ZESZYTY NAUKOWE
POLITECHNIKI RZESZOWSKIEJ

SCIENTIFIC LETTERS
OF RZESZOW UNIVERSITY OF TECHNOLOGY

NR 296

(e-ISSN 2300-6358)

ELEKTROTECHNIKA

Kwartalnik
tom XXV
zeszyt 36 (nr 1/2017)
styczeń-czerwiec

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. 77

SPIS TREŚCI

WSPOMNIENIE

Dr inż. Irena Kuzora-Ziarno
emerytowany docent Politechniki Rzeszowskiej
(1928-2015),

W dniu 22 grudnia 2015 roku odeszła od nas Pani doc. dr inż. Irena Kuzora-Ziarno, która jako jeden z pierwszych pracowników Wydziału Elektrycznego Politechniki Rzeszowskiej, prodziekan w latach 1967--1971 i dziekan w roku akademickim 1971-1972, wniosła znaczący wkład w jego rozwój, aktywnie włączając się w przygotowanie od podstaw bazy dydaktyczno-laboratoryjnej. Dyplom mgr inż. zdobyła w Politechnice Gdańskiej, gdzie już w trakcie studiów prowadziła zajęcia ze studentami z *Matematyki* oraz *Elektrotechniki teoretycznej* na Wydziale Elektrycznym. Po uzyskaniu tytułu doktora wyjechała z Gdańska i podjęła w 1966 roku pracę w ówczesnej Wyższej Szkole Inżynierskiej w Rzeszowie. Objęła stanowisko docenta i kierownictwo w Zakładzie Elektrotechniki, który powstał rok wcześniej w 1965 r. W skład tej jednostki wchodzili także od samego początku mgr inż. A. Łęczycki oraz mgr inż. Z. Skarbowski. Prowadzili oni zajęcia z *Podstaw elektrotechniki* na Wydziale Elektrycznym oraz *Elektrotechniki ogólnej* na Wydziale Mechanicznym. Zakład Elektrotechniki przemianowano na Zespół Elektrotechniki Ogólnej, a w późniejszym czasie na Zespół Podstaw Elektrotechniki. Z roku na rok Zespół prężnie się rozwijał i powiększała się jego kadra. Do grona pracowników dołączali kolejno: dr inż. Izabela Rusin (od 1969 r.), dr inż. Kazimiera Rzepka (od 1970 r.), dr hab. inż. Jerzy Bajorek, prof. PRz (od 1970 r.), prof. dr hab. inż. Lesław Gołębiowski (od 1975 r.). W 1979 roku została zmieniona nazwa Zespołu Podstaw Elektrotechniki na Zakład Elektrotechniki Teoretycznej.

Docent Irena Kuzora-Ziarno prowadziła wykłady, ćwiczenia i laboratoria z Podstaw Elektrotechniki i Elektrotechniki Teoretycznej w licznych grupach na studiach dziennych, wieczorowych i zaocznych. Sprawowała opiekę naukową nad pracownikami, wspomagając ich swoją wiedzą i doświadczeniem oraz umożliwiając zdobycie stopni naukowych w Politechnice Warszawskiej, Akademii Górniczo-Hutniczej i Politechnice Gdańskiej. Pod jej kierownictwem prowadzone były w Zakładzie liczne badania naukowe i realizowane projekty w zakresie modelowania analogowego i cyfrowego. Wykorzystano metody numeryczne w obliczeniach na komputerach serii ODRA, zwłaszcza prowadzono modelowanie cyfrowe złożonych zagadnień teorii pola elektromagnetycznego w elementach układów elektrycznych dla potrzeb symulacji kompu-

terowych stanów dynamicznych w układach elektroenergetycznych i maszynach elektrycznych. Wykonywano prace zlecone przez zakłady przemysłowe z regionu, zawiązała się współpraca z Instytutem Morskim w Gdyni. Pani Docent uczestniczyła w Konferencjach i Seminariach zarówno w kraju i za granicą. Prezentując dorobek naukowy tworzyła przyjazną atmosferę do nawiązania współpracy naukowo-badawczej. Studentom znana była z perfekcyjnie opracowanych i interesujących wykładów. Wysoka jakość kształcenia procentowała później w pracy zawodowej wielu absolwentów. Po przejściu na emeryturę w roku 1991 i przekazaniu kierownictwa profesorowi Jerzemu Bajorkowi, nadal współpracowała z Zakładem Elektrotechniki Teoretycznej (od 2001 roku przemianowanym na Zakład Podstaw Elektrotechniki i Informatyki) prowadząc z dużym zaangażowaniem zajęcia dydaktyczne z przedmiotu *Sygnały i układy* w ramach umów zlecenia, aż do roku 2006 wspólnie z dr. hab. inż. Grzegorzem Masłowskim, prof. PRz., aktualnym kierownikiem utworzonej w 2015 roku Katedry Elektrotechniki i Podstaw Informatyki z Zakładu Podstaw Elektrotechniki i Informatyki. W dniu 17 czerwca 2015 roku uczestniczyła jako gość honorowy w uroczystych obchodach jubileuszu 50-lecia Wydziału Elektrotechniki i Informatyki i było to jej pożegnanie z naszą Uczelnią, Wydziałem i Katedrą, której poświęciła niemal całe swoje życie zawodowe.

Za swą działalność naukową, dydaktyczną i organizacyjną otrzymała wiele wyróżnień i odznaczeń, z których do najważniejszych należy zaliczyć: Medal "Zasłużonym dla Politechniki Rzeszowskiej im. Ignacego Łukasiewicza" (1988), Krzyż Kawalerski Orderu Odrodzenia Polski (1981), Zasłużonym dla województwa rzeszowskiego (1980), Medal Komisji Edukacji Narodowej (1978), Złoty Krzyż Zasługi (1973)

Pani Docent pozostanie w pamięci jako świetny wykładowca, wymagający ale sprawiedliwy egzaminator, a dla współpracowników jako bardzo dobry kierownik i organizator, pomocny w rozwiązywaniu trudnych spraw zawodowych oraz rodzinnych problemów.

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (1/2017), styczeń-czerwiec 2017, s. 7-14

Michal ŠPES[1]
Ľubomír BEŇA[2]
Miroslav MIKITA[3]
Michal MÁRTON[4]
Henryk WACHTA[5]

TESTING OF DIGITAL PROTECTION RELAY REF543

This article describes the digital protective relay REF 543 and its testing possibilities. The aim of this work is to verify overcurrent, undervoltage and overvoltage protection functions by indirect method using test equipment CMC 156. Among other things, IED REF 543 will be presented along with its features. The work is a space reserved for the description of the testing methods of protective relay.

Keywords: protection relay, REF 543, testing of operation, direct and indirect method.

1. Introduction

Operational reliability and safety of the electricity system (ES) depends not only on the use of the latest technology and knowledge of management of ES but due to the rapid progress of the transients and on the prevention of negative impacts of disturbances also for the correct choice of protective relays or digital relays [1]. Any such equipment must be subject to functional and system-based testing prior to its putting into service while verifying the functionality and operation of the individual protective functions for the protected equipment.

[1] Michal Špes, Department of Electric Power Engineering at Technical University of Košice, Mäsiarska 74, 041 20 Košice, 00421 55 602 3584, Michal.Spes@tuke.sk
[2] Ľubomír Beňa, Department of Electric Power Engineering at Technical University of Košice, Mäsiarska 74, 041 20 Košice, 00421 55 602 3561, Lubomir.Bena@tuke.sk
[3] Miroslav Mikita, Department of Electric Power Engineering at Technical University of Košice, Mäsiarska 74, 041 20 Košice, 00421 55 602 3560, Miroslav.Mikita@tuke.sk
[4] Michal Márton, Department of Electronics and Multimedia Communications at Technical University of Košice, Park Komenského 13, 041 20 Košice, Michal.Marton.3@student. tuke.sk
[5] Corresponding author: Henryk Wachta, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, ul. W. Pola 2, 35-959 Rzeszów, 17 865 1977, hwachta@prz.edu.pl

The outcome of the test is a protocol that includes the results of testing to all fault conditions that may endanger the protected equipment. When testing the electrical protection relays we use two methods of verification activities: direct and indirect method [3].

