany jest dystans do niego. Jeżeli odległość się zmieniła, to należy wrócić do pierwszego pomiaru, ponieważ zachodzi obawa, że mieliśmy do czynienia z zakłóceniem jakim może być np. przypadkowy pieszy. Jeżeli odległość nie uległa zmianie, to następuje przejście do kolejnego etapu polegającego na utworzeniu obrazu.

W etapie tworzenia obrazu dioda LED2 zaczyna mrugać, a także zostają włączone diody doświetlające. Zostaje wykonane zdjęcie oraz realizowana jest analiza obrazu. Odczytany tekst zostaje przekazany do bazy w celu stwierdzenia, czy numer tablicy rejestracyjnej znajduje się na liście pojazdów z przydzie-

lonym dostępem. Jeżeli w bazie nie ma takiej rejestracji lub rejestracja jest nierozpoznana to należy przejść do drugiego pomiaru, czyli do ponownej próby odczytania tablicy. Gdy rejestracja została rozpoznana, następuje otwarcie bramy poprzez odblokowanie przekaźnika, a diody doświetlające zostają zgaszone.

Kolejne czynności mają na celu upewnienie się, że nie nastąpi zamknięcie bramy, zanim samochód nie przemieścił się poza region, w którym mógłby ulec uszkodzeniu przy próbie zamknięcia bramy. W tym celu czujnik mierzy ponownie odległość aby sprawdzić obecności samochodu. Jeżeli jest obecny, to urządzenie czeka 2 sekundy, po czym ponownie sprawdza obecność. Operacja jest wykonywana do momentu stwierdzenia, że samochodu już nie ma. Gdy ten odjechał, następuje zamknięcie bramy.



Rys. 5. Algorytm działania systemu

Fig. 5. Algorithm of the system

5. Rozpoznawanie tekstu

Rozpoznawanie tekstu z obrazu jest procesem dość skomplikowanym a przy nieodpowiednio przygotowanym obrazie, bardzo wymagającym obliczeniowo [6,7]. Obecnie do tego celu wykorzystuje się sieci neuronowe, które skutecznie są w stanie rozpoznać badany tekst [8,9]. Poprawność jest uzależniona od wielu czynników, takich jak wielkość tekstu czy jakość zdjęcia. Jednak aby algorytmy szybko działały niezbędne jest wcześniejsze przygotowanie

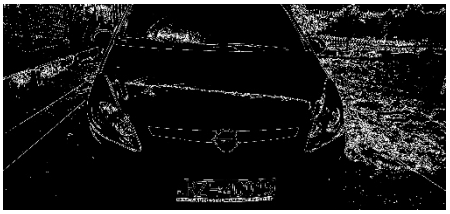
obrazu w celu zminimalizowania zakłóceń. Rozpoznawanie tekstu w opisywanym projekcie zostało podzielne na dwie części, omówione poniżej.

W pierwszej części obraz jest poddany obróbce w celu wyeliminowania zakłóceń, detali oraz innych zbędnych elementów. W tym celu wykorzystano bibliotekę OpenCV [10,11,12], która jest bogatym zbiorem funkcji do szybkiego przetwarzania obrazów. Biblioteka posiada otwarty kod źródłowy (*Open Source*). Oprócz funkcji do obróbki obrazów 2D i 3D, zawiera funkcje wykrywające gesty oraz ruch. Może być także używana w czasie rzeczywistym.

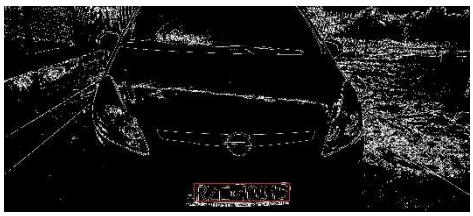
Obróbkę przykładowego zdjęcia, w kontekście prototypowego systemu rozpoznawania tablic rejestracyjnych, przedstawiają rysunki 6-9.

Rys. 6. Obraz w skali szarości
Fig. 6. Image in grayscale

Rys. 7. Obraz zbinaryzowany
Fig. 7. Binary image



Rys. 8. Kontury obrazu
Fig. 8. Contour of image



Rys. 9. Wykryty tekst
Fig. 9. Detected text

Proces detekcji obrazu można opisać w czterech krokach.

1. Pierwszym krokiem jest zmniejszenie wielkości zdjęcia. Obraz składa się z pikseli, a każdy piksel jest opisany trzema kolorami RGB (Red Green Blue). Rozmiar obrazu to iloczyn wysokości w pikselach, szerokość w pikselach oraz koloru w bitach. Kolor zazwyczaj jest opisany 24 bitami. Taki iloczyn daje wielkość obrazu w bitach. Jeżeli natomiast skonwertujemy obraz jako odcienie szarości, to kolor 1 piksela będzie opisywać jedynie 8 bitów, przez co wielkość zmniejszy się 16-krotnie (Rys.6).

2. Drugi krok powoduje binaryzację czyli przedstawienie obrazu w dwóch kolorach: czarnym i białym. W tym kroku również maleje wielkość ponieważ kolor opisuje 1 bit (Rys.7).
3. Trzecim krokiem jest zastosowanie funkcji *Contur*. Dzięki niej możliwe jest wyodrębnienie kontur z przetwarzanego obrazu (Rys. 8).
4. Ostatnim krokiem jest wyodrębnienie z obrazu możliwej tablicy rejestracyjnej (Rys. 9).

Druga cześć odpowiada za rozpoznanie wykrytego obrazu. W tym celu wykorzystano bibliotekę Tesseract OCR [13]. Zawiera ona zestaw funkcji służących do rozpoznawania znaków i całych bloków tekstów w pliku graficznym. Cały mechanizm opiera się na działaniu sieci neuronowej. Na początku klasyfikator sieci poddawany jest treningowi. Trenowanie (uczenie sieci) odbywa się podczas dostarczania obrazów prawidłowych znaków. Po tym procesie sieć zna kształty liter oraz jest w stanie rozpoznać nowe obrazy. Proces ten nie daje jednak 100% skuteczności i występują obrazy, które zostają rozpoznane błędnie.

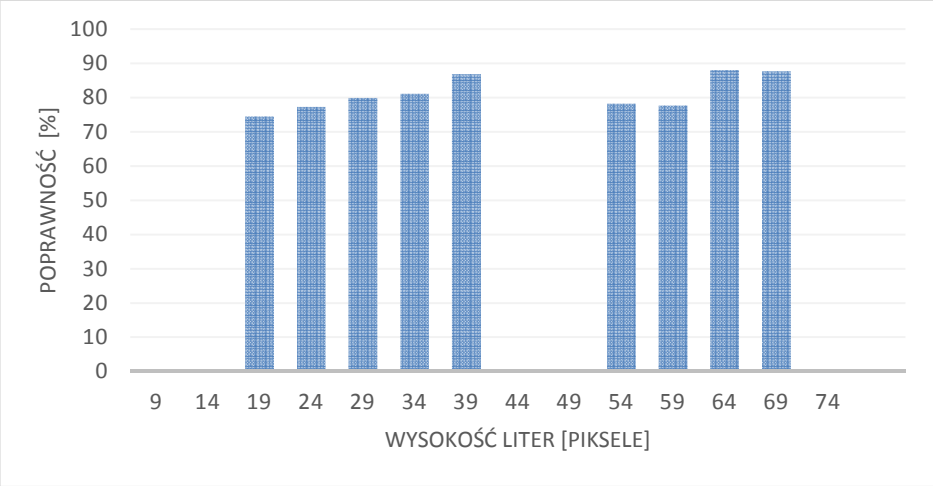
6. Badania i testy

System rozpoznawania tablic przetestowano pod kątem powtarzalności oraz poprawności rozpoznawania obrazów. Do testów wykorzystano zdjęcia 20 tablic zrobione w różnych warunkach atmosferycznych. Zbadano również wpływ odległości od urządzenia.

W pierwszym teście przeprowadzono analizę odczytu biorąc pod uwagę odległość do fotografowanej tablicy. Zmiana odległości przekłada się na zmianę wielkości czcionki. Na Rys. 10. można zaobserwować, że wraz ze wzrostem wielkości wzrasta poprawność dopasowania. Proces ten jest prawie liniowy do momentu osiągnięcia wielkości 44 pikseli.

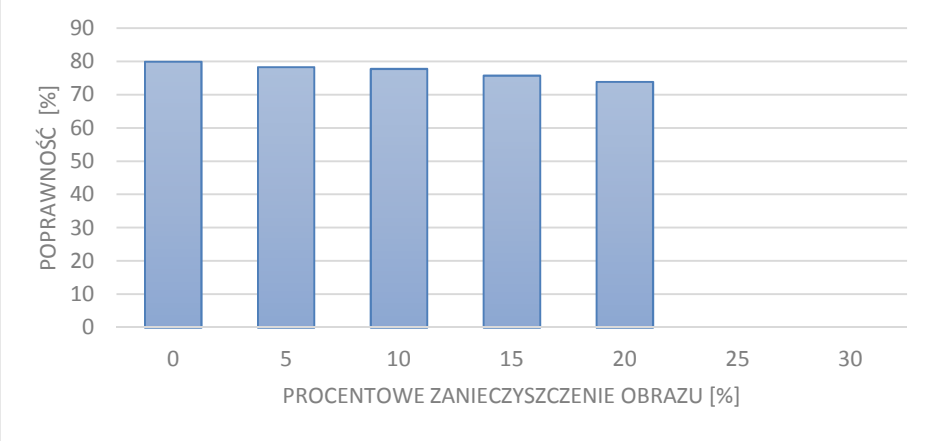
W tym momencie algorytm przestaje działać poprawnie, ponieważ w badanym przypadku tablica rejestracyjna jest umieszczona w plastikowej ramce, na której jest tekst reklamowy. Powoduje to problem w działaniu algorytmu. Tekst o rozmiarze powyżej 49 pikseli jest rozpoznawany prawidłowo aż do 74 pikseli gdzie również nie jest możliwe rozpoznanie.

Drugi test przedstawia symulację zanieczyszczeń obrazu (Rys. 11) wykonaną poprzez nałożenie zakłóceń na obraz. Widać wyraźnie, że im większa skala zakłócenia, tym mniejsza poprawność rozpoznawania tekstu. Przy zastosowaniu zanieczyszczenia obrazu rzędu 25%, tablica rejestracyjna nie zostanie już odczytana.



Rys. 10. Badanie poprawności odczytu tablic w zależności od wielkości tekstu

Fig. 10. Correctness of reading license plates depending on the size of the text



Rys. 11. Badanie poprawności odczytu tablic w zależności od zanieczyszczeń.

Fig. 11. Correctness of reading license plates depending on contamination

7. Podsumowanie

Urządzenie Raspberry Pi 2, jako platforma sprzętowa nadaje się do operacji związanych z przetwarzaniem obrazu. Zastosowanie komponentów sprzętowych, takich jak czujnik zbliżeniowy, pozwala zwiększyć wydajność i skuteczność systemu. Zastosowanie bezprzewodowej karty sieciowej pozwoliło na zdalne zarządzanie urządzeniem, zaś diody LED w łatwy sposób informują o aktualnym stanie systemu. Dodatkowe diody umożliwiają odczytywanie nu-

merów rejestracyjnych w nocy. Dzięki systemowi Linux oraz utworzonej aplikacji, urządzenie stało się niezależną jednostką obliczeniową, która do prawidłowej pracy potrzebuje jedynie zasilania.

Zastosowanie sieci neuronowej do rozpoznawania tablic rejestracyjnych pokazało, że ten sposób rozpoznawania obrazu w znacznym stopniu poprawia wydajność oraz poprawność odczytywanego tekstu. Specjalnie zaprojektowany algorytm pozwala na detekcję niechcianych obiektów oraz umożliwia rozpoznawanie numerów tablic rejestracyjnych w celu zarządzania dostępem.

Przeprowadzone testy dowiodły, że odległość od mierzonego obiektu ma znaczenie. Nie jest to jednak zależność liniowa. Test pokazał również, że istnieje wielkość liter dla której odczyt jest niemożliwy. Wprowadzenie zanieczyszczenia do badanej rejestracji powoduje zmniejszenie poprawności odczytu. Nie powoduje jednak zakłóceń w samym procesie odczytu. Odczyt jest poprawny do pewnego progu występowania zakłócenia. Po przekroczeniu niego, odczyt jest już niemożliwy.

W kolejnym etapie prac należałoby zastosować kamerę na podczerwień w celu poprawy jakości zdjęć nocnych. Pozwoli to zrezygnować z zastosowanych diod do oświetlenia w nocy oraz przyśpieszy działanie całego procesu ponieważ obraz odczytany z kamery podczerwonej automatycznie jest jak w skali szarości.

Bibliografia

[1] Upton E.: Raspberry Pi User Guide Wiley 2013.
[2] http://www.raspberrypi-spy.co.uk/wp-content/uploads/2013/05/Raspberry-Pi-Camera-Module-Diagram.png
[3] https://www.raspberrypi.org/documentation/hardware/camera/README.md
[4] https://docs.google.com/document/d/1Y-yZnNhMYy7rwhAgyL_pfa39RsB-x2qR4vP8saG73rE/edit
[5] http://www.postgresql.org.pl/
[6] Tadeusiewicz R.: Sieci neuronowe, Akademicka Oficyna Wydawnicza, Warszawa 1993.
[7] Clarke A.: OCR Functional Skills, Hodder & Stoughton, 2010.
[8] http://www.ftj.agh.edu.pl/~stegowski/rozne/neurony/art_kern_1.pdf
[9] Michalewicz Z.: Algorytmy genetyczne + struktury danych = programy ewolucyjne, Wydawnictwo WNT, 2003.
[10] Bradski G., Kaehler A.: Learning OpenCV Computer Vision with the OpenCV Library , Publisher: O'Reilly Media, Final Release Date: September 2008, Pages: 580.
[11] Mori S., Nishida H., Yamada H.: Optical Character Recognition, Authors: Publication: Cover Image Book Optical Character Recognition, 1st John Wiley & Sons, Inc. New York, USA, 1999, ISBN 0471308196.
[12] http://opencv.org/
[13] https://github.com/tesseract-ocr/tesseract/wiki

PROTOTYPE SYSTEM OF RECOGNIZING NUMBER PLATES WITH USING ARTIFICIAL NEURAL NETWORKS

S u m m a r y

The article has been presented prototype system of recognizing a number of plates based on Raspberry Pi 2. The system was designed as the low-budget alternative to dear commercial solutions. This article is describing individual equipment components, the application controlling, the recognition process of the text and conducted examinations, showing the correctness of the reading. An applied algorithm has been described, as well as recognizing the text based on artificial neural networks.