Electrical protection relays are connected to the protected object through Current Transformers, where the secondary side of the current transformers is 5 A or 1 A and the secondary side of the voltage transformers is 100 V [4], [5].

This fact is used in indirect test methods when we connect electrical protection to a protective test device that secondary injects the voltage and current test voltage while monitoring the protection response. Direct method protection testing is one of the most important tests where we verify the functionality of the entire device and the connection. Against the indirect method, there is a fundamental difference in testing. Voltage and current is injected to the primary side of the transformer. This method of testing is difficult, since current and voltage on the primary side must respond to the operating variables.

This method verifies the operation of the relay, the correctness of wiring system, the connection of instrument transformers.

2. Feeder terminal REF 543

Feeder Terminal REF 543 (Fig. 1) is designed for protection, control, measurement and supervision in medium voltage networks.

Fig. 1. Feeder terminal REF543 [2]

The REF 543 feeder terminal can be used with different kinds of switchgear, including single bus bar, double bus bar and duplex systems [2]. The protection functions also support different types of networks, such as isolated neutral networks, resonant-earthed networks and partially earthed networks. The application area also covers medium-sized three phase asynchronous motors as well as protection and control of shunt capacitor banks used for reactive power

compensation. In addition to protection, measurement, control, condition monitoring and general functions, the REF 543 feeder terminals are provided with a large amount of PLC functions, which allow for several automation and sequence logic functions, needed for substation automation, to be integrated into one unit.

The data communication properties include the following communication standards: SPA bus, LON bus, IEC 60870-5-103, IEC 61850 via SPA-ZC 400, Profibus DPV1 via SPA-ZC 302, DNP 3.0 and Modbus communication with higher level equipment. Further, the LON communication together with the PLC functions minimizes the need for hardwiring between the feeder terminals.

3. Configuration and testing of overcurrent protective functions

Testing and configuration of the digital protective relay REF 543 is possible using the programming interface PCM600 or using the control keys located on the front panel of this terminal.

In terms of configuration, it is necessary to identify the active group functions. Available are group 1 or 2. Configuring the functions of one group is independent of the configuration of the second group.

To verify the operation of the protective relay, the following overcurrent functions and their characteristics were configured:

- definite time (NOC3 LOW),
- definite time (NOC3 HIGH),
- definite time (NOC3 INST).

The configuration values of the protective functions are shown in the Table 1.

Table 1. Summary of configuration parameters of overcurrent functions

Protective function	Parameters	Set value
NOC3 INST	Start value	3 x I_N
	Operating delay time	0.04 s
	Directional mode	Non directional
NOC3 HIGH	Start value	2.5 x I_N
	Operating delay time	0.30 s
	Directional mode	Non directional
NOC3 LOW	Start value	2 x I_N
	Operating delay time	0.60 s
	Directional mode	Non directional

The actual verification activities of the terminal is based on the connection and configuration of the test equipment CMC 156 of relays, which includes the same configuration parameters as the IED REF 543. It is also necessary to set the allowed tolerance of the current (0.05A) and time (0.04s).

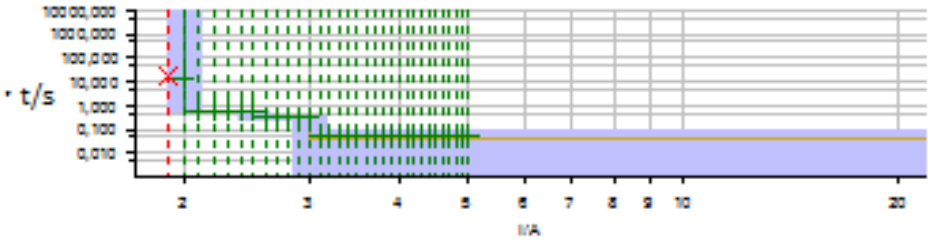


Fig. 2. Overcurrent protective characteristic

In the testing process, we specify the steps for which there is a change of injected current ranging from 1.90 A to 5.00 A. The resulting characteristic of protection with test points is marked in the Fig. 2. In the Table 2 are listed the individual test points with turn-off time of relay for protective overcurrent function NOC3 LOW. In the Table 3 and 4 are listed test points for protective overcurrent function NOC3 High and NOC3 INST. Response time of the terminal is evaluated by a test device as either passed or failed.

Table 2. Summary of test points of protective function NOC3 LOW

Type	Relative To	Factor	Magnitude	Angle	t_{nom}	t_{act}	Result
L1-E	(---)	n/a	1.90 A	n/a	No trip	15.31 s	Passed
L1-E	(---)	n/a	2.00 A	n/a	0.60 s	13.75 s	Passed
L1-E	(---)	n/a	2.10 A	n/a	0.60 s	0.61 s	Passed
L1-E	(---)	n/a	2.20 A	n/a	0.60 s	0.61 s	Passed
L1-E	(---)	n/a	2.30 A	n/a	0.60 s	0.61 s	Passed
L1-E	(---)	n/a	2.40 A	n/a	0.60 s	0.61 s	Passed

Table 3. Summary of test points of protective function NOC3 HIGH

Type	Relative To	Factor	Magnitude	Angle	t_{nom}	t_{act}	Result
L1-E	(---)	n/a	2.50 A	n/a	0.30 s	0.61 s	Passed
L1-E	(---)	n/a	2.60 A	n/a	0.30 s	0.32 s	Passed
L1-E	(---)	n/a	2.70 A	n/a	0.30 s	0.32 s	Passed
L1-E	(---)	n/a	2.80 A	n/a	0.30 s	0.32 s	Passed
L1-E	(---)	n/a	2.90 A	n/a	0.30 s	0.32 s	Passed

Table 4. Summary of test points of protective function NOC3 INST

Type	Relative To	Factor	Magnitude	Angle	t_{nom}	t_{act}	Result
L1-E	(---)	n/a	3.00 A	n/a	0.04 s	0.32 s	Passed
L1-E	(---)	n/a	3.10 A	n/a	0.04 s	0.06 s	Passed
L1-E	(---)	n/a	3.20 A	n/a	0.04 s	0.06 s	Passed
L1-E	(---)	n/a	3.30 A	n/a	0.04 s	0.06 s	Passed
L1-E	(---)	n/a	3.40 A	n/a	0.04 s	0.06 s	Passed
L1-E	(---)	n/a	3.50 A	n/a	0.04 s	0.06 s	Passed
L1-E	(---)	n/a	3.60 A	n/a	0.04 s	0.06 s	Passed
L1-E	(---)	n/a	3.70 A	n/a	0.04 s	0.06 s	Passed
L1-E	(---)	n/a	3.80 A	n/a	0.04 s	0.05 s	Passed
L1-E	(---)	n/a	3.90 A	n/a	0.04 s	0.05 s	Passed
L1-E	(---)	n/a	4.00 A	n/a	0.04 s	0.06 s	Passed
L1-E	(---)	n/a	4.10 A	n/a	0.04 s	0.05 s	Passed
L1-E	(---)	n/a	4.20 A	n/a	0.04 s	0.05 s	Passed
L1-E	(---)	n/a	4.30 A	n/a	0.04 s	0.05 s	Passed
L1-E	(---)	n/a	4.40 A	n/a	0.04 s	0.05 s	Passed
L1-E	(---)	n/a	4.50 A	n/a	0.04 s	0.05 s	Passed
L1-E	(---)	n/a	4.60 A	n/a	0.04 s	0.05 s	Passed
L1-E	(---)	n/a	4.70 A	n/a	0.04 s	0.05 s	Passed
L1-E	(---)	n/a	4.80 A	n/a	0.04 s	0.05 s	Passed
L1-E	(---)	n/a	4.90 A	n/a	0.04 s	0.05 s	Passed
L1-E	(---)	n/a	5.00 A	n/a	0.04 s	0.05 s	Passed

4. Configuration and testing overvoltage and undervoltage protective functions

To verify the overvoltage and undervoltage protective functions, the functions OV3 LOW and UV3 LOW are configured. The configuration values are given in the Table 5.