Keywords: OCR, OpenCV, Python, Raspberry PI 2

DOI: 10.7862/re.2017.9

Tekst złożono w redakcji: wrzesień 2017
Przyjęto do druku: październik 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (2/2017), lipiec-wrzesień 2017, s. 41-50

Robert Żelazny[1]

URZĄDZENIA ELEKTRYCZNEGO OGRZEWANIA ROZJAZDÓW ORAZ OŚWIETLENIA ZEWNĘTRZNEGO NA TERENIE PKP POLSKIE LINIE KOLEJOWE S.A.

W artykule omówiono urządzenia elektrycznego ogrzewania rozjazdów oraz oświetlenie zewnętrzne montowane na terenie PKP Polskie Linie Kolejowe S.A. Urządzenia elektrycznego ogrzewania rozjazdów zapewniają skuteczną ochronę rozjazdów w warunkach negatywnego oddziaływania warunków atmosferycznych. Ze względu na dużą energochłonność urządzeń elektrycznego ogrzewania rozjazdów omówiono sposoby zmniejszania zużycia energii elektrycznej. Oświetlenie głowic rozjazdowych ma na celu zwiększenie bezpieczeństwa prowadzenia ruchu pociągów. Dodatkowo w artykule wskazano możliwości efektywnego sterowania oświetleniem w wybranych rejonach stacji podczas zmniejszonego ruchu pociągów. Przedstawiono podstawowe wymagania dotyczące jakości energii elektrycznej zasilającej urządzenia na terenach kolejowych.

Słowa kluczowe: elektryczne ogrzewanie rozjazdów, oświetlenie terenów kolejowych, jakość energii elektrycznej

1. Wprowadzenie

Bezpieczeństwo prowadzenia ruchu kolejowego na terenie PKP Polskie Linie Kolejowe S.A., szczególnie w okresie zimowym, bezwzględnie musi być zapewnione. Newralgiczne elementy, które odpowiadają za prowadzenie ruchu kolejowego to rozjazdy. W celu zapewnienia sprawności rozjazdów, montuje się w ich elementach urządzenia elektrycznego ogrzewania rozjazdów (rys. 1). W warunkach ograniczonej widoczności dla zapewnienia bezpiecznego prowadzenia ruchu pociągów montuje się oświetlenie głowic rozjazdowych. Rozjazdy z zamontowanymi urządzeniami elektrycznego ogrzewania rozjazdów nie są narażone na zablokowanie w skutek negatywnych oddziaływań niskich temperatur jak również śniegu i lodu. Śnieg dostający się pomiędzy iglicę a opornicę

[1] Robert Żelazny, PKP Polskie Linie Kolejowe S.A. oraz Politechnika Częstochowska Wydział Elektryczny, email: Robert1980@interia.eu

rozjazdu i w rejony zamknięć nastawczych może powodować trudności w sterowaniu rozjazdem oraz w przypadku niesprzyjających warunków atmosferycznych jego zablokowanie. Zakłady Linii Kolejowych jako zarządcy infrastruktury są zobowiązane do zapewnienia skutecznej ochrony rozjazdów przed negatywnymi wpływami atmosferycznymi [2] oraz oświetlenia głowic rozjazdowych w stacjach [3], celem bezpiecznego prowadzenia ruchu pociągów.

2. Wymagania ogólne i podstawowe parametry jakości energii elektrycznej w instalacjach PKP Polskie Linie Kolejowe S.A.

W celu zachowania bezpieczeństwa, urządzenia na terenie kolejowym muszą być zasilane energią elektryczną o określonych parametrach [1, 4, 9], aby nie nastąpiło ich uszkodzenie. Do zasilania odbiorów kolejowych PKP Polskie Linie Kolejowe S.A. są często wykorzystywane linie potrzeb nietrakcyjnych (zasilane z podstacji trakcyjnych) oraz linie zasilające energetyki zawodowej [7]. Jakość energii elektrycznej, którą są zasilane urządzenia kolejowe [5, 6], jest bardzo ważnym czynnikiem, ponieważ bezpośrednio wpływa ona na bezpieczeństwo prowadzenia ruchu kolejowego [13, 22]. Szczegóły dotyczące podstawowych parametrów są wymienione poniżej, gdzie niezależnie od źródła zasilania energią elektryczną powinny być spełnione następujące wymagania:

1. Znamionowe napięcie zasilania U_N: 230 V AC lub 3x400 V AC.
2. Dopuszczalne zmiany wartości napięcia zasilania: ± 10% (zgodnie z rozporządzeniem [12] i normą PN-EN 50160 [9]).
3. Znamionowa częstotliwość napięcia zasilającego f_N: 50 Hz.
4. Dopuszczalne zmiany częstotliwości napięcia zasilającego: ± 1% przez 95% tygodnia; + 4% / - 6% przez 100% tygodnia (zgodnie z rozporządzeniem [12] i normą PN-EN 50160 [9]).
5. Maksymalna wartość współczynnika THD napięcia zasilania, uwzględniający wyższe harmoniczne do rzędu 40: 8% (zgodnie z rozporządzeniem [12] i normą PN-EN 50160 [9]).
6. Maksymalne wartości harmonicznych zgodnie z tabelą nr 1 (zgodnie z rozporządzeniem [12]).
7. Dopuszczalne zmiany wartości napięcia między fazami oraz siecią główną: 5 % [13].
8. Minimalna przeciążalność: 150% przez 5 minut.
9. Maksymalna wartość przepięć o częstotliwości sieciowej: U_N + 250 V dla $t > 5$ s; U_N + 1 200 V dla $t < 5$ s (zgodnie z normą PN-IEC 60364 [8]).
10. Kompatybilność elektromagnetyczna zgodnie z normą PN-EN 50121-2 [15].

Tabela 1. Dopuszczalne wartości harmonicznych napięcia zasilania

Table 1. Acceptable harmonic voltage supply voltage values

Rząd harmonicznej [h]	Wartość względna napięcia w stosunku do składowej podstawowej [%]	Rząd harmonicznej [h]	Wartość względna napięcia w stosunku do składowej podstawowej [%]	Rząd harmonicznej [h]	Wartość względna napięcia w stosunku do składowej podstawowej [%]
2	2	11	3,5	20	0,5
3	5	12	0,5	21	0,5
4	1	13	3	22	0,5
5	6	14	0,5	23	1,5
6	0,5	15	0,5	24	0,5
7	5	16	0,5	25	1,5
8	0,5	17	2	>25	0,5
9	1,5	18	0,5		
10	0,5	19	1,5		

Urządzenia elektroenergetyki kolejowej w instalacjach PKP Polskie Linie Kolejowe S.A. najczęściej zasilane są napięciem o wartości do 1 kV. Jest to napięcie nazywane jako niskie o wartościach 230V 50 Hz lub 3x400 V 50 Hz.

Wykaz ważniejszych odbiorów elektroenergetyki kolejowej:

1. Elektryczne ogrzewanie rozjazdów (EOR).
2. Oświetlenie peronów, przejść i torów stacyjnych.
3. Oświetlenie przejazdów kolejowo-drogowych oraz zasilanie urządzeń technicznych.
4. Oświetlenie ramp i placów ładunkowych.
5. Instalacje w budynkach kolejowych.
6. Urządzenia zamontowane na nastawniach kolejowych.
7. Urządzenia SRK (sterowania ruchu kolejowego) zamontowane na szlakach i stacjach kolejowych.

3. Elektryczne ogrzewanie rozjazdów

Na terenie PKP Polskie Linie Kolejowe S.A. najczęściej stosowanymi systemami ogrzewania wybranych elementów rozjazdów są systemy elektrycznego ogrzewania rozjazdów (EOR). Ogrzewanie rozjazdów w okresie zimowym ma na celu usunięcie śniegu lub lodu (rys. 1). Elementy ogrzewane to przede wszystkim: iglica, opornica, zamknięcia nastawcze oraz inne elementy w zależności od typu rozjazdu. Dobór i rozmieszczenie poszczególnych grzejników jest podany w kartach EOR stanowiących załącznik nr 1 do „Wytycznych projektowania urządzeń elektrycznego ogrzewania rozjazdów – Tom-1". Do ogrzewania rozjazdów służą grzejniki opornikowe [16] przytwierdzone do stopki opornicy poprzez uchwyty [17] oraz płyty grzewcze i inne grzejniki specjalne. Urządzenia EOR składają się z elementów takich jak: grzejniki [16], transformatory separacyjne [18] i szafy rozdzielcze [19]. Sterowanie rozbudowanymi urządzeniami odbywa się za pomocą przetworników pogodowych, które umożliwiają automatyczne przełączanie w celu dostosowania intensywności ogrzewania do warunków pogodowych w danym okresie. Nowoczesne układy są dostosowane do zdalnej kontroli oraz do zmiany ustawień w układzie sterowania. Transformatory separacyjne urządzeń EOR przeznaczone są do zasilania grzejników zamontowanych w rozjazdach. Zadania dodatkowe transformatorów separacyjnych to ochrona obsługi przed porażeniem ze strony zasilania napięciem 230V, separacja obwodów zasilających od przepływu prądów błądzących oraz zapobieganie przeniesienia potencjału 3 kV prądu stałego poza strefę oddziaływania trakcji elektrycznej w warunkach zakłóceniowych. W zależności od typu i zastosowania transformatory EOR mogą być o mocach od 150 do 4600 VA. Urządzenia EOR są produkowane i stosowane w rozjazdach o mocach pojedynczej grzałki od 50 do 1600 W, natomiast moc całego układu EOR dla jednego rozjazdu zawiera się w przedziale od 2400 do ponad 25000 W. Do ogrzewania iglic oraz opornic w rozjazdach stosowane są grzejniki o mocach 900, 1050, 1250 i 1600 W. Grzejnik składa się z pręta, wewnątrz którego umieszczona jest spirala o mocy 330 W/m, przewodu zasilającego o przekroju 3x1,5 mm^2 z przewodem ochronnym podłączonym do płaszcza grzejnika oraz mufy kablowej oznaczonej odpowiednim kolorem w zależności od mocy grzałki. Szafy rozdzielcze EOR służą do zasilania skrzyń transformatorowych elektrycznego ogrzewania rozjazdów. Obudowa szafy rozdzielczej powinna być wykonana z tworzywa sztucznego odpornego na działanie promieniowania UV, z powłoką pozwalającą na łatwe zmywanie graffiti. W nowych urządzeniach nie dopuszcza się do stosowania szaf rozdzielczych elektrycznego ogrzewania rozjazdów z metalu. Obwody grzewcze powinny być zaprojektowane w taki sposób, aby było możliwe załączanie oraz wyłączanie poszczególnych rozjazdów w zależności od sytuacji ruchowej [14].

Rys. 1. Wytopiony śnieg w rozjeździe na skutek zamontowanego urządzenia elektrycznego ogrzewania rozjazdów

Fig. 1. Melted snow In the turnout as a result of the mounted switch heating electrical

4. Oświetlenie terenów kolejowych, przejść oraz przejazdów kolejowo-drogowych

Oświetlenie terenów kolejowych musi spełniać wiele różnych wymagań [3, 20]. Źródła światła nie powinny negatywnie wpływać na warunki obserwacji oraz rozpoznawania sygnalizatorów świetlnych przez kierujących pojazdami kolejowymi.

Źródła światła stosowane na terenach kolejowych to przede wszystkim:

1. Lampy wyładowcze sodowe wysokoprężne (stosowane na terenach otwartych).
2. Lampy wyładowcze metalohalogenkowe (stosowane na terenach otwartych).
3. Świetlówki liniowe (stosowane w celu oświetlenia zadaszonych peronów, przejść i tuneli).
4. Źródła światła LED (rys. 2).
5. Lampy wyładowcze rtęciowe (stosowane na terenach otwartych, lecz ze względu na ich energochłonność oraz ochronę środowiska sukcesywnie wycofywane).

Rys. 2. Nowoczesne oprawy oświetleniowe typu LED na słupach kompozytowych na przejeździe kolejowo-drogowym

Fig 2. Modern LED luminaires on composite poles at railroad crossing

Aby oprawa oświetleniowa mogła być stosowana na terenach kolejowych, ze względu na poziom bezpieczeństwa, na które ma wpływ oświetlenie, musi przejść pozytywne badania Centrali Biura Energetyki PKP PLK S.A. i po pozytywnej weryfikacji może być dopuszczona do eksploatacji. Wykaz elementów podsystemów i technologii pozytywnie zweryfikowanych, spełniających wymagania techniczne określone w Dokumentach Normatywnych przyjętych do stosowania na PKP PLK S.A. jest przedstawiony (i na bieżąco aktualizowany) na stronie internetowej PKP Polskie Linie Kolejowe S.A. Oprawy oświetleniowe powinny cechować się dużą trwałością i niezmiennością parametrów w czasie. Powinny być odporne na negatywne działania warunków atmosferycznych.

Charakterystyka urządzeń oświetlenia zewnętrznego oraz podstawowe wymagania:

1. Źródła światła powinny mieć parametry zapewniające najkorzystniejsze warunki postrzegania i rozpoznawania obiektów.
2. Źródła światła powinny mieć I lub II klasę ochronności, napięcie znamionowe - 230 V, 50 Hz.

3. Oprawy oświetleniowe charakteryzujące się współczynnikiem IP≥65 dla komory układu optycznego i komory osprzętu elektrycznego.
4. Klosz powinien być płaski wykonany z hartowanego szkła, klasa wytrzymałości opraw na uderzenia IK≥08 (dla naświetlaczy IK≥06).
5. Oprawy oświetleniowe - symetryczna bryła fotometryczna w płaszczyźnie C0÷C180 z maksimum światłości zawartej pomiędzy kątami 60° a 80°, powyżej kąta 80° światłość oprawy powinna być bliska zeru, pod kątem 90° oprawa nie powinna wysyłać strumienia świetlnego.
6. Naświetlacze - maksymalna światłość w płaszczyźnie optycznej C0÷C180 w zakresie kąta od 0° do 60°, maksymalny kąt odcięcia światła 80°, w płaszczyźnie optycznej C90÷C270 w zakresie kątów -20° do +20°.
7. Sprawność świetlna urządzeń powinna wynosić: ≥70% dla opraw oświetleniowych, ≥75% dla naświetlaczy oraz ≥65% dla opraw świetlówkowych.
8. Obudowa opraw wykonana z aluminium (z tworzywa sztucznego dla opraw świetlówkowych).
9. Kolor obudowy opraw oświetleniowych - szary (według katalogu RAL 7035) [20].

Na modernizowanych liniach kolejowych oświetlenie zewnętrzne powinno być włączone do Lokalnego Centrum Sterowania (LCS). Do wykonywania manipulacji sterowania oświetleniem zewnętrznym powinien być wydzielony terminal komputerowy. Sterowanie odbywające się z LCS powinno umożliwiać realizację poleceń załączania oraz wyłączania wydzielonych linii oświetleniowych z możliwością wybrania opcji sterowania ręcznego lub automatycznego. W ciągach oświetleniowych powinny być zastosowane źródła światła o jednakowej barwie światła. W przypadku oświetlania powierzchni na dużym terenie dopuszcza się zastosowanie masztów oświetleniowych z opuszczaną koroną z zamontowanymi naświetlaczami o szerokim rozsyle strumienia światła [22]. Konstrukcje wsporcze oświetlenia zewnętrznego muszą być posadowione zgodnie z wymaganiami dotyczącymi skrajni budowli na terenie kolejowym.

Na terenach PKP PLK S.A. należy stosować konstrukcje wsporcze oświetlenia w wykonaniach jako:

1. Słupy metalowe.
2. Maszty z opuszczaną koroną.
3. Słupy strunobetonowe wirowane.
4. Inne słupy spełniające wymagania określone przez Centralę PKP Polskie Linie Kolejowe S.A.
5. Konstrukcje obiektów kolejowych umożliwiających montaż opraw oświetleniowych (budynki, budowle, wieże).

Podstawowe wymagania dotyczące oświetlenia przejść oraz przejazdów kolejowo-drogowych określa Rozporządzenie Ministra Infrastruktury i Rozwoju [21]. Dodatkowe wymagania dla oświetlenia przejść oraz przejazdów kolejowo-drogowych zawarte są w standardach technicznych [22]. Oświetlenie przejazdu kolejowo-drogowego oraz przejścia powinno być tak usytuowane, aby nie powodowało olśnienia kierujących pojazdami kolejowymi i uczestników ruchu drogowego. Dodatkowo oświetlenie nie powinno zakłócać widoczności sygnałów i znaków kolejowych oraz drogowych.

5. Wnioski

Urządzenia elektrycznego ogrzewania rozjazdów oraz oświetlenia zewnętrznego na terenach kolejowych charakteryzują się dużą energochłonnością. W celu zapewnienia bezpieczeństwa ruchu kolejowego jak również zmniejszania energochłonności obecnie zabudowanych urządzeń, podczas modernizacji należy je wymieniać na nowoczesne energooszczędne urządzenia. Urządzenia powinny być wyposażone w nowoczesne układy sterowania szczególnie dla urządzeń elektrycznego ogrzewania rozjazdów, które w warunkach pogodowych nie powodujących konieczności ogrzewania wybranych elementów rozjazdu, nie pobierają energii elektrycznej, a ruch pociągów odbywa się bezpiecznie i bez zakłóceń. Dodatkowo dla urządzeń EOR wymiana transformatorów separacyjnych na inne o większej sprawności również powoduje zmniejszenie zużycia energii elektrycznej [10, 11]. Modernizacja urządzeń oświetlenia zewnętrznego (wycofanie nieefektywnych źródeł światła) oraz, w zależności od natężenia ruchu kolejowego, zastosowanie możliwości sterowania oświetleniem wybranych rejonów stacji, również mają znaczny wpływ na oszczędności zużycia energii elektrycznej. Reasumując stwierdzam, że urządzenia elektrycznego ogrzewania rozjazdów oraz urządzenia oświetlenia zewnętrznego i inne odbiory na terenie PKP Polskie Linie Kolejowe S.A. powinny być zasilane energią elektryczną o parametrach zgodnych z wymaganiami obowiązującymi na terenie PKP PLK S.A., w celu uniknięcia ich uszkodzeń, co miałoby znaczący wpływ na bezpieczeństwo ruchu kolejowego. Dodatkowo modernizacje energochłonnych urządzeń oraz zastosowanie nowoczesnych układów sterowania znacząco wpłynie na zmniejszenie zużycia energii elektrycznej.

Literatura

[1] Hanzelka Z.: Jakość energii elektrycznej. Część 4. Wyższe harmoniczne napięć i prądów.
[2] Iet-1 Instrukcja eksploatacji i utrzymania urządzeń elektrycznego ogrzewania rozjazdów, PKP Polskie Linie Kolejowe S.A., Warszawa 2014.

[3] Iet-3 Instrukcja eksploatacji urządzeń oświetlenia zewnętrznego terenów kolejowych, PKP Polskie Linie Kolejowe S.A., Warszawa 2015.
[4] Ustawa z dnia 10 kwietnia 1997r. z późniejszymi zmianami Prawo energetyczne Dz.U. z 2012r., poz. 1059. Z 2013r., poz. 984 i poz.1238, z 2014r., poz. 457, poz. 490, poz. 900, poz. 942, poz. 11010, poz. 1662 oraz z 2015r. poz. 151, poz. 478 i poz. 942.
[5] PN - EN 61000-3-2 Kompatybilność elektromagnetyczna (EMC) - Część 3-2: Poziomy dopuszczalne - Poziomy dopuszczalne emisji harmonicznych prądu (fazowy prąd zasilający odbiornika ≤16 A).
[6] PN-EN 61000-3-12 Kompatybilność elektromagnetyczna (EMC) - Część 3-12: Dopuszczalne poziomy - Dopuszczalne poziomy harmonicznych prądów powodowanych działaniem odbiorników, które mają być przyłączone do publicznej sieci zasilającej niskiego napięcia z fazowym prądem zasilającym odbiornika > 16 A i ≤ 75 A.
[7] Instrukcja Ruchu i Eksploatacji Sieci Dystrybucyjnej (zatwierdzona decyzją Prezesa URE nr DRR-4321-29(5)/2013/MKo4 z dnia 10 września 2013 r.) str. 99-101
[8] PN-IEC 60364: 2006-2009. Instalacje elektryczne w obiektach budowlanych.
[9] PN-EN 50160:2010 Parametry napięcia zasilającego w publicznych sieciach elektroenergetycznych s.13.
[10] Jagieła K., Rak J., Gała M., Kępiński M.: Straty mocy w transformatorach energetycznych zasilających dużych odbiorców przemysłowych Energoenergetyka nr 3(9)/2011.
[11] „K-Factor Isolation Transformer" (AET-2009-AET_K13 Factor_400V_R1.pdf), www.aet.com.sg.
[12] Rozporządzenie Ministra Gospodarki z 4 maja 2007 r. w sprawie szczegółowych zasad funkcjonowania systemu elektroenergetycznego (Dz. U. z 2007 r. Nr 93, poz. 623, z późn. zm.) s. 5665-5668.
[13] Opracowanie wymagań na zasilanie energią elektryczną urządzeń sterowania ruchem kolejowym. Praca CNTK nr 4034/10, Warszawa 2003.
[14] Iet-5 Wytyczne projektowania urządzeń elektrycznego ogrzewania rozjazdów. Warszawa 2015.
[15] PN-EN 50121-2: 2004. Zastosowania kolejowe. Kompatybilność elektromagnetyczna. Część 2: Oddziaływanie systemu kolejowego na otoczenie.
[16] Iet-118 Dokument normatywny 01-8/ET/2008. Grzejniki elektrycznego ogrzewania rozjazdów - PKP PLK S.A. Warszawa 2008.
[17] Iet-119 Dokument normatywny 01-9/ET/2008. Uchwyty grzejników elektrycznego ogrzewania rozjazdów - PKP PLK S.A. Warszawa 2008.
[18] Iet-117 Dokument normatywny 01-7/ET/2008. Skrzynia transformatorowa elektrycznego ogrzewania rozjazdów - PKP PLK S.A. Warszawa 2008.
[19] Iet-116 Dokument normatywny 01-6/ET/2008. Szafa rozdzielcza elektrycznego ogrzewania rozjazdów - PKP PLK S.A. Warszawa 2008.
[20] Iet-115 Dokument normatywny 01-5/ET/2008. Oprawy oświetleniowe - PKP PLK S.A. Warszawa 2008.
[21] Rozporządzenie Ministra Infrastruktury i Rozwoju z 20 października 2015 r. w sprawie warunków technicznych, jakim powinny odpowiadać skrzyżowania linii kolejowych oraz bocznic kolejowych z drogami i ich usytuowanie.

[22] Standardy techniczne – szczegółowe warunki techniczne dla modernizacji lub budowy linii kolejowych do prędkości Vmax≤200 km/h (dla taboru konwencjonalnego) / 250 km/h (dla taboru z wychylnym pudłem), Warszawa 2009.

SWITCH HEATING ELECTRICAL EQUIPMENT AND EXTERNAL LIGHTING AT PKP POLISH RAILWAY LINES

S u m m a r y

The article discusses the devices for electric heating of turnouts and external lighting mounted on the premises of PKP Polish Railway Lines. Switchgear electrical switchgear devices provide effective protection of turnouts in conditions of adverse weather conditions. Due to the high consumption of switchgear heating devices, ways to reduce electricity consumption are discussed. Lighting of traveling heads is iontended to increase the safety of running trains. Additionally, the article indicates the possibilities of effective lighting control in selected areas of the station during reduced train traffic. Basic requirements for the quality of electricity supplying equipment on railway areas have been presented.

Keywords: electric heating of turnouts, lighting of traveling heads, the quality of electricity

DOI: 10.7862/re.2017.10

Tekst złożono w redakcji: wrzesień 2017
Przyjęto do druku: październik 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (2/2017), lipiec-wrzesień 2017, s. 51-65

Przemysław KAŁUCKI[1]
Paweł DYMORA[2]
Mirosław MAZUREK[3]

BADANIE WYDAJNOŚCI WYBRANYCH SYSTEMÓW WIRTUALIZACJI

Obecnie koncepcja wirtualizacji wkroczyła praktycznie do każdej dziedziny informatyki. Wzrost mocy obliczeniowej serwerów sprawił, że optymalne wykorzystanie ich zasobów stało się istotnym problemem. Celem artykułu jest scharakteryzowanie wybranych rozwiązań technologicznych umożliwiających wirtualizację fizycznych serwerów. W artykule przedstawiono wybrane oprogramowanie do wirtualizacji systemów, a następnie przedstawiono badanie ich wydajności.

Słowa kluczowe: wirtualizacja, hyperwizor, ESXi, Hyper-V, XenServer

1. Wybrane oprogramowanie do wirtualizacji systemów

Wirtualizacja polega na wydzieleniu w obrębie jednego fizycznego serwera wielu (od kilku, nawet do kilkuset) znacznie mniejszych środowisk wirtualnych, rozszerzającym potencjał pojedynczego środowiska. Umożliwia efektywniejsze wykorzystanie istniejących zasobów sprzętowych środowiska informatycznego poprzez dowolne (w ramach możliwości sprzętowych czy programowych oraz założeń projektowych) modyfikowanie cech wirtualizowanych zasobów, dostosowując je do indywidualnych wymagań użytkownika. Istnieje szereg rozwiązań programowych realizujących wirtualizację, np. VMware ESXi, Hyper-V, XenServer, które to kolejno zostały scharakteryzowane poniżej.

1.1. VMware ESXi

VMware (https://www.vmware.com/) to istniejący na rynku od 1998 roku lider komercyjnych rozwiązań wirtualizacji i producent wirtualizatora typu 1, *Elastic Sky X integrated* (ESXi). ESXi to główna część bogatego pakietu

[1] Autor do korespondencji: Przemysław Kałucki, adres e-mail: pakalucki@gmail.com
[2] Paweł Dymora, Politechnika Rzeszowska, Zakład Systemów Złożonych, pawel.dymora@prz.edu.pl
[3] Mirosław Mazurek, Politechnika Rzeszowska, Zakład Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

do wirtualizacji i rozwiązań w chmurze vSphere. Wirtualizator ten bazuje na linuxowym jądrze i jest instalowany jako *bare-metal*, czyli bezpośrednio na sprzęcie. Jądro ESXi bezpośrednio zarządza zasobami korzystając z techniki *scan before execution*, dzięki czemu może wychwycić i obsłużyć wrażliwe i niebezpieczne instrukcje systemów gości. Wirtualizator dodatkowo wykorzystuje parawirtualne sterowniki dla wirtualnych urządzeń i obsługi operacji wejścia/wyjścia co znacznie poprawia wydajność. Maszyny wirtualne w ESXi działają z wykorzystaniem wsparcia sprzętowego z dodatkiem parawirtualizowanych sterowników dla optymalizacji operacji wejścia/wyjścia. Wirtualizatorem można zarządzać przez sieć, łącząc się za pomocą aplikacji vSphere Client (aplikacja desktopowa) lub vSphere Web Client (aplikacja webowa). Dodatkowo istnieje oprogramowanie będące częścią pakietu vSphere o nazwie vCenter Server. Może być ono zainstalowane na fizycznej bądź wirtualnej maszynie z systemem Windows Server 2012 lub jako samodzielna maszyna wirtualna bazująca na jądrze Linuxa. vCenter Server zapewnia dużo większą kontrolę nad wirtualizatorem ESXi, jak i daje możliwość zarządzania siecią kilkunastu wirtualizatorów [1].

1.2. Microsoft Hyper-V

Wirtualizator Hyper-V (www.microsoft.com/pl-pl/cloud-platform/virtualization) to istniejące na rynku od 2008 roku podejście do wirtualizacji firmy Microsoft. Może funkcjonować jako właściwość (ang. *feature*) doinstalowywana do systemów klasy Windows Server, Windows Pro i Enterprise (od wersji 8.1 w górę) lub jako oddzielny produkt działający w trybie *bare-metal*. Do zarządzania Hyper-V wykorzystuje się cienkiego klienta Hyper-V Manager, który tak jak sam wirtualizator można dodać jako właściwość do wcześniej wspomnianych systemów z rodziny Windows. Ten wirtualizator stosuje izolację maszyn wirtualnych na zasadzie partycji. Systemy operacyjne gości działają w oddzielnych partycjach, zaś główne procesy wirtualizatora działają w osobnej, głównej partycji. Zbiór funkcji i zasobów wirtualizatora, inaczej stos wirtualizacyjny ma z głównej partycji bezpośredni dostęp do sterowników sprzętowych. Partycja użytkowa nie ma ani dostępu do procesora, ani nie obsługuje prawdziwych przerwań. Wirtualizator może udostępnić partycjom maszyn wirtualnych fragment procesora, dzięki temu, że sam obsługuje przerwania i odpowiednio przekierowuje je wykorzystując mechanizm SynIC (ang. *Synthetic Interrupt Controller*). Maszyny wirtualne stworzone w Hyper-V posiadają przegląd dostępnych zasobów i sprzętu w postaci wirtualnych urządzeń. Każdy sygnał do wirtualnego urządzenia jest przekierowywany przez logiczny kanał zwany VMBus do głównej partycji, a odpowiedź tą samą drogą z powrotem do maszyny wirtualnej. W obrębie głównej partycji działa Dostawca Usługi Wirtualizacji (ang. *Virtualization*

Service Provider), który odpowiada za obsługę sygnałów otrzymanych od Konsumenta Usługi Wirtualizacji (ang. *Virtualization Service Client*) działającego w partycji użytkowej i zarządzającego sygnałami wysyłanymi przez maszyny wirtualne. Cały ten proces jest jawny dla systemu gościa. Całość opiera się na sprzętowym wsparciu wirtualizacji. Hyper-V 2016 jest oprogramowaniem komercyjnym z zamkniętymi źródłami, ale wersję samodzielną można za darmo pobrać ze strony producenta i użytkować, ciesząc się pełną funkcjonalnością [2-3].