Table 5. Summary of configuration parameters of overvoltage and undervoltage protective functions

Protective function	Parameters	Set value
OV3 LOW	Start value	1.1 x U_N
	Operating delay time	0.04 s
	Num. of start phases	3 out of 3
UV3 LOW	Start value	0.85 x U_N
	Operating delay time	0.05 s
	Num. of start phases	3 out of 3

To test these protective functions, a Ramping module was selected in the test environment TEST UNIVERSE. The actual test consists of two parts. The first part (*State 1*) the voltage drop was set from 100 V to 50 V in steps of 100 mV at 1 V/s. In the second part (*State 2*) the voltage increase was set from 50 V up to a maximum of 115 V (Table 6).

Table 6. Summary of simulated conditions

State	***State 1***	***State 2***
Start value (V)	100	50
Final value (V)	50	115
Step (mV)	100	100
Time (ms)	100	100
Ramp steps	501	651

Fig. 3 shows the progress of the test. A power relay evaluated that conditions as a fault at a value 85 V. Then it began its action as shown in Fig. 4. The terminal operates in all 501 testing points.

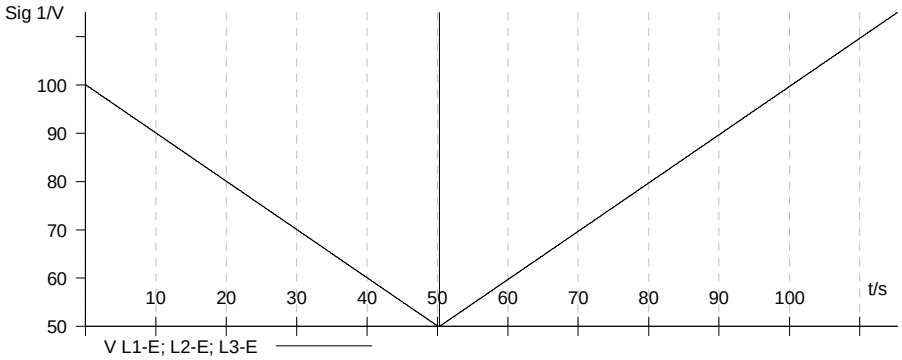


Fig. 3. The course of the injected voltage

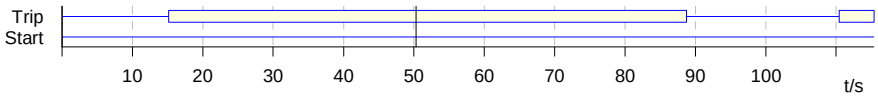


Fig. 4. Operation of protective functions

In the second part of testing (*State 2*) the voltage increase occurs. Protective relay evaluated conditions as a fault at a value 110V. Then the overvoltage protective function OV3 LOW is operated.

5. Conclusion

Before deploying protective relay in service, which are installed in switchboards as functional units for protection of generators, substations and outlets it is necessary in consideration of the importance and operational reliability of the individual components of the power system, to carry out the functional and system testing of these protective devices.

The test also corresponds to the verification of the operation of protections relay by the indirect method using the CMC156-tested test device.

This article is to point out the methods for testing the terminal, depending on whether it is a fault in which there is a change of the measured quantity, current or voltage.

Results of testing is a protocol that gives clear and accurate information about the correct operation of protective relay.

References

[1] Kolcun M., Griger V., Beňa Ľ., Rusnák J.: *Prevádzka elektrizačnej sústavy*. Košice 2007. ISBN 978-80-8073-837-2.

[2] ABB. "Product Guide. Feeder Protection and Control REF543". [Online].

[3] Chladný V., Janíček F., Beláň A.: *Digitálne ochrany v elektrizačných sústavách*. Košice 2003. ISBN 80-89061-73-7.

[4] Liptai P., Moravec M., Lumnitzer E., Lukáčová K.: I*mpact analysis of the electromagnetic fields of transformer stations close to residential buildings*. In: SGEM 2014, volume 1, p. 17-26, 2014, STEF92 Technology, p. 355-360. ISBN 978-619-7105-17-9.

[5] Lumnitzer E., Drahoš R., Liptai P.: *Elektromagnetické polia v životnom a pracovnom prostredí Objektivizácia a hodnotenie faktorov prostredia*. 1. vyd – Košice, Technická univerzita, 2014, s. 96. ISBN 978-80-553-1910-0.

TESTOWANIE CYFROWEGO TERMINALU ZABEZPIECZENIOWEGO REF543

S t r e s z c z e n i e

Artykuł opisuje cyfrowy terminal zabezpieczeniowy REF 543 i możliwość jego testowania. Celem tej pracy jest sprawdzenie funkcji nadprądowej, podnapięciowej i ochrony przed przepięciami metodą pośrednią z wykorzystaniem urządzenia testującego CMC 156. Wśród innych ele-

mentów pracy przedstawiono wykorzystanie REF 543 z jego funkcjami. Praca obejmuje opis metod testowania terminalu zabezpieczeniowego.

Słowa kluczowe: przekaźnik zabezpieczający, REF 543, badanie działania, bezpośrednia i pośrednia metoda

DOI: 10.7862/re.2017.1

Tekst złożono w redakcji: marzec 2017
Przyjęto do druku: maj 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (1/2017), styczeń-czerwiec 2017, s. 15-25

Michal ŠPES[1]
Ľubomír BEŇA[2]
Miroslav MIKITA[3]
Michal MÁRTON[4]
Henryk WACHTA[5]

VERIFICATION OF THE DISTANCE PROTECTION RELAY OPERATION

This paper describes the possibilities of testing digital protection relay. Consequently, the SIEMENS SIPROTEC 7SA611 distance protection, its protection functions and its use for protection of the line are further characterized. At the end of the article, testing of this distance protection is described along with several variations of Advance distance module testing.

Keywords: distance protection relay, testing of operation, indirect method

1. Introduction

The electric power system is formed by generators that convert energy of rotating masses into electrical energy, equipment serving for the transformation, transmission and consumption of electricity [1].

Power system is characterized by:

- vastness - power system is spread over a particular space,
- complexity - between elements of active feedback,
- random nature of the load - not known in advance the load size.

[1] Michal Špes, Department of Electric Power Engineering at Technical University of Košice, Mäsiarska 74, 041 20 Košice, 00421 55 602 3584, Michal.Spes@tuke.sk
[2] Ľubomír Beňa, Department of Electric Power Engineering at Technical University of Košice, Mäsiarska 74, 041 20 Košice, 00421 55 602 3561, Lubomir.Bena@tuke.sk
[3] Miroslav Mikita, Department of Electric Power Engineering at Technical University of Košice, Mäsiarska 74, 041 20 Košice, 00421 55 602 3560, Miroslav.Mikita@tuke.sk
[4] Michal Márton, Department of Electronics and Multimedia Communications at Technical University of Košice, Park Komenského 13, 041 20 Košice, Michal.Marton.3@student. tuke.sk
[5] Corresponding author: Henryk Wachta, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, ul. W. Pola 2, 35-959 Rzeszów, 17 865 1977, hwachta@prz.edu.pl

Due to the rapid transition process, the operational reliability and safety of the power system depend not only on the most advanced technologies and knowledge, but also on the appropriate choice of protective devices [2].

Prior to the introduction of protective devices and relays, functional and system testing of the correct operation of these devices must be carried out before they are put into service.

The conclusion of such a test is usually the test report, which includes the results of the operation verification of the individual protective functions that protect the device against fault condition, which may occur after putting into operation [2], [4].

2. Method of verifying the operation of protective devices

In order to verify the operation of the protective devices, we can identify two test methods:

- direct method,
- indirect method.

The connection of protective devices is realized via instrument transformers. In terms of construction, different voltage levels and different current it is not appropriate to dimension individual devices for each protected object. For these reasons, protective devices and terminals are connected via instrument transformers.

Depending on the chosen measured quantity we use current transformers (overcurrent protection), voltage transformers (overvoltage / undervoltage protection), or combinations thereof (distance protection). In terms of choice of instrument transformers current it is crucial for us the location of protection relay from attachment sites in substations. For long supply lines it is necessary to respect the losses that arise when supplying the protection with long feeds. Therefore, it is necessary to choose the current transformer with secondary current value of 1 A [3].

In case there can be a loss of transmitted secondary current, we choose a current instrument transformer with a secondary current value of 5 A.

The voltage transformers secondary side is 100 V. From these facts, it is inferred indirect assay method. The test device injects secondary voltage / current until the protection relay responds [3].

3. Distance protection relay 7SA611

The SIPROTEC 47SA611 distance protection relay is a universal relay for protection, control and automation with a 4-line display on the basis of the SIPROTEC 4 system. Its high level of flexibility makes it suitable to be implemented at all voltage levels [5].

Digital distance protection relay is equipped with features that are typically used for line protection and is therefore universally applicable. It is also possible to use the device as a time lapse backup protection to all kinds of protective devices operating on the principle of comparing for the lines, transformers, generators, motors and busbars of all voltage levels [5].

Typical features of protection relay SIPROTEC 7SA611:

- high-speed tripping time,
- impedance setting range allows very small settings for the protection of very short lines,
- self-setting detection for power swing frequencies up to 7 Hz,
- current transformer saturation detector prevents non-selective tripping by distance protection in the event of CT saturation,
- phase-segregated teleprotection for improved selectivity and availability,
- digital relay-to-relay communication by means of an integrated serial protection data interface,
- adaptive auto-reclosure (ADT) [5] (Fig. 1).

Fig. 1. Distance protection relay 7SA611 [5]

3.1. Description of the functions of the distance protection relay 7SA611

Distance protection relay 7SA611 includes features for protection of overhead lines and cable lines at all voltage levels from 5 to 765 kV. The unit may issue one or three-pole TRIP commands, and CLOSE commands. It is perhaps the single-pole, three-pole and more pole automatic reclosing. The device operates reliably and selectively even under the most burdensome power line conditions [5].

The Distance protection relay is equipped with the following protective functions:

a) the protection functions for protecting Earth-fault (ANSI 50N/ ANSI 51N/ ANSI 67N),
b) distance protection function (ANSI 21/ ANSI 21N),
c) overcurrent protection functions with a time delay, immediately acting protective functions and overcurrent protection functions with the direction (ANSI 50 / ANSI 51 / ANSI 67),
d) overvoltage and undervoltage protection function (ANSI 59/ ANSI 27),
e) overfrequency and underfrequency protection function (ANSI 81O/ ANSI 81U),
f) automatic reclosing (ANSI 79),
g) checking of the synchronization (ANSI 25),
h) protection of the failure of breaker (ANSI 50BF),
i) thermal protection (ANSI 49) [5].

In addition to protective functions, this digital protection terminal also has control and monitoring functions:

- Control function

The instrument has extensive control functions, such as instrumentation hardware as well as software. Measured values are continuously monitored.

- Management of functions

Function management is performed by the control center of the device. Coordinates the running of protection and ancillary functions, processes their decisions and the information coming from the device.

4. Parameterization of Distance protection relay SIPROTEC 7SA611 in DIGSI software environment

For parameterization and setting the Distance protection relay SIEMENS SIPROTEC 7SA611 is appropriate to use configuration program DIGSI 4. First, we need to create a new project that we call "SIPROTEC" for the sake of clarity. For proper configuration, you must add a digital terminal. In "SIPROTEC" we choose "Folder" through the main rail route Insert> DIGSI> Device SIPROTEC add protective relay (Fig. 2).

Consequently, it is necessary after opening the library for the digital protective terminal we specify the parameters of protection, we use the nameplate (Fig. 3).

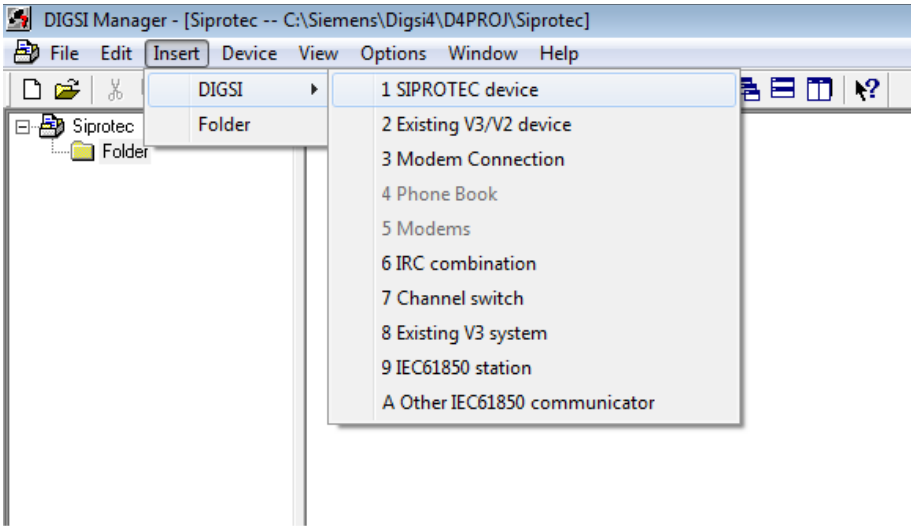


Fig. 2. Adding digital protective relay in the software environment

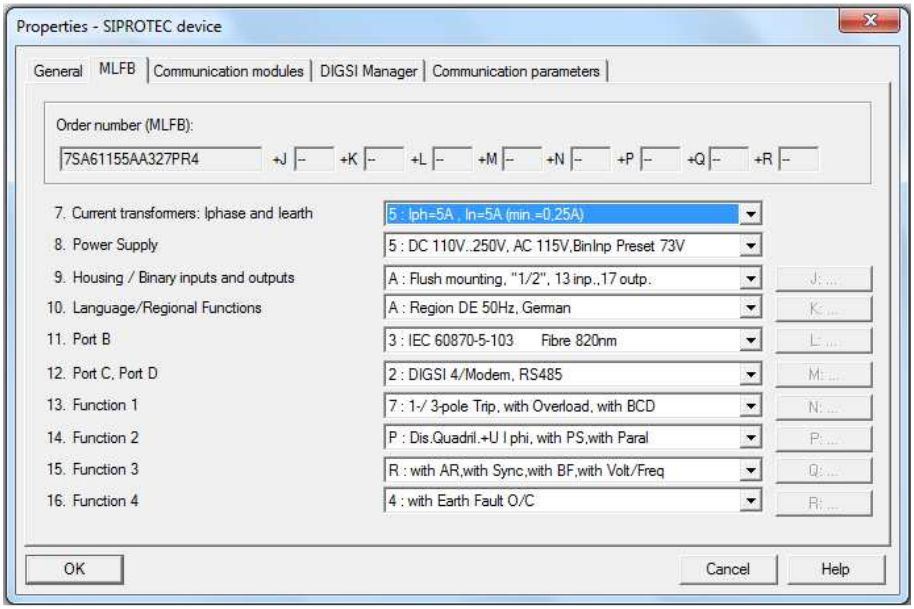


Fig. 3. Setting the basic parameters of protection relay according to nameplate

After this step, we can proceed to parameterization of the distance protection and the setting of protective functions (Fig. 4). Our role in terms of protecting is to set parameters for digital protection relay of the 110 kV line (V6834) in

substation Kechnec (it is a part of the 110 kV distribution system in Eastern Slovakia).