1.3. Citrix XenServer

XenServer to projekt open source zarządzany przez firmę Citrix (http://xenserver.org/), dostarczający platformę do wirtualizacji bazującą na wirtualizatorze Xen. Xen zapoczątkowany był jako projekt naukowy w University of Cambridge, a pierwsze publiczne wydanie wirtualizatora Xen miało miejsce w 2003 roku. XenServer można za darmo pobrać ze strony produktu i używać w pełnej wersji. Dodatkowo istnieje możliwość rozszerzania platformy o funkcje i aplikacje produkowane przez firmy trzecie i innych użytkowników. Do zarządzania wirtualizatorem powstała aplikacja XenCenter przeznaczona na systemy Windows. Zarządzenie z innych systemów możliwe jest za pomocą innych aplikacji np. Xen Orchestra. Hyperwizor Xen to warstwa abstrakcji działająca bezpośrednio na sprzęcie, przed systemem operacyjnym. Oprócz zarządzania maszynami wirtualnymi jest dodatkowo odpowiedzialny za zarzadzanie procesorem i pamięcią operacyjną. Do działania całego środowiska konieczne jest funkcjonowanie maszyny wirtualnej zwanej *Domain 0*, w skrócie *Dom0*. Jest to automatycznie tworzona maszyna wirtualna zawierająca zmodyfikowane jądro systemu Linux, posiadająca specjalne prawa dostępu do fizycznych zasobów jak i możliwość interakcji z innymi maszynami wirtualnymi. *Dom0* posiada dwa sterowniki *Network Backend Driver* i *Block Backend Driver* pozwalające jej na zarządzanie dostępnymi interfejsami sieciowymi i dyskami. Pod nazwą *Domain U* kryje się przestrzeń, w której działają normalne maszyny wirtualne i ich systemy nie mające bezpośredniego dostępu do fizycznych zasobów. W Xen systemy gości mogą działać w trybie parawirtualizacji oraz w trybie pełnej wirtualizacji z wykorzystaniem wsparcia sprzętowego [4-6].

2. Badanie wydajności i efektywności wybranych rozwiązań wirtualizacji

2.1. Oprogramowanie testowe

Do wykonania testów wydajnościowych zdecydowano się na skorzystanie z narzędzia *SiSoftware Sandra Lite* (http://www.sisoftware.net/). Jest to

popularna i darmowa wersja programu diagnostycznego dla komputerów z systemami z rodziny Windows, umożliwiająca uruchomienie kompleksowego zestawu testów sprawdzających wszystkie istotne elementy systemu. W celu sprawdzenia wydajności maszyn wirtualnych uruchomiono pakiet składający się z testów wymienionych w tabeli 1 [7].

Tabela 1. Pakiety testów wydajnościowych
Table 1. Performance testing packages

Nazwa testu	Kategoria	Opis	Jednostka
Processor Multi-Media	Procesor	Wydajność jednostek Single Instruction, Multiple Data (SIMD). Im wyższy wynik tym lepiej.	Mpix/s – MegaPixels Per Second
Processor Cryptography	Procesor	Wydajność operacji szyfrowania, deszyfrowania i haszowania. Im wyższy wynik tym lepiej.	GB/s – GigaBytes Per Second
Processor Financial Analysis	Procesor	Wydajność procesora w przeprowadzaniu analizy finansowej za pomocą popularnych modeli. Im wyższy wynik tym lepiej.	kOPT/s – Kilo Options Per Second
Processor Scientific Analysis	Procesor	Wydajność procesora w przeprowadzaniu analizy naukowej za pomocą popularnych modeli. Im wyższy wynik tym lepiej.	GFLOPS – Giga Float Operations Per Second
.NET Arithmetic	Maszyna Wirtualna .NET	Wydajność obliczeń arytmetycznych w maszynie wirtualnej .NET Im wyższy wynik tym lepiej.	GOPS – Giga Operations Per Second
Memory Bandwidth	Pamięć operacyjna	Przepustowość pamięci operacyjnej. Im wyższy wynik tym lepiej.	GB/s - GigaBytes Per Second
Memory Latency	Pamięć operacyjna	Czas dostępu do pamięci operacyjnej. Im niższy wynik tym lepiej.	ns - nanosekundy
File System Bandwidth	Dysk	Wydajność systemu plików. Im wyższy wynik tym lepiej.	MB/s – MegaBytes Per Second

2.2. Metodologia badań

Do sprawdzenia wydajności i możliwości użytkowych wirtualizatorów zdecydowano się na przeprowadzenie kilku scenariuszy testowych:

- uruchomienie zestawu testów na jednej maszynie wirtualnej, gdy wszystkie pozostałe maszyny są nieaktywne;
- uruchomienie zestawu testów na jednej maszynie wirtualnej, kiedy łącznie aktywnych jest kolejno 30, 20, 15 i 10 maszyn;

- uruchomienie zestawu testów na wszystkich aktywnych maszynach w celu symulowania obciążenia, kolejno dla 30, 20, 15 i 10 maszyn.

Aby zmniejszyć wpływ błędu pomiaru na wyniki, wykonano 10 powtórzeń pomiarów dla każdego testu w każdym scenariuszu i obliczono średnie wyniki. Aktywna maszyna wirtualna oznacza, że dana maszyna jest uruchomiona i zakończył się proces inicjalizacji systemu operacyjnego. Za nieaktywną maszynę wirtualną uznaje się całkowicie wyłączoną maszynę. Na maszynach wirtualnych zainstalowano system Windows Server 2016. Do maszyn przydzielono zasoby w postaci 2 GB pamięci RAM oraz dwa wirtualne procesory. Dodatkowo maszyny działały jako połączone klony, dzieląc między sobą cześć plików systemowych i aplikacji [8].

2.3. Analiza wyników dla ESXI

Tabela 2 przedstawia średnie wyniki pomiarów uzyskane w testach wydajności maszyn wirtualnych w wirtualizatorze ESXi 6.5.0 dla scenariuszy testowych sprawdzających wydajność pojedynczej maszyny wirtualnej wraz ze zwiększającą się liczbą aktywnych łącznie maszyn, ale bez obciążania ich. Choć w teorii wirtualizator powinien dynamicznie alokować zasoby do maszyny wirtualnej, na której działa program przeprowadzający testy jako tej z największym zapotrzebowaniem i niwelować przez to spadek wydajności wynikający z braku zasobów, to jak widać wraz ze wzrostem liczby aktywnych maszyn, niewiele ale stopniowo pogarszają się też otrzymywane w testach wyniki, jednak nie dochodzi do sytuacji, w których obciążenie jest na tyle duże aby uniemożliwić płynne korzystanie z maszyn wirtualnych.

Tabela 2. Wyniki pomiarów dla ESXi bez obciążeń
Table 2. Data results for ESXi without load

Nazwa testu / Liczba maszyn	1	1 z 10	1 z 15	1 z 20	1 z 30	Jednostka
Processor Multimedia	83.272	82.633	82.621	82.406	82.112	Mpix/s
Processor Cryptography	2.982	2.899	2.888	2.868	2.814	GB/s
Processor Financial Analysis	5.941	5.940	5.922	5.901	5.880	kOPT/s
Processor Scientific Analysis	13.655	13.622	13.424	13.378	13.311	GFLOPS
.NET Arithmetic	9.830	9.171	9.021	8.888	8.599	GOPS
Memory Bandwidth	23.763	23.753	22.166	16.911	14.908	GB/s
Memory Latency	33.111	33.998	34.607	45.122	55.888	ns
File System Bandwidth	1774.112	1694.608	1678.690	1666.103	1653.513	MB/s

W Tabeli 3 umieszczono średnie rezultaty testów wydajności maszyn wirtualnych w scenariuszach testowych wprowadzających element obciążenia poprzez uruchomienie programu testującego na wszystkich aktywnych maszynach wirtualnych, kolejno dla coraz większej liczby maszyn, aż do 30. W tym przypadku już dla 28 maszyny można zaobserwować większe spadki w wydajności, a w ostatnim przypadku, kiedy aktywne i obciążone jest 30 maszyn wirtualnych można odczuć już problemy z płynnym użytkowaniem maszyn wirtualnych.

Tabela 3. Wyniki pomiarów dla ESXi z obciążeniem

Table 3. Data results for ESXi with load

Nazwa testu / Liczba maszyn	10	15	20	30	Jednostka
Processor Multimedia	58.346	43.193	40.429	40.414	Mpix/s
Processor Cryptography	1.639	1.293	1.098	0.995	GB/s
Processor Financial Analysis	3.948	2.759	1.999	1.535	kOPT/s
Processor Scientific Analysis	5.365	3.859	3.376	2.472	GFLOPS
.NET Arithmetic	6.530	4.699	3.631	2.644	GOPS
Memory Bandwidth	18.049	14.141	14.161	7.176	GB/s
Memory Latency	42.910	63.260	63.705	74.820	ns
File System Bandwidth	1599.061	1184.148	1017.989	839.566	MB/s

2.4. Analiza wyników dla Hyper-V

Tabela 4 prezentuje średnie wyniki uzyskane w testach wydajnościowych przez maszyny wirtualne działające w wirtualnej pracowni komputerowej zaimplementowanej w wirtualizatorze Hyper-V 2016 w scenariuszu testowym bez dodatkowego obciążenia. Choć wirtualizator powinien dynamicznie rozdzielać zasoby między maszynami wirtualnymi, tak aby nie występowały spadki wydajności wynikające z braku zasobów (kiedy jedna z maszyn ma większe zapotrzebowanie niż pozostałe) to mimo tego można zaobserwować spadek wydajności wraz ze wzrostem liczby aktywnych maszyn. Warto zwrócić też uwagę na szczególnie dobry wynik uzyskiwany przez maszyny wirtualne w Hyper-V w teście *File System Bandwidth* sprawdzającym prędkość systemu plików i dysku.

Tabela 4. Wyniki pomiarów dla Hyper-V bez obciążeń

Table 4. Data results for Hyper-V without load

Nazwa Testu / Liczba maszyn	1	1 z 10	1 z 15	1 z 20	1 z 30	Jednostka
Processor Multimedia	81.211	81.201	81.191	81.110	80.980	Mpix/s
Processor Cryptography	2.899	2.886	2.884	2.874	2.869	GB/s
Processor Financial Analysis	5.870	5.844	5.822	5.818	5.811	kOPT/s
Processor Scientific Analysis	12.573	12.466	12.433	12.417	12.399	GFLOPS
.NET Arithmetic	9.771	9.666	9.545	9.513	9.471	GOPS
Memory Bandwidth	23.409	23.110	22.998	22.989	22.983	GB/s
Memory Latency	31.633	32.211	32.134	32.101	32.033	ns
File System Bandwidth	4698.416	4567.512	4122.854	3889.899	3521.920	MB/s

W Tabeli 5 zaprezentowano rezultaty testów przeprowadzonych na maszynach wirtualnych w Hyper-V, w warunkach ze zwiększonym obciążeniem. Jak można się spodziewać w tym przypadku odnotowano już większe spadki wydajności we wszystkich testach. Ostatni z testów, dotyczący dysku i systemu plików wyprodukował znacznie lepsze wyniki, niż w innych sprawdzanych wirtualizatorach.

Tabela 5. Wyniki pomiarów dla Hyper-V z obciążeniem

Table 5. Data results for Hyper-V with load

Nazwa Testu / Liczba maszyn	10	15	20	30	Jednostka
Processor Multimedia	57.648	44.156	34.980	25.906	Mpix/s
Processor Cryptography	1.772	1.294	1.024	0.848	GB/s
Processor Financial Analysis	3.819	2.714	2.018	1.332	kOPT/s
Processor Scientific Analysis	5.315	3.828	2.875	2.213	GFLOPS
.NET Arithmetic	6.437	4.669	3.480	2.638	GOPS
Memory Bandwidth	20.712	20.023	13.798	11.036	GB/s
Memory Latency	37.080	42.967	46.865	61.153	ns
File System Bandwidth	4343.215	4003.142	3844.297	2296.898	MB/s

2.5. Analiza wyników dla XenServer

Tabela 6 prezentuje rezultaty testów wydajnościowych, w których nie symulowano obciążenia dla maszyn wirtualnych w środowisku zaimplementowanym z wykorzystaniem wirtualizatora XenServer. W tym przypadku, dla scenariuszy z mniejszą liczbą aktywnych maszyn wirtualnych można zaobserwować wysokie wyniki w testach sprawdzających wydajność procesora, jednak wraz ze wzrostem liczby aktywnych maszyn osiągane wyniki szybko ulegają pogorszeniu.

Tabela 6. Wyniki pomiarów dla XenServer bez obciążenia

Table 6. Data results for XenServer without load

Nazwa testu / Liczba maszyn	1	1 z 10	1 z 15	1 z 20	1 z 30	Jednostka
Processor Multimedia	100.520	98.510	96.501	88.767	88.440	Mpix/s
Processor Cryptography	3.994	3.579	3.163	3.101	2.985	GB/s
Processor Financial Analysis	7.280	7.170	7.060	6.999	6.480	kOPT/s
Processor Scientific Analysis	15.730	14.745	13.760	13.430	13.250	GFLOPS
.NET Arithmetic	10.960	10.465	9.970	8.410	8.260	GOPS
Memory Bandwidth	14.523	14.247	13.970	13.968	12.151	GB/s
Memory Latency	39.910	40.360	40.777	41.623	42.414	ns
File System Bandwidth	1327.855	1288.780	1259.705	1250.330	1241.380	MB/s

Tabela 7. Wyniki pomiarów dla XenServer z obciążeniem

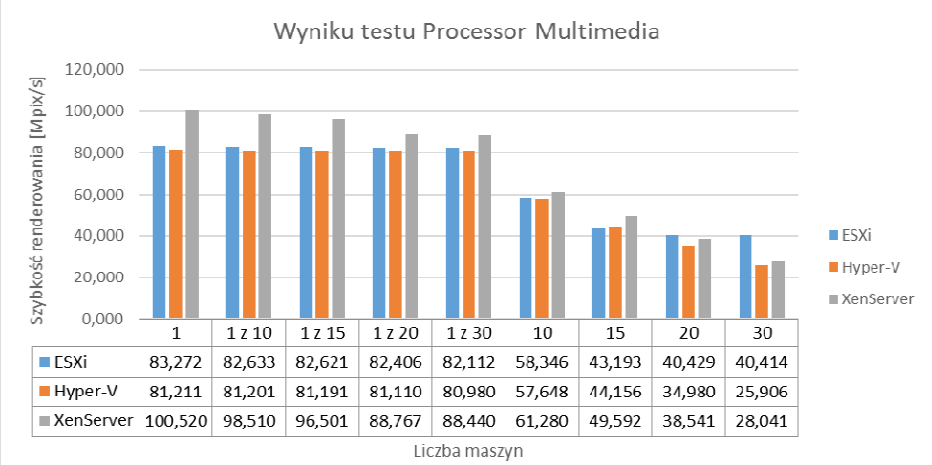
Table 7. Data results for XenServer with load

Nazwa testu / Liczba maszyn	10	15	20	30	Jednostka
Processor Multimedia	61.280	49.592	38.541	28.041	Mpix/s
Processor Cryptography	1.065	0.851	0.674	0.536	GB/s
Processor Financial Analysis	4.007	2.684	2.042	1.340	kOPT/s
Processor Scientific Analysis	3.830	3.177	2.205	1.890	GFLOPS
.NET Arithmetic	6.247	4.664	3.407	2.412	GOPS
Memory Bandwidth	5.451	5.134	3.984	3.864	GB/s
Memory Latency	77.720	95.200	144.825	158.540	ns
File System Bandwidth	709.070	425.858	246.361	156.107	MB/s

Rezultaty testów wydajnościowych w XenServer przedstawiono w Tabeli 7. Wprowadzono obciążenie poprzez uruchamianie programu testującego na coraz większej liczbie maszyn jednocześnie. Z otrzymanych wyników wynika, że powyżej progu 15 aktywnych i obciążonych maszyn wirtualnych, XenServer zaczyna osiągać wyraźnie gorsze wyniki niż pozostałe wirtualizatory, a w ostatnim przypadku, dla 30 równocześnie pracujących maszyn wirtualnych trudno jest wykonywać operacje w systemie gościa maszyn wirtualnych ze względu na opóźnienie.

2.6. Analiza porównawcza rezultatów symulacji

Na rysunku 1. przedstawiono rezultaty uzyskane przez wszystkie testowane wirtualizatory w teście *Processor Multimedia*, który sprawdza wydajność jednostek SIMD (ang. *Single Instruction Multiple Data*) procesora poprzez generowanie zestawu fraktali i przedstawia zdolność procesora do obsługi instrukcji związanych z danymi i instrukcjami występującymi podczas obróbki grafiki [7]. W otrzymanych wynikach można zaobserwować wyraźną przewagę wirtualizatora XenServer, aż do testu dla 20 i 30 maszyn wirtualnych, gdzie wyraźnie przestaje radzić sobie z obciążeniem i najlepsze wyniki zaczyna uzyskiwać ESXi. Wirtualizatory ESXi, Hyper-V i XenServer w tym teście odnotowały kolejno 51.467 %, 68.100 % i 72.103 % spadek wydajności pomiędzy testem przy najmniejszym obciążeniu a największym.



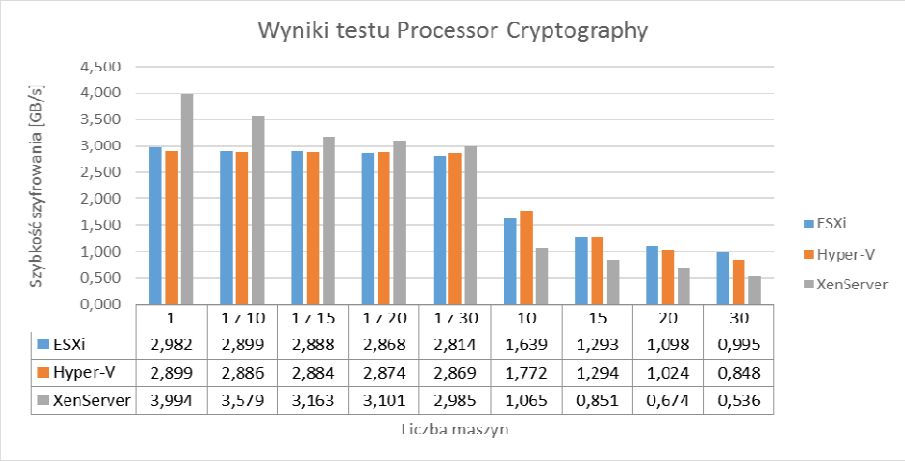
	1	1 z 10	1 z 15	1 z 20	1 z 30	10	15	20	30
ESXi	83,272	82,633	82,621	82,406	82,112	58,346	43,193	40,429	40,414
Hyper-V	81,211	81,201	81,191	81,110	80,980	57,648	44,156	34,980	25,906
XenServer	100,520	98,510	96,501	88,767	88,440	61,280	49,592	38,541	28,041

Rys. 1. Wyniki testu Processor Multimedia

Fig. 1. The results of the *Processor Multimedia* test

Rysunek 2. przedstawia rezultaty testu *Processor Cryptography*, który mierzy wydajność procesora w przeprowadzaniu typowych operacji wykonywanych na

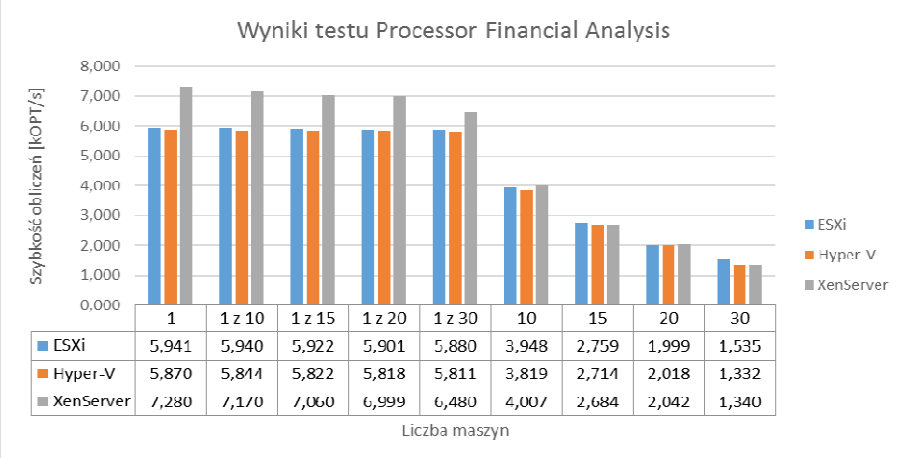
wrażliwych danych takich jak szyfrowanie, deszyfrowanie i haszowane danych używając algorytmów typu AES (ang. *Advanced Encryption Standard*) i SHA (ang. *Secure Hash Algorithm*) [7]. Tak jak we wcześniejszym teście najlepsze wyniki początkowo osiąga XenServer, wyraźnie tracąc prowadzenie wraz ze wzrostem obciążenia na rzecz ESXi i Hyper-V. Wirtualizatory ESXi, Hyper-V i XenServer w tym teście odnotowały kolejno 66.633 %, 70.749 % i 86.580 % spadek wydajności pomiędzy testem przy najmniejszym obciążeniu a największym.



	1	1 z 10	1 z 15	1 z 20	1 z 30	10	15	20	30
ESXi	2,982	2,899	2,888	2,868	2,814	1,639	1,293	1,098	0,995
Hyper-V	2,899	2,886	2,884	2,874	2,869	1,772	1,294	1,024	0,848
XenServer	3,994	3,579	3,163	3,101	2,985	1,065	0,851	0,674	0,536

Rys. 2. Wyniki testu *Processor Crypt*ography

Fig. 2. The results of the *Processor Cryptography* test



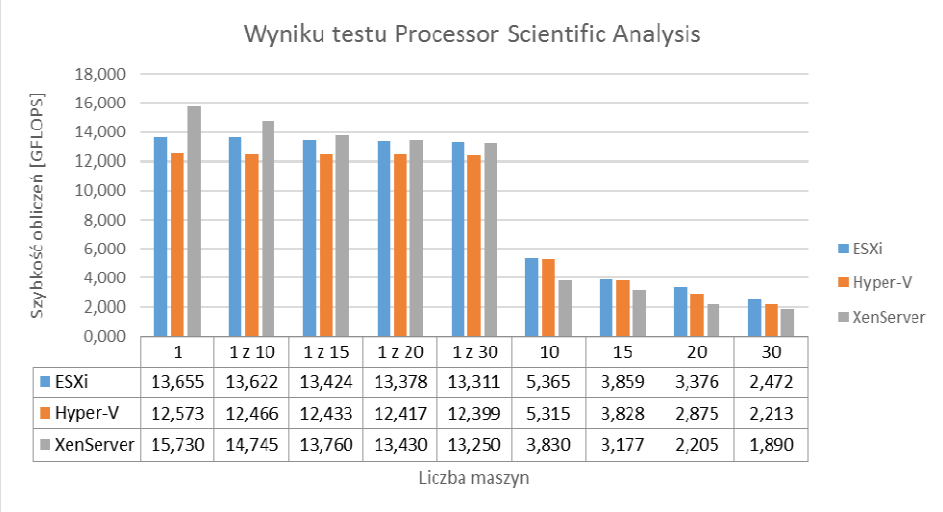
	1	1 z 10	1 z 15	1 z 20	1 z 30	10	15	20	30
ESXi	5,941	5,940	5,922	5,901	5,880	3,948	2,759	1,999	1,535
Hyper-V	5,870	5,844	5,822	5,818	5,811	3,819	2,714	2,018	1,332
XenServer	7,280	7,170	7,060	6,999	6,480	4,007	2,684	2,042	1,340

Rys. 3. Wyniki testu Processor Financial Analysis

Fig. 3. The results of the *Processor Financial Analysis* test

Na rysunku 3. przedstawiono porównanie rezultatów osiągniętych przez testowane wirtualizatory w kolejnych scenariuszach testowych w teście *Processor Financial Analysis*, który polega na sprawdzeniu wydajności procesora bazując na tym jak efektywnie wykonuje obliczenia z wykorzystaniem popularnych modeli stosowanych w finansach do określania przyszłej wartości akcji [7]. Przy mniejszym obciążeniu wirtualizator XenServer osiąga najlepsze wyniki. Wraz ze wzrostem obciążenia wirtualizatory zaczynają osiągać zbliżone wyniki, z niewielką przewagą dla ESXi. Wirtualizatory ESXi, Hyper-V i XenServer w tym teście odnotowały kolejno 74.163 %, 77.308 % i 81.593 % spadek wydajności pomiędzy testem przy najmniejszym obciążeniu a największym.

Wykres widoczny na rys. 4. przedstawia wyniki testu *Processor Scientific Analysis*, który mierzy wydajność procesora w wykonywaniu obliczeń takich jak operacje na macierzach czy transformata Fouriera [7]. Dla najmniejszego obciążenia najlepsze wyniki osiąga XenServer, a następnie ESXi. Wraz ze wzrostem obciążenia wydajność wirtualizatora XenServer wyraźnie spada, a ESXi osiąga nieznacznie lepsze wyniki niż Hyper-V. Wirtualizatory ESXi, Hyper-V i XenServer w tym teście odnotowały kolejno 81.897 %, 82.399 % i 87.985 % spadek wydajności pomiędzy testem przy najmniejszym obciążeniu, a największym.



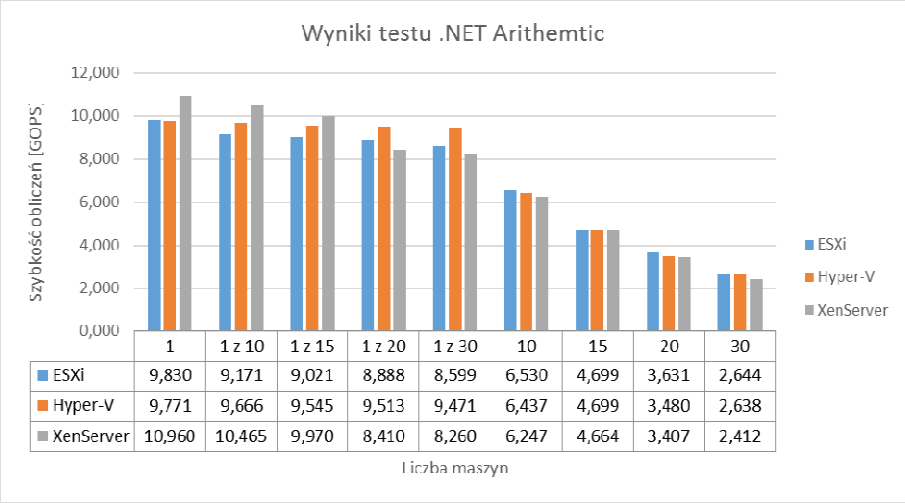
	1	1 z 10	1 z 15	1 z 20	1 z 30	10	15	20	30
ESXi	13,655	13,622	13,424	13,378	13,311	5,365	3,859	3,376	2,472
Hyper-V	12,573	12,466	12,433	12,417	12,399	5,315	3,828	2,875	2,213
XenServer	15,730	14,745	13,760	13,430	13,250	3,830	3,177	2,205	1,890

Rys. 4. Wyniki testu Processor Scientific Analysis

Fig. 4. The results of the *Processor Scientific Analysis* test

Test *.NET Arithmetic*, którego wyniki przedstawiono na rys. 5., mierzy wydajność wykonywania operacji arytmetycznych w frameworku .NET [7]. W tym przypadku dla testów przy najmniejszym obciążeniu najlepsze wyniki

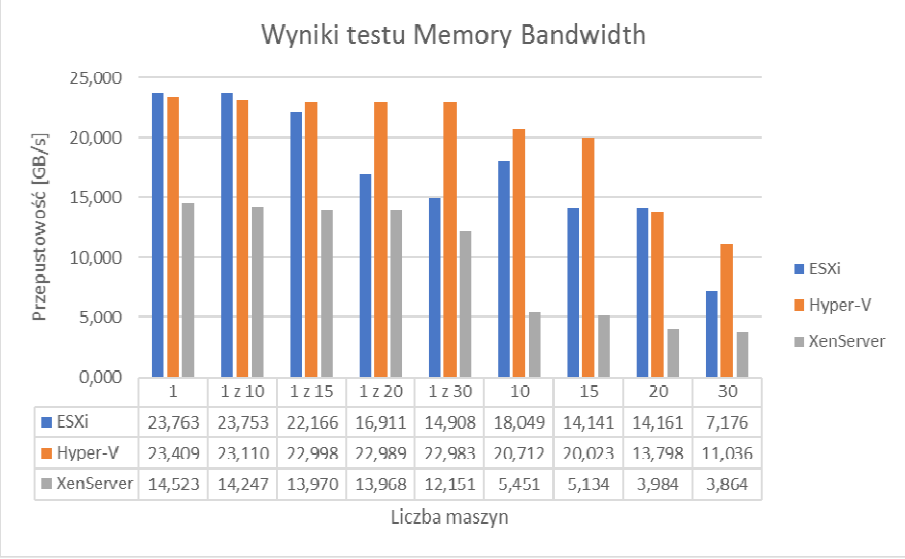
uzyskuje XenServer z wyjątkiem dla testu przy 1 z 20 i 1 z 30 maszyn wirtualnych, gdzie góruje Hyper-V. Wirtualizatory ESXi, Hyper-V i XenServer w tym teście zanotowały kolejno 73.103 %, 73.002 % i 77.993 % spadek wydajności pomiędzy testem przy najmniejszym obciążeniu a największym.