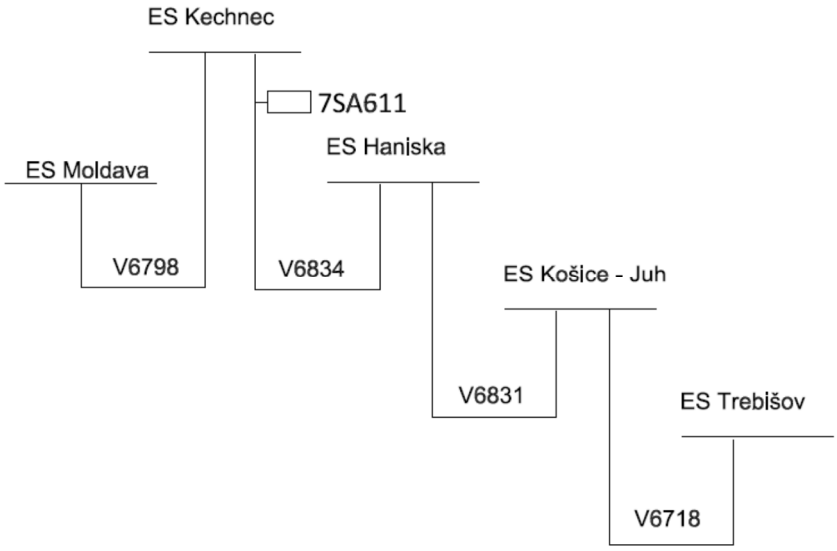


Fig. 4. The topology of the protected electricity grid

Firstly, it is necessary to define the various transfers of instrument transformers. Since we choose the setting parameters for the 110 kV line it is necessary to select a voltage transformer with primary voltage value of 110 000 V.

In the case of current transformers, the value of the current on the secondary side is for us I_{2N} = 5A.

Before setting individual zones, you must first define protected zones and lines:

- Zone 1: In this zone is impedance-adjusted at 85% of line impedance V6834,
- Zone 2: In this zone is impedance-adjusted at 100% of line impedance V6834 and 60% of line impedance V6831,
- Zone 3: In this zone is impedance-adjusted at 100% of line impedance V6834, 100% of line impedance V6831 and 40% of line impedance V6718,
- Zone 4: This zone is backward zone and the impedance is adjusted at 30% of line impedance V6718,
- Zone 5: In this zone is impedance-adjusted at 100% of line impedance V6834, 100% of line impedance V6831 and 100% of line impedance V6718.
- Zone 6: This zone is not activated.

The configuration of individual zones are as follows (Table 1-3):

Table 1. Setting Zone 1 and Zone 2

Zone	Z1	Zone	Z2
Status	Active	Status	Active
Direction	Forward	Direction	Forward
Charakteristics	Polygon	Charakteristics	Polygon
Values	Secondary	Values	Secondary
X_1	0.196 Ω	X_2	0.420 Ω
R_1, PG	0.181 Ω	R_2, PG	0.405 Ω
R_1, PP	0.060 Ω	R_2, PP	0.135 Ω
α_1	70°	α_2	70°
t_1	0 s	t_2	0.5 s

Table 2. Setting Zone 3 and Zone 4

Zone	Z3	Zone	Z4
Status	Active	Status	Active
Direction	Forward	Direction	Backward
Charakteristics	Polygon	Charakteristics	Polygon
Values	Secondary	Values	Secondary
X_3	0.896 Ω	X_4	0.152 Ω
R_3, PG	0.935 Ω	R_4, PG	0.141 Ω
R_3, PP	0.311 Ω	R_4, PP	0.047 Ω
α_3	70°	α_4	70°
t_3	1 s	t_4	0.5 s

Table 3. Setting Zone 5 and Zone 6

Zone	Z5	Zone	Z6
Status	Active	Status	Non Active
Direction	Forward	Direction	-
Charakteristics	Polygon	Charakteristics	-
Values	Secondary	Values	-
X_5	1.420 Ω	X_6	-
R_5, PG	1.537 Ω	R_6, PG	-
R_5, PP	0.512 Ω	R_6, PP	-
α_5	70°	α_6	-
t_5	5 s	t_6	-

5. Verification of the operation of digital protections relay SIEMENS SIPROTEC 7SA611

After setting and saving parameters in the protection relay we proceeded to verify the operation of the protection relay through device CMC 156. To verify the operation of protection relay SIPROTEC 7SA611 we used the module "Advance distance". In order to test the protection, we also need to set up protection zones in the "Advance distance" module. This is possible in two ways.

The first method is to manually set the zones. We will fill in all the necessary data based on the set values in the protection relay. Each zone we create using points and then we assign zones tripping times.

The first method is rather tedious. Therefore, it is possible to create individual protection zones by exporting the .rio file with the DIGSI, which is consequently recorded in "test objects parameters" in the "Advance distance" module. After setting all the necessary parameters and zones we can choose the fault to be tested, we can select the points to be tested, or search zones (Fig. 5).

Testing digital protective relay was performed for interphase short circuit L1-L2.

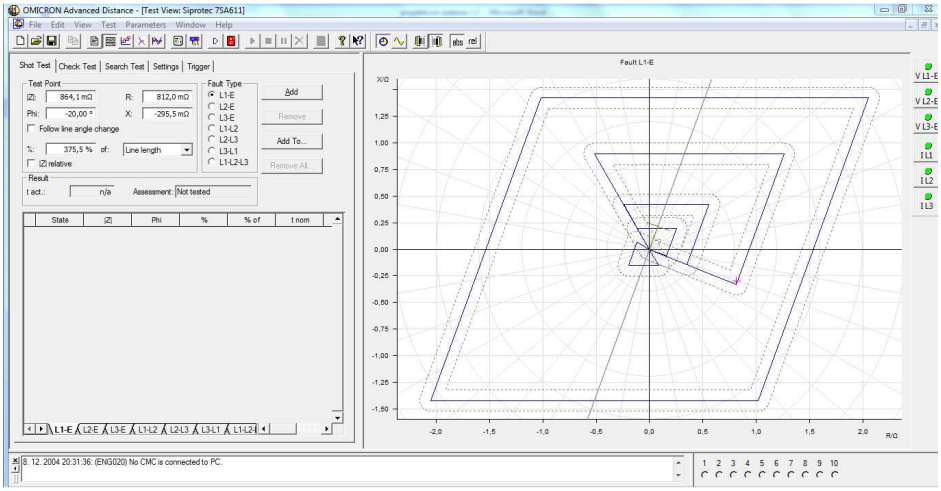


Fig. 5. Testing in the module Advance distance

5.1. Verification of the operation of digital protection relay SIEMENS SIPROTEC 7SA611 for individual test points

The actual operation of the test equipment of protections relays CMC 156 is based on injection of voltages and currents in the protective relay, wherein the testing device monitors the reaction of the relay, and evaluates the actual test.

In Test Universe software, you can choose several ways of testing. It is possible to select the manual input of the individual points in the zone it protects, and then track equipment's time of the protective relay for that fault.

Test points that we have entered can be seen in the figure below (Fig. 6). The results of the testing are in the table below (Table 4).