	1	1 z 10	1 z 15	1 z 20	1 z 30	10	15	20	30
ESXi	9,830	9,171	9,021	8,888	8,599	6,530	4,699	3,631	2,644
Hyper-V	9,771	9,666	9,545	9,513	9,471	6,437	4,699	3,480	2,638
XenServer	10,960	10,465	9,970	8,410	8,260	6,247	4,664	3,407	2,412

Rys. 5. Wyniki testu .NET Arithmetic

Fig. 5. The results of the *.NET Arithmetic* test

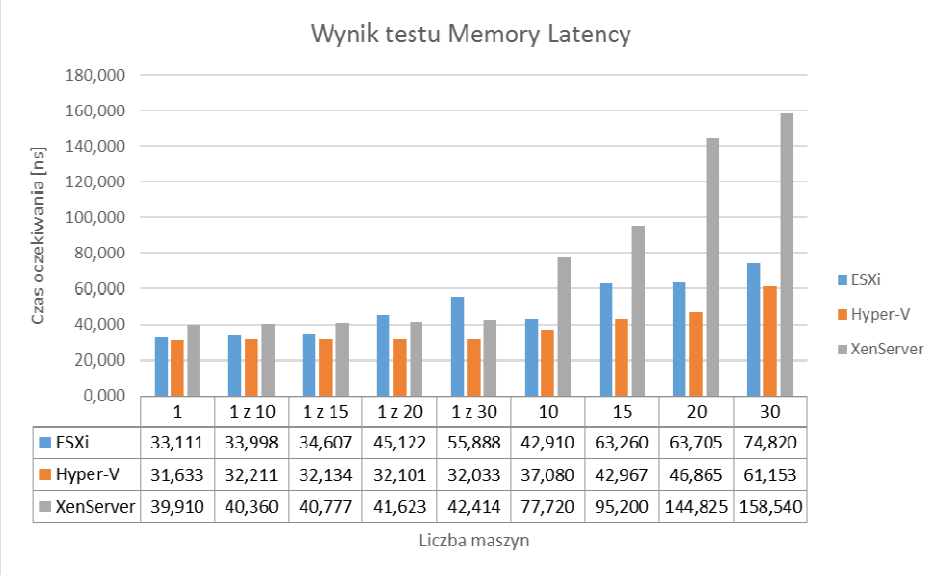


	1	1 z 10	1 z 15	1 z 20	1 z 30	10	15	20	30
ESXi	23,763	23,753	22,166	16,911	14,908	18,049	14,141	14,161	7,176
Hyper-V	23,409	23,110	22,998	22,989	22,983	20,712	20,023	13,798	11,036
XenServer	14,523	14,247	13,970	13,968	12,151	5,451	5,134	3,984	3,864

Rys. 6. Wyniki testu Memory Bandwidth

Fig. 6. The results of the *Memory Bandwidth* test

Test *Memory Bandwidth*, przedstawiony na rys. 6. czyli test przepustowości pamięci operacyjnej bazuje na popularnym benchmarku STREAM [7]. Dla tego testu najlepsze wyniki zaobserwowano dla wirtualizatorów ESXi i Hyper-V. Wraz ze wzrostem obciążenia wyraźnie lepsze wyniki zachowuje Hyper-V. Warto też zauważyć, że ESXi lepiej radzi sobie z mniejszą liczbą obciążonych maszyn niż większą działających bez obciążenia, porównując wynik dla testu 1 z 20 czy 1 z 30 do testu dla 10 i 15 maszyn. Wirtualizatory ESXi, Hyper-V i XenServer w tym teście odnotowały kolejno 69.802 %, 52.856 % i 73.394 % spadek wydajności pomiędzy testem przy najmniejszym obciążeniu a największym.

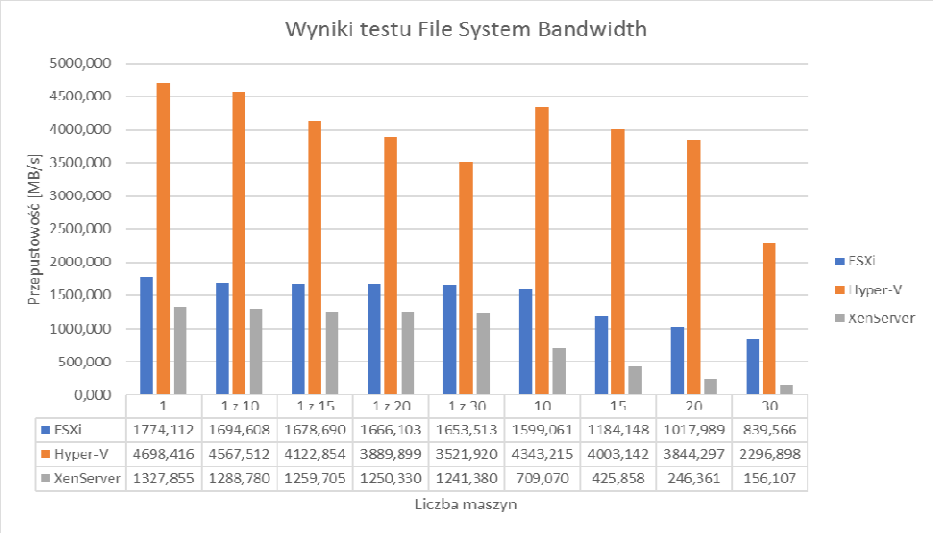


	1	1 z 10	1 z 15	1 z 20	1 z 30	10	15	20	30
ESXi	33,111	33,998	34,607	45,122	55,888	42,910	63,260	63,705	74,820
Hyper-V	31,633	32,211	32,134	32,101	32,033	37,080	42,967	46,865	61,153
XenServer	39,910	40,360	40,777	41,623	42,414	77,720	95,200	144,825	158,540

Rys. 7. Wyniki testu *Memory latency*

Fig. 7. The results of the *Memory Latency* test

Test *Memory Latency*, którego wyniki można zaobserwować na rys. 7. obrazuje czas odpowiedzi pamięci operacyjnej jako czas w nanosekundach potrzebny na uzyskanie danych z pamięci [7]. W każdym przypadku można zaobserwować, że najlepszy wynik uzyskuje Hyper-V, a następnie ESXi. XenServer odczuwa znaczny spadek wydajności wraz ze wzrostem obciążenia. Tak jak w poprzednim teście pamięci ESXi lepiej radzi sobie z mniejszą liczbą obciążonych maszyn niż z większą liczbą mniej obciążonych maszyn, w przeciwieństwie do reszty wirtualizatorów. Wirtualizatory ESXi, Hyper-V i XenServer w tym teście zanotowały kolejno 55.746 %, 48.272 % i 74.827 % spadek wydajności pomiędzy testem przy najmniejszym obciążeniu, a największym.



	1	1 z 10	1 z 15	1 z 20	1 z 30	10	15	20	30
ESXi	1774,112	1694,608	1678,690	1666,103	1653,513	1599,061	1184,148	1017,989	839,566
Hyper-V	4698,416	4567,512	4122,854	3889,899	3521,920	4343,215	4003,142	3844,297	2296,898
XenServer	1327,855	1288,780	1259,705	1250,330	1241,380	709,070	425,858	246,361	156,107

Rys. 8. Wyniki testu *File System Bandwidth*

Fig. 8. The results of the *File System Bandwidth* test

Test *File System Bandwidth*, którego wyniki przedstawia rys. 8., czyli test przepustowości systemu plików pokazuje wydajność operacji na dysku. Nie jest to wynik zależny wyłącznie od prędkości dysku, ale też od różnych czynników jak m.in. system plików, cache systemu operacyjnego czy pozycja dysku [7]. W tym teście znacznie lepsze wyniki uzyskuje wirtualizator Hyper-V, dodatkowo można zauważyć, że obciążenie ma w większości przypadków znacznie mniejszy wpływ na przepustowość systemu plików w Hyper-V i wirtualizator lepiej radzi sobie z mniejszą ilością obciążonych maszyn niż z większą ilością mniej obciążonych maszyn. Drugi w kolejności jest ESXi, natomiast najsłabsze wyniki osiąga XenServer. Wirtualizatory ESXi, Hyper-V i XenServer w tym teście odnotowały kolejno 52.677 %, 51.113 % i 88.244 % spadek wydajności pomiędzy testem przy najmniejszym obciążeniu, a największym.

3. Podsumowanie

Przeprowadzone dla poszczególnych wirtualizatorów testy wydajności oraz porównanie oferowanych funkcjonalności wykazały, że ESXi firmy VMWare oferuje w większości przypadków najstabilniejsze rezultaty przy zwiększającym się obciążeniu. Dodatkową kwestię, którą można poruszyć w tym porównaniu to dużo bogatszy od konkurencji pakiet funkcjonalności i opcji konfiguracji. Wadą tego rozwiązania jest konieczność zakupu licencji.

Kolejny wirtualizator, czyli Hyper-V firmy Microsoft osiągał porównywalne lub lepsze wyniki w testach wydajności (znacznie lepsze w testach dysku) jednak wyraźnie przeznaczony jest do działania w środowisku, gdzie wykorzystywane są tylko rozwiązania firmy Microsoft i w porównaniu do reszty ma ograniczoną funkcjonalność i jest trudniejszy w konfiguracji.

Ostatni z testowanych wirtualizatorów, jedyny reprezentant wolnego programowania, XenServer wyraźnie lepiej radził sobie z wirtualizacją operacji procesora przy niższych obciążeniach i choć natywnie nie oferuje tak wielu funkcjonalności jak ESXi, to ze względu na otwarte źródła i dużą, aktywną społeczność tworzącą rozszerzenia i ulepszenia, potencjalna możliwość rozbudowy i dostosowywania tego rozwiązania do własnych potrzeb jest ogromna.

Literatura

[1] http://www.vmware.com/products/vsphere-hypervisor.html, [dostęp: 10.12.2016].

[2] https://hyperv.veeam.com/blog/what-is-hyper-v-technology/, [dostęp: 10.12.2016].

[3] https://technet.microsoft.com/windows-server-docs/compute/hyper-v/hyper-vtechnology-overview, [dostęp: 10.12.2016].

[4] http://xenserver.org/, [dostęp: 10.12.2016].

[5] http://www-archive.xenproject.org/files/Marketing/HowDoesXenWork.pdf, [dostęp: 10.12.2016].

[6] Chris Takemura, Luke S. Crawford, The Book of Xen, NoStart Press 2010.

[7] Dokumentacja programu SiSoftware Sandra Lite

[8] https://www.vmware.com/support/ws5/doc/ws_clone_overview.html, [dostęp: 01.01.2017].

VIRTUALIZATION OF INFORMATION SYSTEMS

S u m m a r y

Nowadays concept of virtualization is common technology in almost every information technology based discipline. As the processing power of servers rise, it turns out that optimal use of available resources becomes meaningful issue. The purpose of this article is to summarize a few chosen virtualization platforms available for server virtualization. At the beginning, selected hypervisors and theirs characteristics are roughly described. Afterwards, results of overall performance tests inside environments implementing mentioned before hypervisors are presented and analyzed.

Keywords: virtualization, hypervisor, ESXi, Hyper-V, XenServer

DOI: 10.7862/re.2017.11

Tekst złożono w redakcji: wrzesień 2017
Przyjęto do druku: październik 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (2/2017), lipiec-wrzesień 2017, s. 67-78

Michał BALASA [1]
Paweł DYMORA[2]
Mirosław MAZUREK[3]

CZY NASZE DANE W CHMURZE SĄ BEZPIECZNE?

Błyskawiczny rozwój technologii oprogramowania oraz zwiększenie wydajności urządzeń przyczynia się do tworzenia nowoczesnych rozwiązań problemów, z którymi borykają się korporacje, firmy jak i zwykli użytkownicy chmury. Obecnie większość przedsiębiorstw nie wyobraża sobie pracy bez wykorzystania chmury do przechowywania swoich danych. Jednak jednym z największych problemów wykorzystania chmury to jej bezpieczeństwo. W artykule przedstawiono modele usług wraz z modelem rozmieszczenia chmur oraz rodzaje ataków.

Słowa kluczowe: chmura obliczeniowa, bezpieczeństwo, ataki

1. Czym jest „*Cloud Computing*”?

Wykorzystanie słowa chmura *(ang. Cloud)* dla opisania pomysłu Cloud Computingu nie jest przypadkowe. Chmura kojarzy się ze środowiskiem, czyli dostępnością. W biznesie liczy się przede wszystkim łatwość dostępu do danych, usług, aplikacji itp. Większość instytucji nie interesuje jak przebiega przetwarzanie w chmurze, a jej efekt końcowy, czyli gotowa platforma z naszymi aplikacjami i danymi. Interesujące jest co uzyskamy wykorzystując technologię Cloud Computingu i koszt tej usługi. Technologia chmury powinna być dostępna na żądanie podobnie jak energia elektryczna, gaz czy dostęp do źródeł wody [1].

2. Modele usług chmury obliczeniowej

Każdy użytkownik ma odrębne potrzeby i zastosowania dla chmury obliczeniowej. Jedni potrzebują gotowych aplikacji, niektórzy potrzebują systemu

[1] Autor do korespondencji: Michał Balasa, Politechnika Rzeszowska, Zakład Systemów Złożonych, adres e-mail: mbalasa123@gmail.com
[2] Paweł Dymora, Politechnika Rzeszowska, Zakład Systemów Złożonych, pawel.dymora@prz.edu.pl
[3] Mirosław Mazurek, Politechnika Rzeszowska, Zakład Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

operacyjnego, aby móc tworzyć własne aplikacje inni zaś potrzebują jedynie zasobów sprzętowych, żeby implementować własne rozwiązania systemowe. Wybiegając naprzeciw wymaganiom konsumentów firmy wprowadziły podział chmur obliczeniowych na trzy główne modele udostępniania usług: SaaS (ang. *Software as a Service*), PaaS (ang. *Platform as a Service*), IaaS (ang. *Infrastructure as a Service*) [2].

Wykorzystując oprogramowanie jako usługę *(ang. Software as a Service)* użytkownik uzyskuje dostęp do gotowej aplikacji poprzez przeglądarkę internetową lub gotowego programu. Korzystający nie musi zarządzać lub sterować infrastrukturą chmury, a nawet niektórych funkcji aplikacji z wyjątkiem spersonalizowanych ustawień konfiguracyjnych. Dużą zaletą tego modelu jest zniwelowanie kosztów zatrudniania wyspecjalizowanych osób w zakresie serwisu IT. Przykładem usługi SaaS jest Google Apps udostępniający pakiet aplikacji biurowych, kalendarz, pocztę mailową oraz serwis społecznościowy Google+. Schemat odpowiedzialności modelu SaaS przedstawiono na rys. 1. [2].