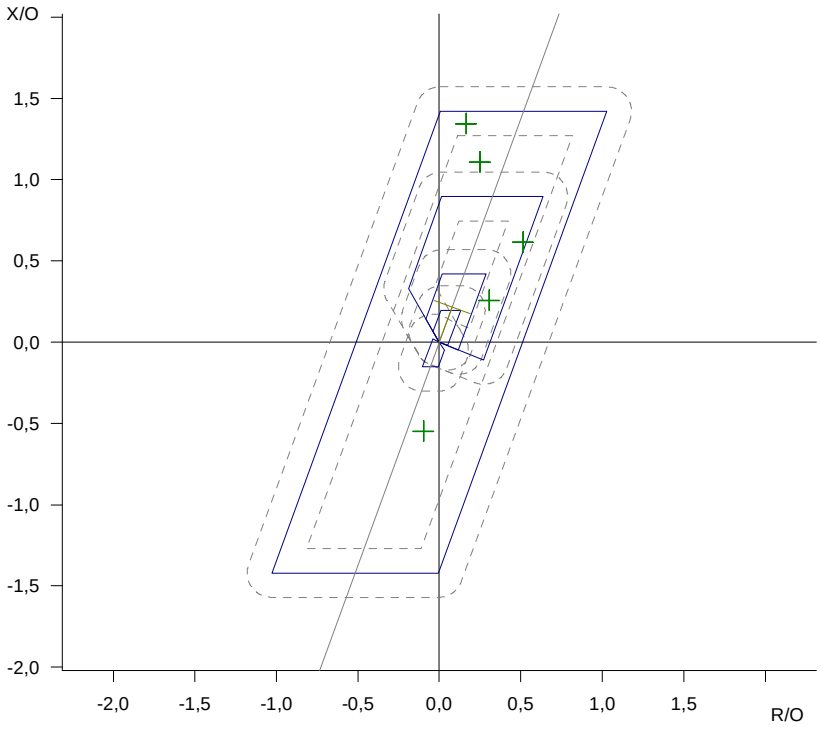


Fig. 6. Points for test of distance protection relay

Table 4. Results from testing of distance protection relay

| Z |	Phi	%	t_{nom}	t_{act}	Dev.	I_{Test}	Result
1.352 Ω	83.07°	n/a	5.000 s	5.034 s	0.676%	10.00 A	Passed
1.137 Ω	77.31°	n/a	5.000 s	5.039 s	0.788%	10.00 A	Passed
800.0 mΩ	50.00°	n/a	1.000 s	1.034 s	3.41%	10.00 A	Passed
400.0 mΩ	40.00°	n/a	1.000 s	1.034 s	3.41%	10.00 A	Passed
558.2 mΩ	-100.00°	n/a	5.000 s	5.034 s	0.678%	10.00 A	Passed

5.2. Verification of the operation of digital protection relay SIEMENS SIPROTEC 7SA611 for a line of testing

The second variant of testing is time easier. Unlike the first testing method, we do not select individual points of testing but we set "a line" points, first to the

endpoint testing. Test points were not set individually, but the built-in line crossed all impedance zones. Test points on the line segment were generated by the module automatically. The results of the testing are shown in the table below (Table 5) and the line segment with the test points is in the figure (Fig. 7).

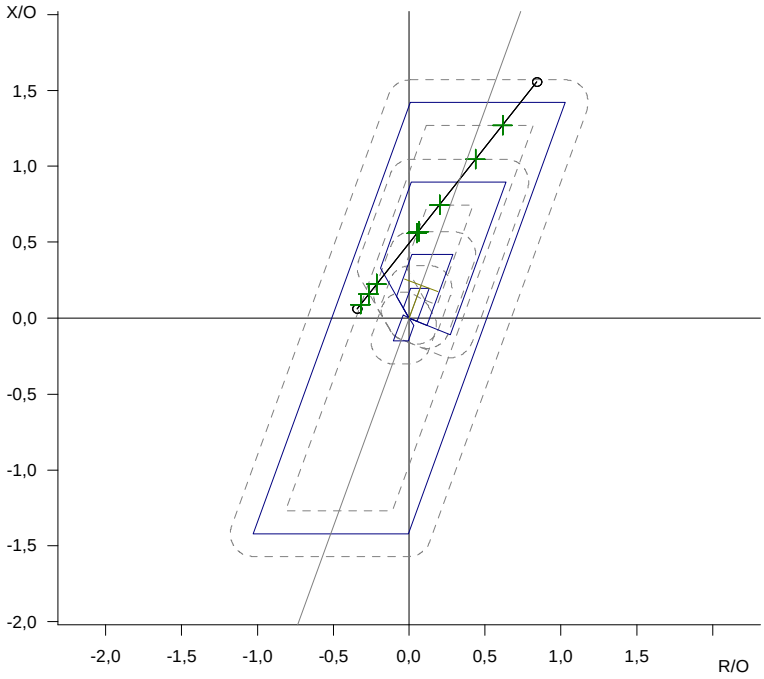


Fig. 7. A line for test of distance protection relay

Table 5. Results from testing of distance protection relay

| Z |	Phi	t_{nom}	t_{act}	Dev.	ITest	Result
332.0 mΩ	164.32°	5.000 s	5.054 s	1.08%	10.00 A	Passed
308.9 mΩ	149.12°	5.000 s	5.054 s	1.082%	10.00 A	Passed
309.2 mΩ	133.56°	5.000 s	5.059 s	1.17%	10.00 A	Passed
560.2 mΩ	84.72°	1.000 s	1.034 s	3.43%	10.00 A	Passed
573.3 mΩ	83.87°	1.000 s	1.034 s	3.43%	10.00 A	Passed
772.5 mΩ	74.94°	1.000 s	1.034 s	3.42%	10.00 A	Passed
1.134 Ω	67.25°	5.000 s	5.034 s	0.688%	10.00 A	Passed
1.412 Ω	64.11°	5.000 s	5.034 s	0.678%	10.00 A	Passed

6. Conclusion

The issue of testing protective relays is quite difficult and even before the actual deployment of the relay into operation is required functional and system

testing. The aim of this paper is to describe a testing method of the description of the protective relay SIEMENS SIPROTEC 7SA611.

This protection relay includes protection distance between overhead lines and cable lines. In view of the fact that it is a digital relay, this device has a more security features that have been described at the beginning of article. For the test this digital protective relay one protective function was chosen, "ANSI 21 - Distance Protection".

In total, two tests were carried out in different parts of the protection zones. As shown in the attached tables, the actual tripping time in individual testing points deviates from the preset minimum time and therefore protective relay can be used in operation.

References

[1] Kolcun M., Griger V., Beňa Ľ., Rusnák J.: *Prevádzka elektrizačnej sústavy*, Košice 2007. ISBN 978-80-8073-837-2

[2] Lumnitzer E., Drahoš R., Liptai P.: *Elektromagnetické polia v životnom a pracovnom prostredí Objektivizácia a hodnotenie faktorov prostredia*, 1. vyd - Košice, Technická univerzita, 2014, s. 96. ISBN 978-80-553-1910-0.

[3] Chladný V., Janíček F., Belaň A.: *Digitálne ochrany v elektrizačných sústavách*, Košice 2003. ISBN 80-89061-73-7

[4] Liptai P., Moravec M., Lumnitzer E., Lukáčová K.: *Impact analysis of the electromagnetic fields of transformer stations close to residential buildings*. In: SGEM 2014, volume 1, p. 17-26, 2014, STEF92 Technology, p. 355-360. ISBN 978-619-7105-17-9.

[5] Siemens, Siprotec Distance Protection 7SA611, Manual, 6.2013.