Rys. 1. Schemat odpowiedzialności modelu SaaS

Fig. 1. Responsibility scheme of the SaaS model

Rys. 2. Schemat odpowiedzialności modelu PaaS

Fig. 2. Responsibility scheme of the PaaS model

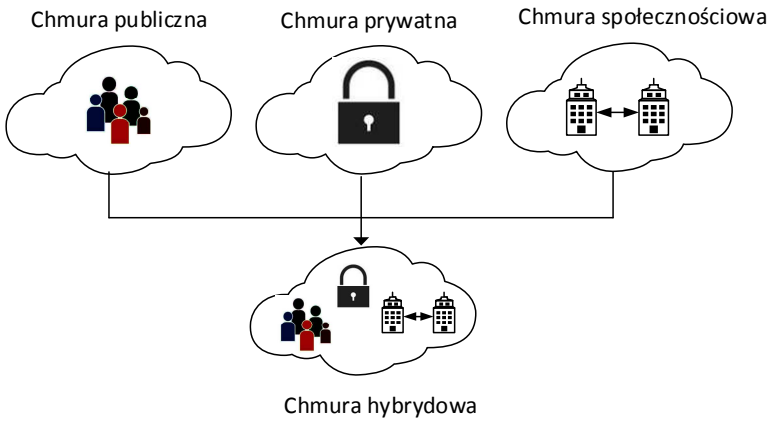
Wykorzystując platformę jako usługę *(ang. Platform as a Service)* użytkownik uzyskuje dostęp do całej usługi – najczęściej jest to zainstalowany system operacyjny z bazą danych. Deweloperzy oprogramowania oraz aplikacji internetowych mogą tworzyć i uruchamiać swoje oprogramowanie bez konieczności zakupu i serwisowania urządzeń fizycznych, a także infrastruktury sieciowej czy programowej. Przykładem usługi PaaS jest Microsoft Azure udostępniający swoje gotowe rozwiązania systemowe użytkownikom chcącym tworzyć aplikacje na systemie firmy Microsoft. Schemat odpowiedzialności modelu PaaS przedstawiono na rys. 2. [2].

W modelu infrastruktura jako usługa *(ang. Infrastructure as a Service)* użytkownik uzyskuje dostęp do gotowych zasobów obliczeniowych oraz infrastruktury sieciowej. Odbiorca może wdrażać dowolne oprogramowanie, które

może zawierać systemy operacyjne oraz aplikacje. Może także kontrolować systemy operacyjne, magazyny danych, a także zainstalowane oprogramowanie, lecz nie może zarządzać infrastrukturą chmury i ma ograniczony dostęp do kontroli ustawień sieci (np. Zapory sieciowej hosta) [2]. Przykładem usługi IaaS jest Amazon Elastic Compute Cloud, która pozwala na tworzenie własnych obrazów maszyn wirtualnych, dodawanie własnych instancji oraz zarządzanie nimi. Schemat odpowiedzialności modelu PaaS do funkcjonalności, za które odpowiada użytkownik wymienia: *Aplikacje, Środowisko, Bezpieczeństwo, Bazy danych oraz System operacyjny*. Pozostałe funkcje (*Wirtualizacja*, Serwery, *Pamięć masowa* i *Sieć* to odpowiedzialność dostawcy.

3. Modele rozmieszczenia chmury obliczeniowej

- **Chmura prywatna** (ang. *Private Cloud*) umiejscowiona jest najczęściej na terenie firmy, która ją wykorzystuje aby zapewnić najwyższe bezpieczeństwo danych. Chmura ta jest wykorzystywana oraz zarządzana przez jedną organizację, lecz w wyjątkowych przypadkach dopuszcza się możliwość umiejscowienia chmury w firmie zewnętrznej. Jedyny dostęp do zasobów chmury może mieć firma wykupująca usługę. Często do zaprojektowania chmury wykorzystywana jest istniejąca infrastruktura firmy.
- **Chmura publiczna** (ang. *Public Cloud*) w przeciwieństwie do chmury prywatnej umiejscowiona jest w firmie zewnętrznej. Organizacja wykupująca ofertę chmury publicznej nie musi być wyposażona w serwerownie, oprogramowanie jak również infrastrukturę, ponieważ jest własnością dostawcy, który odpowiada także za jej zarządzanie. Klient łącząc się poprzez sieć za odpowiednią opłatą uzyskuje dostęp do aplikacji lub zasobów sprzętowych chmury. Chmury publiczne cechują się większą podatnością na ataki z zewnątrz.
- **Chmura społecznościowa** (ang. *Community Cloud*) wykorzystywana jest do komunikacji grup pracujących nad wspólnym projektem, zadaniem lub celem. Znajduje zastosowanie w pojedynczych organizacjach jak i w kilku firmach, które łączą wspólne cele biznesowe. Chmurą zarządza jedna z organizacji wchodząca w skład chmury lub przez firmę zewnętrzną.
- **Chmura hybrydowa** (ang. *Hybrid Cloud*) jest połączeniem chmury publicznej, prywatnej i społecznościowej. Łącząc kilka chmur zachowujemy odrębność każdej z nich, umożliwiając zabezpieczoną komunikację, a także udostępnianie wybranych zasobów. Obecnie jest najczęściej wybieranym modelem przez przedsiębiorstwa ze względu na jej wszechstronność zastosowania – najważniejsze dane przechowujemy w chmurze prywatnej, dane mniej newralgiczne przechowujemy w chmurze publicznej.



Rys. 3. Model rozmieszczenia chmur

Fig. 3. Cloud deployment model

4. Bezpieczeństwo chmury obliczeniowej

Chmura obliczeniowa z założenia umożliwia dostęp do swoich zasobów z każdego miejsca oraz w każdej chwili przez wiele osób jednocześnie. Jednak z łatwością dostępu do chmury łączą się problemy z jej bezpieczeństwem co jest najczęstszym powodem rezygnacji z jej wdrożenia w firmie. Zdecydowana większość przedsiębiorstw nie wyobraża sobie aby ich dane wyciekły poza „mury" firmy. Użytkownicy wybierając oferty chmur obliczeniowych od różnych dostawców najczęściej wybierają dostawców w zależności od jakości bezpieczeństwa ich danych jak również ceny, którą proponują firmy w zamian za zasady bezpieczeństwa. Wiele publikacji uczula odbiorców cloud computingu na to aby na pierwszym miejscu stawiali bezpieczeństwo swoich danych. Największe zagrożenie upublicznienia danych stwarza chmura publiczna w modelu Software as a Service. Wszystkie dane oraz usługi w tym modelu są pod całkowitą kontrolą firmy oferującej usługę – provider zgodnie z umową zawartą z klientem musi zapewnić bezpieczeństwo całej infrastruktury sprzętowej jak i programowej [3].

Największe bezpieczeństwo naszych danych zapewnia chmura prywatna o modelu IaaS, ponieważ o bezpieczeństwo danych dba organizacja, która wykorzystuje daną chmurę. Dane z wykorzystanych usług nie są przekazywane do organizacji zewnętrznych, jednak zaprojektowanie tego modelu chmury wymaga od nas większych nakładów finansowych. Za bezpieczeństwo chmury (w zależności od wielkości instytucji) tzn. jej bezawaryjne działanie i zabezpieczenie transmisji danych odpowiedzialna jest grupa wykwalifikowanego personelu. Kolejną potrzebą jest inwestycja sporych środków finansowych na stwo-

rzenie własnych punktów przechowywania danych (serwerownie, infrastruktura sieciowa itd.).

W przypadku wdrożenia nowej usługi najczęściej nie wystarczy obecna infrastruktura, a modernizacja może się opłacić jeżeli projektant odpowiednio wyskalował sieć na przyszłe rozbudowy [3].

5. Rodzaje ataków na chmurę obliczeniową

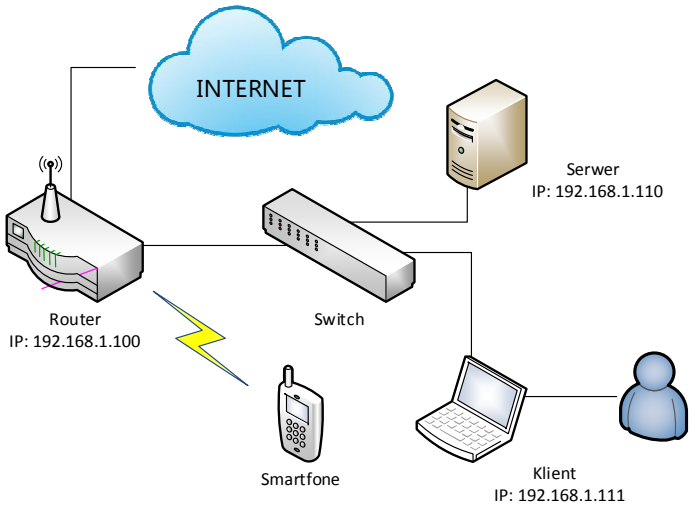
Zabezpieczenie chmury jest bardzo trudnym zadaniem, ponieważ na bezpieczeństwo chmury ma wpływ wiele czynników tzn. zaczynając od zabezpieczenia fizycznego poprzez politykę bezpieczeństwa w przedsiębiorstwie korzystającym z usługi przetwarzana w chmurze, zatem jest bardzo wiele możliwości potencjalnych sposobów zaatakowania chmury [4].

- **Application Attack** - jak sama nazwa wskazuje jest skierowany w aplikację. W celu jej zaatakowania tworzony jest exploit, który wykorzystuje luki w przestarzałym oprogramowaniu, aby uzyskać dostęp do aplikacji, która nie jest uruchomiona. Przykładowym i najbardziej popularnym tego typu atakiem jest przepełnienie bufora na stosie.
- **Brute Force** - atak służy do łamania haseł zabezpieczających chmurę. Polega na podjęciu dużej ilości prób złamania hasła dostępowego. Dobrym zabezpieczeniem przed tego typu włamaniem jest ograniczenie prób logowania z blokadą czasową. W ten sposób w 2014 roku złamano zabezpieczenia chmur firmy Apple uzyskując dostęp do prywatnych zasobów najsłynniejszych celebrytów.
- **Malware/botnet activity** - atak skierowany głównie w duże korporacje polegający na rozprzestrzenianiu szkodliwego oprogramowania na komputerach niszcząc lub pobierając informację jak również tworząc drogi dostępowe do komputera (ang. *back door*). Urządzenia infekowane są poprzez atak bezpośredni lub spam mailowy.
- **Misconfiguration** - atak wykorzystuje błędy w konfiguracji sieci, podłączonych komputerów oraz aplikacji. Przyczyną ataków jest brak zainstalowanych najnowszych poprawek, a także niedbałość administratorów sieci, ponieważ błędne skonfigurowanie aplikacji może spowodować utworzenie luki w systemie operacyjnym czyniąc go łatwym celem. Z roku na rok staje się coraz mniej spotykanym atakiem, ponieważ administratorzy maja coraz większą wiedzę na temat bezpieczeństwa i są wyczuleni na aktualizację oprogramowania.
- **Reconnaissance i Vulnerability scans** - do rozpoczęcia powyższych ataków wystarczy bardzo prosty i łatwo dostępny program do podsłuchu i skanowania sieci. Jednak wystarczy zaktualizowane oprogramowanie antywirusowe, aby ustrzec się tego rodzajów ataku.

- **Web Application Attack** - atak skierowany na aplikacje webowe jest jednym z najniebezpieczniejszych ataków, ponieważ w łatwy sposób uzyskuje dostęp do aplikacji jak również jest bardzo ciężki do powstrzymania. Wystarczy zainstalować odpowiednie oprogramowanie (np. HAVIJ), aby wykonać atak SQL Injection, które jest najpopularniejszym rodzajem ataku na aplikacje internetowe.

6. Test chmur do przechowywania danych

Test wydajności chmur przeprowadzono dla operacji przesyłania pliku o rozszerzeniu .7z (ok. 130 MB), 32 zdjęć JPEG (100 MB) oraz pobraniu pliku .7z, a także 32 zdjęć JPEG wcześniej przesłanych do chmury. W celu otrzymania dokładniejszych wyników testu, każdą procedurę powtórzono 10 krotnie, policzono z nich średnią arytmetyczną oraz ustawiono pobieranie danych dla Internetu jak również sieci lokalnej na poziomie pobierania i wysyłania plików – 10 Mbit/s.



Rys. 4. Topologia testowa dla przesyłania danych

Fig. 4. Test topology for data transfer

Eksperymenty przeprowadzono na przeglądarce Google Chrome 51.0.2704.79 oraz łączu internetowym osiągającym średnio wartość odbierania i wysyłania pakietów na poziomie 25 Mbit/s. Aby ograniczyć prędkość łącza internetowego/lokalnego wykorzystano program NetLimiter 4. Aby obliczyć czas potrzebny na pobranie/wysłanie pliku użyto programu Wireshark 2.0.4.

Na rysunku 4. przedstawiono topologię na której zostały przeprowadzone testy, a w tabeli 1 zestawiono otrzymane rezultaty.