WERYFIKACJA OPERACJI PRZEKAŹNIKA ZABEZPIECZENIOWEGO ODLEGŁOŚCIOWEGO

S t r e s z c z e n i e

W artykule opisano możliwości testowania cyfrowego przekaźnika zabezpieczeniowego. W związku z tym w pracy zostały opisane funkcje ochronne przekaźnika zabezpieczeniowego odległościowego SIEMENS SIPROTEC 7SA611 i wykorzystanie ich do ochrony linii energetycznych. Ostatnia część artykułu zawiera elementy testowania zabezpieczenia odległościowego wraz z kilkoma odmianami w module testowania „Advance distance".

Słowa kluczowe: przekaźnik zabezpieczający, testowanie pracy, metoda pośrednia

DOI: 10.7862/re.2017.2

Tekst złożono w redakcji: marzec 2017
Przyjęto do druku: maj 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (1/2017), styczeń-czerwiec 2017, s. 27-40

Mariusz GAMRACKI[1]

BUDOWA I DZIAŁANIE SYSTEMU DETEKCJI I LOKALIZACJI WYŁADOWAŃ ATMOSFERYCZNYCH BLITZORTUNG

W pracy opisano budowę i podstawy funkcjonowania systemu detekcji i lokalizacji wyładowań atmosferycznych Blitzortung. Początkowe rozdziały opisują podstawy dotyczące działania tego typu systemów, zakresy częstotliwości stosowane przy detekcji wyładowań oraz najczęściej stosowane metody detekcji i lokalizacji wykorzystywane w tego typu systemach. Wspomniano także o innych komercyjnych systemach detekcji i lokalizacji wyładowań pracujących na świecie. Opisano zalety i wady systemów detekcji pracujących na niskich i na wysokich częstotliwościach. Szerzej opisano funkcjonowanie systemu Blitzortung a także elementy wchodzące w skład każdej stacji detekcji, rodzaje obecnie działających stacji (wersje urządzeń o nazwach RED i BLUE), ich możliwości i funkcjonalność. Opisano rodzaje i budowę anten używanych do detekcji pola elektromagnetycznego przez stacje systemu Blitzortung. Na przykładzie kontrolera w wersji RED pokazano działanie stacji odbierającej sygnały z anten i jego możliwości w zakresie filtracji sygnałów nie pochodzących od wyładowania. Pokazano rozmieszczenie stacji detekcji na ternie centralnej Europy i USA. Opisano wybrane inne możliwości jakie daje system Blitzortung i porównano jego możliwości z systemami profesjonalnymi. Pokazano przykładowe rejestracje systemu w postaci wycinka mapy z zaznaczonymi miejscami wyładowań a także mapę gęstości wszystkich wyładowań zarejestrowanych przez system w roku 2015 na terenie Polski oraz przykładowe zarejestrowane charakterystyki czasowe wyładowania.

Słowa kluczowe: wyładowanie atmosferyczne, system detekcji wyładowań, lokalizacja wyładowań, pole elektromagnetyczne.

1. Wprowadzenie

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 burzowych systemów ostrzegawczych [1]. Są tam dokładnie opisane kolejne

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

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].

Bardzo szerokie spektrum częstotliwościowe pola elektromagnetycznego pochodzącego od pola piorunowego pozwala na stosowanie metod bazujących na częstotliwościach zarówno bardzo niskich jak i bardzo wysokich. Naziemne systemy lokalizacji wyładowań działają często z wykorzystaniem dwóch techniki detekcji, które wzajemnie się uzupełniają. Z najbardziej znanych systemów można wymienić europejskie LINET, SAFIR (polski PERUN), ATD, EUCLID i amerykańskie NALDN, IMPACT, LPATS, LDAR [2]. Bardzo dynamicznie rozwija się amatorska sieć detekcji i lokalizacji wyładowań atmosferycznych pod nazwą Blitzortung. Jej duża skuteczność i możliwości wynikają głównie z bardzo dużej ilości detektorów rozmieszczonych na terenie całej Europy, Stanów zjednoczonych i Australii, ale także Azji i dalekim wschodzie (Japonia). Obecnie naziemne systemy detekcji i lokalizacji wyładowań piorunowych są szeroko wykorzystywane w takich dziedzinach jak meteorologia, lotnictwo, pożarnictwo, energetyka, ubezpieczenia, ochrona ludzi i inne [1, 2]. System Blitzortung udostępnia użytkownikom szerokie spektrum wyników i statystyk dla zarejestrowanych wyładowań. Możliwe jest uzyskanie przebiegów czasowych i częstotliwościowych pola piorunowego, statystyki dotyczące gęstości wyładowań na konkretnych obszarach i wiele innych danych.

2. Metody detekcji i lokalizacji wyładowań piorunowych

Powstająca podczas wyładowania atmosferycznego fala elektromagnetyczna ma bardzo szerokie spektrum częstotliwości. Zaczynając od ekstremalnie niskich częstotliwości, 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 zastosowanie 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 międzychmurowe, dodatnie i ujemne).

Stosowane obecnie techniki detekcji 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. Zastosowany 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 czego przykładem są brytyjski ATD tylko z 7 stacjami na terenie Europy oraz system Blitzortung, który składa się z ponad tysiąca stacji detekcji rozmieszczonych na całym świecie. Pole elektromagnetyczne z zakresów VLF i LF emitowane przez kanał piorunowy jest wyjątkowo silne dla wyładowań głównych doziemnych [2, 3].

Analizując pole elektromagnetyczne w zakresie bardzo wysokich częstotliwości (VHF) można uzyskać dużą precyzję odzwierciedlenia kształtu fali sięgającą nawet nanosekund. Pozwala to dokładnie odzwierciedlić np. kształt czoła zarejestrowanej fali elektromagnetycznej o małym czasie narastania rzędu ułamków mikrosekund. Z kolei duża gęstość próbkowania sygnału powoduje, że utrudnione jest zbieranie danych dla długich czasów trwania rejestracji (np. wyładowań wielokrotnych), gdyż taka analiza generuje duże ilości próbek. Odwrotna sytuacja występuje przy analizie w pasmach VLF i LF, gdzie można uzyskać rozdzielczość jedynie na poziomie 1-2 mikrosekund. Niestety nie pozwala to na dokładne odzwierciedlenie kształtu czoła fali piorunowej, można natomiast analizować długie wyładowania także w sekwencji wielokrotnej sięgającej kilku sekund.

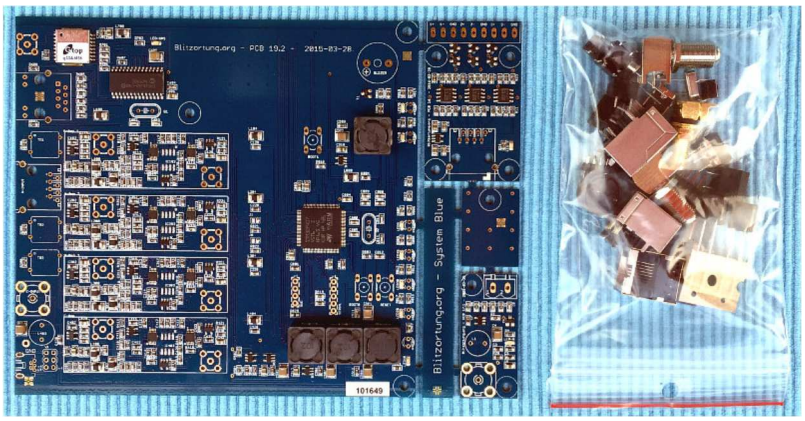
Pisząc o detekcji wyładowań atmosferycznych warto wspomnieć o systemach lokalizacji wyładowań, które składają się z sieci rozmieszczonych stacji detekcji. Przy analizie kształtu pola piorunowego jest to istotne, ponieważ systemy lokalizacji pozwalają dość dokładnie określić położenie poszczególnych wyładowań, a co za tym idzie wyznaczyć odległości wyładowań od każdej stacji detekcji. Zastosowanie techniki detekcji wysokich częstotliwości (VHF) pozwala uzyskać dużą dokładność lokalizacji sięgającą nawet 200 m jednak wymaga zastosowania stacji rozmieszczonych w niewielkich odległościach rzędu 100 km. Technika bazująca na analizie sygnałów niskich częstotliwości pozwala natomiast na umieszczanie stacji w odległościach nawet tysięcy kilometrów od siebie lecz lokalizacja wyładowań takich systemów jest mniejszej dokładności i nie umożliwia rozpoznawania wyładowań wewnątrz i między chmurami. Dla pasm VLF i LF detekcja obejmuje więc przeważnie wyładowania doziemne i ma duży zasięg detekcji, natomiast dla zakresu VHF wszystkie typy wyładowań z mniejszym zasięgiem detekcji [1, 2].