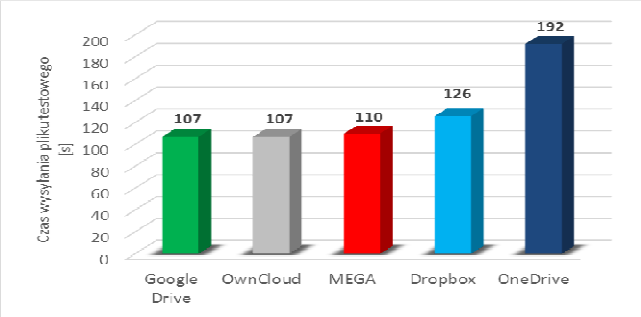
Tabela 1. Wyniki testów dla ograniczonego ruchu – 10 Mbit/s
Table 1. Test results for limited traffic – 10 Mbit/s

10 Mbit/s	Wysyłanie pliku 7z 130 MB	Wysyłanie 32 zdjęć JPEG 100 MB	Pobieranie pliku 7z 130 MB	Pobieranie 32 zdjęć JPEG 100 MB
Dropbox	Test 1: 127s Test 2: 126s … Test 10: 126s **Średnia: 126s**	Test 1: 143s Test 2: 145s … Test 10: 146s **Średnia: 145s**	Test 1: 107s Test 2: 108s … Test 10: 108s **Średnia: 108s**	Test 1: 85s Test 2: 85s … Test 10: 85s **Średnia: 85s**
Google Drive	Test 1: 108s Test 2: 107s … Test 10: 107s **Średnia: 107s**	Test 1: 105s Test 2: 106s … Test 10: 105s **Średnia: 105s**	Test 1: 108s Test 2: 107s … Test 10: 108s **Średnia: 108s**	Test 1: 96s Test 2: 96s … Test 10: 97s **Średnia: 96s**
MEGA	Test 1: 111s Test 2: 109s … Test 10: 111s **Średnia: 110s**	Test 1: 102s Test 2: 101s … Test 10: 104s **Średnia: 102s**	Test 1: 114s Test 2: 114s … Test 10: 115s **Średnia: 114s**	Test 1: 107s Test 2: 106s … Test 10: 105s **Średnia: 106s**
OneDrive	Test 1: 192s Test 2: 197s … Test 10: 187s **Średnia: 192s**	Test 1: 85s Test 2: 86s … Test 10: 86s **Średnia: 86s**	Test 1: 107s Test 2: 107s … Test 10: 106s **Średnia: 107s**	Test 1: 170s Test 2: 173s … Test 10: 175s **Średnia: 173s**
OwnCloud	Test 1: 106s Test 2: 107s … Test 10: 107s **Średnia: 107s**	Test 1: 82s Test 2: 82s … Test 10: 82s **Średnia: 82s**	Test 1: 108s Test 2: 107s … Test 10: 107s **Średnia: 82s**	Test 1: 87s Test 2: 88s … Test 10: 87s **Średnia: 87s**

6.1. Test wysyłania pliku 7z – ograniczenie ruchu 10 Mbit/s

Doświadczenie zostało przeprowadzone poprzez wysyłanie skompresowanego filmu z wykorzystaniem kompresji danych 7z. Najlepiej z zadaniem poradziły sobie chmury Google Drive, ownCloud, które wysłały pliki w czasie 107

sekund. Najgorszy rezultat uzyskała chmura OneDrive (czas przesyłania wyniósł 192 sekundy) prawdopodobnie przez słabą współpracę z plikami o 7z. Różnica pomiędzy najlepszym i najgorszym wynikiem wyniosła 85 sekund. Na rysunku 5. przedstawiono porównanie średniego czasu wysyłania pliku. Kolory na wykresie oznaczają kolor przewodni producenta chmury.

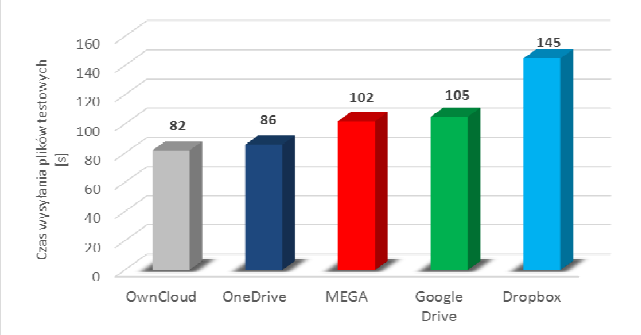


Rys. 5. Wysyłanie pliku 7z o rozmiarze 130 MB - 10 Mbit/s

Fig. 5. Sending 7z file of size 130 MB - 10 Mbit/s

6.2. Test wysyłania 32 zdjęć JPEG – ograniczenie ruchu 10 Mbit/s

Kolejny test został przeprowadzony z wykorzystaniem przesyłania 32 zdjęć o rozszerzeniu JPEG zrzuconych do jednego folderu, lecz nieskompresowanych, aby sprawdzić opcje kolejkowania poszczególnych platform. Najszybciej zdjęcia zostały przesłane w chmurze OwnCloud.



Rys. 6. Wysyłanie 32 zdjęć JPEG o rozmiarze 100 MB

Fig. 6. Sending 32 JPEG images of size 100 MB

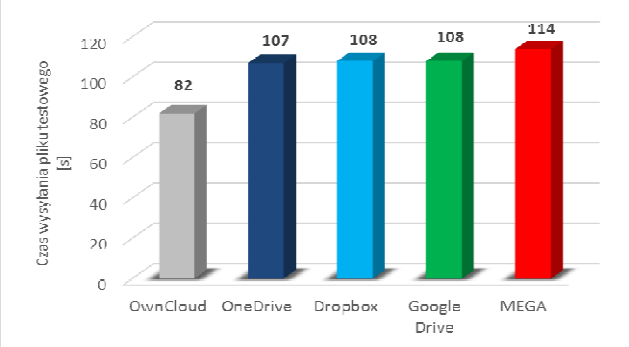
Do przesłania danych wystarczyło 82 sekundy. Najwolniej swoje zadanie wykonała chmura Dropbox, ponieważ po każdym przesłanym zdjęciu indeksowała pliki powodując opóźnienia w wysyłaniu (czas przekazywania – 145 sekund), jednak należy wyróżnić indeksowanie plików także jako zaletę, ponie-

waż pliki są dokładnie przesyłane do chmury zapewniając dokładność w przekazywaniu plików z komputera klienta na serwer. Różnica czasowa pomiędzy najlepszym i najgorszym rezultatem wyniosła 63 sekundy. Na rysunku 6. przedstawiono porównanie średniego czasu przekazywania zdjęć.

6.3. Test pobierania pliku 7z – ograniczenie ruchu 10 Mbit/s

Eksperyment wykonano za pomocą pobierania skompresowanego filmu z wykorzystaniem kompresji danych 7z. Chmura ownCloud pobrała plik w czasie 82 sekund, czyli najszybciej z testowanych rozwiązań. Pozostałe chmury uzyskały bardzo zbliżone rezultaty pobierania: OneDrive - 107 sekund, Dropbox – 108 sekund, Google Drive - 108 sekund i MEGA – 114 sekund. Różnica pomiędzy chmurami wyniosła 32 sekundy.

Na rysunku 7 przedstawiono porównanie średniego czasu pobierania pliku.

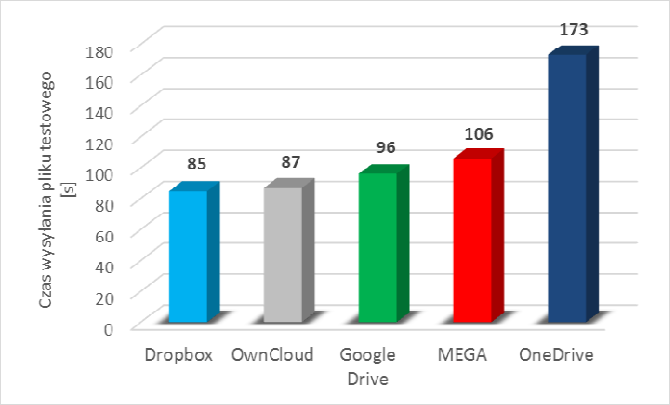


Rys. 7. Pobieranie pliku 7z o rozmiarze 130 MB - 10 Mbit/s

Fig. 7. Download 7z file size 130 MB - 10 Mbit/s

6.4. Test pobierania 32 zdjęć JPEG – ograniczenie ruchu 10 Mbit/s

Kolejny test został przeprowadzony za pomocą operacji pobierania 32 zdjęć o rozszerzeniu JPEG dodanych do jednego folderu. Dla dokładniejszego sprawdzenia pobierania zdjęć wybrano pobieranie razem z kompresją, więc platformy musiały dodatkowo skompresować zdjęcia. Wyniki eksperymentu wskazują, że chmura Dropobox osiągnęła najlepszy rezultat z czasem 85 sekund. O 2 sekundy wolnej pliki pobrano z platformy ownCloud. Najwolniej pliki pobrano z usługi OneDrive, ponieważ chmura bardzo długo „pakowała” pliki. Różnica pomiędzy najlepszym i najgorszym czasem wyniosła 88 s, czyli z chmury OneDrive dwukrotnie dłużej pobierano pliki niż z Dropboxa i OwnCloud. Na rysunku 8. przedstawiono porównanie średniego czasu pobierania zdjęć dla tego testu.



Rys. 8. Pobieranie 32 zdjęć JPEG o rozmiarze 100 MB - 10 Mbit/s

Fig. 8. Download 32 JPEG images of 100 MB - 10 Mbit/s

6.5. Porównanie bezpieczeństwa chmur do przechowywania danych

W celu przedstawienia różnic dotyczących bezpieczeństwa pomiędzy przedstawionymi rozwiązaniami stworzono tabelę 2. Porównanie bezpieczeństwa przeprowadzono dla chmur w darmowych pakietach. W tabeli 2. porównywano czy chmury mają możliwość weryfikacji dwuetapowej, zabezpieczenie SSL, rodzaj zabezpieczenie AES, czy indeksowane są pojedyncze pliki podczas przesyłania oraz możliwość przywracania usuniętych plików z kosza.

Tabela 2. Porównanie bezpieczeństwa chmur

Table 2. Comparison of cloud security

Nazwa dostawcy	Weryfikacja dwuetapowa	SSL	Rodzaj AES	Indeksowanie pojedynczych plików	Przywracanie plików z kosza
Dropbox	TAK	TAK	AES-256	TAK	TAK
Google Drive	TAK	TAK	AES-256	NIE	TAK
MEGA	NIE	TAK	AES-256	NIE	TAK
OneDrive	NIE	TAK	BRAK	NIE	TAK
OwnCloud	NIE	TAK	AES-256	NIE	TAK

Z przeprowadzonego porównania wynika że najbezpieczniejszym rozwiązaniem dla naszych plików jest wykorzystanie chmury Dropbox, a najmniej bezpieczną chmurą jest rozwiązanie firmy Microsoft – OneDrive.

7. Podsumowanie

Wykorzystanie chmury do przechowywania danych wiąże się z koniecznością wykorzystania sieci do przesłania danych (często bardzo ważnych lub prywatnych). Korzystając z rozwiązań chmury prywatnej mamy dużo większą szansę, że nasze dane nie wejdą w posiadanie osób trzecich, ponieważ cała infrastruktura opiera się na zasobach sprzętowych oraz topologii sieciowej naszej firmy. Rozwiązanie to jednak łączy się z dużymi kosztami utrzymania infrastruktury oraz kosztami przygotowania urządzeń, które umożliwią swobodne korzystanie z naszych danych. Chmura publiczna umożliwia nam dostęp do naszych danych z każdego miejsca, ponieważ za dystrybucję odpowiada firma zewnętrzna. Zatem za miesięczny/roczny abonament uzyskujemy dostęp do danych bez konieczności dbania o naszą infrastrukturę. Wiąże się to jednak z tym że firma zewnętrzna ma na swoich serwerach nasze dane, a my nie mamy wpływu na zabezpieczenia takiego serwera. Podczas ataku na serwery takiej firmy nasze dane mogą zdobyć osoby trzecie lub możemy je po prostu utracić. Przeglądając oferty oraz możliwości chmur musimy podjąć decyzję jak istotne będą przechowywane tam dane. Tworząc chmurę dla naszej firmy powinniśmy też zastanowić się na utworzeniem kopii zapasowej danych, które przesyłamy do chmury.

Decyzję o rodzaju wykorzystanej chmury należy podjąć po analizie ilości przesyłanych danych, ilości użytkowników wykorzystujących oprogramowanie oraz możliwości finansowych do utworzenia oraz utrzymania ewentualnej infrastruktury. Podczas wykorzystywania chmury należy pamiętać o przestrzeganiu podstawowych zasad bezpieczeństwa: przestrzegania zasad bezpiecznych haseł, posiadania aktualnego oprogramowania antywirusowego oraz zablokowanie dostępności osobom trzecim do własnego konta. Bezpieczeństwo naszych danych w większości przypadków zależy od nas i od tego w jaki sposób dbamy o ich zabezpieczenie.

Literatura

[1] Aljawarneh S.: *Cloud Computing Advancements in Design, Implementation and Technologies*, Isra University, Jordan 2013.
[2] Mell P., Grance T.: *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, Gaithersburg 2011.
[3] Mather T., Kumaraswamy S., Latif S.: *Cloud Security and Privacy. An Enterprise Perspective on Risks and Comliance*, O'Reilly Media Inc. United States of America 2009.
[4] http://websecurity.pl/tag/chmura-zagrozenia/, [dostęp: 10.04.2017].

IS OUR DATA SAFE IN THE CLOUD?

S u m m a r y

Rapid development in software technology and increase in efficiency of devices lead to finding new solutions for problems that corporations, companies, as well as common users of the cloud faced for years. Currently, most companies cannot imagine working without the cloud, where their data can be stored. One of the biggest issues concerning the cloud is the safety of its usage. The article shows various service and deployment models along with types of attacks.

Keywords: computing cloud, cloud security, attacks on the cloud

DOI: 10.7862/re.2017.12

Tekst złożono w redakcji: wrzesień 2017
Przyjęto do druku: październik 2017

Informacje dodatkowe

1. Lista recenzentów współpracujących będzie opublikowana w numerze 296 Zeszytów Naukowych Politechniki Rzeszowskiej, Elektrotechnika z. 36 (4/2017) oraz zamieszczona na stronie internetowej:

   http://oficyna.prz.edu.pl/pl/zeszyty-naukowe/elektrotechnika/

2. Zasady recenzowania są udostępnione na stronie internetowej:

   http://oficyna.prz.edu.pl/zasady-recenzowania/

3. Informacje dla autorów artykułów są udostępnione na stronie internetowej:

   http://oficyna.prz.edu.pl/informacje-dla-autorow/

4. Formularz recenzji jest udostępniony na stronie internetowej:

   http://oficyna.prz.edu.pl/pl/zeszyty-naukowe/elektrotechnika/

5. Instrukcja dla autorów omawiająca szczegółowo strukturę artykułu, jego układ, sposób przygotowywania materiału ilustracyjnego i piśmiennictwa jest zamieszczona na stronach internetowych:

   http://oficyna.prz.edu.pl/pl/instrukcja-dla-autorow/

   oraz

   http://oficyna.prz.edu.pl/pl/zeszyty-naukowe/elektrotechnika/

   w zakładce „Instrukcja dla autorów".

6. Dane kontaktowe do redakcji czasopisma, adresy pocztowe i e-mail do przesłania artykułów oraz dane kontaktowe do wydawcy są podane na stronie internetowej (Komitet Redakcyjny):

   http://oficyna.prz.edu.pl/pl/zeszyty-naukowe/elektrotechnika/

Zasady recenzowania, informacje dla autorów, formularz recenzji, instrukcja dla autorów i dane kontaktowe do redakcji czasopisma i wydawcy będą również opublikowane w czwartym numerze *Zeszytów Naukowych Politechniki Rzeszowskiej, Elektrotechnika*, z. 36 (4/2017).

Nakład 80 egz. Ark. wyd. 4,33. Ark. druk. 5,0. Papier offset. 80g B1.
Oddano do druku w grudniu 2017 r. Wydrukowano w grudniu 2017 r.
Drukarnia Oficyny Wydawniczej, al. Powstańców Warszawy 12, 35-959 Rzeszów
Zam. nr 161/17