3. Stacje detekcji wyładowań piorunowych Blitzortung

Spośród systemów detekcji i lokalizacji wyładowań atmosferycznych na wyróżnienie zasługuje amatorski system Blitzortung [4]. System powstał około roku 2003 z kilkoma stacjami detekcji, a od 2012 bardzo dynamicznie się rozwija. Pierwsze stacje detekcji wyposażone były w kontrolery o nazwie GREEN podłączane za pomocą złącza RS232, a później USB do dowolnego komputera

PC i za pośrednictwem sieci Internet przekazywały zarejestrowane dane do serwera. Obecnie system pracuje głównie z wykorzystaniem kontrolerów o nazwie RED i najnowszych BLUE podłączanych bezpośrednio do sieci LAN. Jest to samodzielne urządzenie, które przeważnie poprzez sieć lokalną podłączone jest do Internetu. Kontroler konfiguruje się i obsługuje poprzez przeglądarkę internetową. Dodatkowo możliwa jest także korekta pewnych parametrów pracy kontrolerów zdalnie z poziomu centralnego serwera zarządzającego.

Twórcą i pomysłodawcą systemu jest prof. Egon Wanke z Uniwersytetu w Dusseldorfie, który wraz z dwoma współpracownikami rozwija i koordynuje projekt. Projekt ma swoją ogólnodostępną stronę internetową i grupę dyskusyjną oraz dodatkowe specjalne strony internetowe dla aktywnych użytkowników systemu (po zalogowaniu do systemu) [4]. Z założenia system jest otwarty dla osób chcących uczestniczyć w projekcje. Należy w tym celu zakupić odpowiedni zestaw do samodzielnego zmontowania i wykonać odpowiednią antenę. Zestaw składa się z kontrolera (obecnie w wersji BLUE) i dwóch przedwzmacniaczy składowej magnetycznej pola i składowej elektrycznej. Przedwzmacniacze umieszcza się bezpośrednio przy antenach. Dodatkowe stopnie wzmacniaczy umieszczone są w kontrolerze. System RED składa się natomiast z kontrolera, przedwzmacniacza składowej elektrycznej oraz dwóch wzmacniaczy składowej magnetycznej pola i składowej elektrycznej. System RED ma dodatkowo wyświetlacz LCD, na którym pokazywane są najważniejsze informacje dotyczące statusu pracy urządzenia. Obecnie system BLUE nie ma LCD, lecz opcja ta jest rozpatrywana przez twórców i projektantów systemu. Na rysunku 1 pokazano kompletny zestaw płytek drukowanych systemu BLUE składający się z głównego kontrolera i dwóch przedwzmacniaczy składowych magnetycznej i elektrycznej pola oraz pozostałe elementy do samodzielnego przylutowania [4].



Rys. 1. Zestaw wszystkich trzech płytek dla systemu BLUE i dodatkowe części do wlutowania

Fig. 1. Set of three PCB's for the system BLUE and additional parts be soldered

Na dostarczonych płytkach drukowanych wlutowane są tylko podzespoły w technologii SMD, pozostałe większe elementy należy zamontować samodzielnie. Można także zakupić kilka innych elementów takich ja obudowa, specjalne dodatkowe filtry cyfrowe i pręty ferrytowe do wykonania anten. Aktualnie dostępne są tylko zestawy BLUE, natomiast najwięcej pracujących stacji działa z systemami RED i bardzo niewiele w starej wersji GREEN. Obecnie wspierane są jedynie wersje RED i BLUE, dla których okresowo wydawane są nowe wersje firmware poprawiające stabilność i funkcjonalność pracy systemów. Firmware wgrywa się do kontrolera samodzielnie z poziomu przeglądarki internetowej poprzez stronę konfiguracyjną urządzenia. Na rysunku 2 pokazano wygląd dwóch stron obudowy dla kontrolera w wersji BLUE.

Rys. 2. Obudowa kontrolera w wersji BLUE [4]

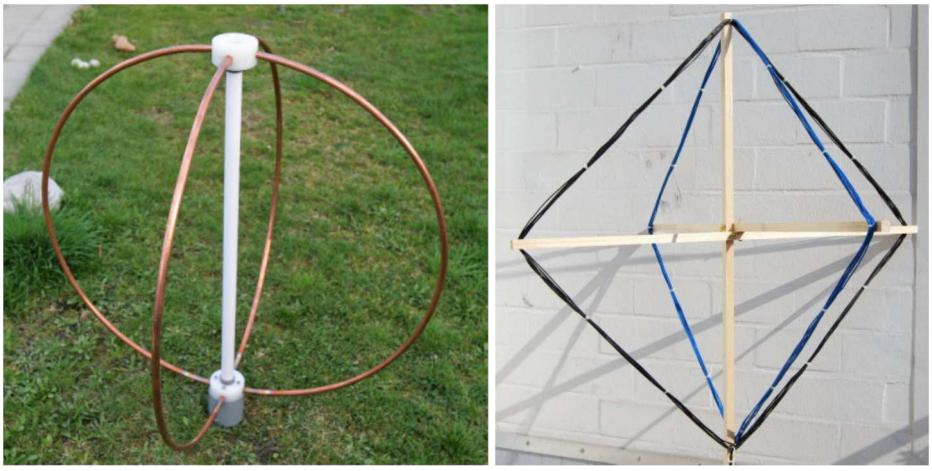
Fig. 2. Housing for system BLUE controller [4]

Na rysunku 3 pokazano po lewej stronie zestaw trzech nieekranowanych anten ferrytowych w układzie horyzontalnym z umieszczonym pośrodku przedwzmacniaczem składowej magnetycznej, natomiast po prawej stronie anteny ferrytowe w układzie 3D. Jeżeli ktoś decyduje się na użycie anten pętlowych musi wykonać je we własnym zakresie. Obecnie zaleca się wykonanie anten o całkowitej powierzchni „zbierania" sygnału ok. 2,4 m^2. Stosując anteny o średnicy pętli 1 m wystarczą 3 pętle (zwoje) natomiast dla średnicy 38 cm należy wykonać 21 pętli. Obecnie zaleca się stosowanie jednak anten pętlowych o maksymalnej średnicy pętli do ok. 40 cm. Dodatkowo anteny pętlowe można wykonać jako ekranowane wykorzystując do tego celu np. rurkę miedzianą lub nawet grubą folię aluminiową, którą owija się anteny. Ekran anten składowych magnetycznych powinien być otwarty, a więc nie powinien być zwarty na obwodzie ponieważ jego zadaniem jest ekranowanie niepotrzebnej w tym wypadku składowej elektrycznej pola. Ekran należy dołączyć jednym jego końcem do ekranu przewodów antenowych i dalej do uziemienia lub ew. do przewodu uziemiającego instalacji elektrycznej. Podobnie jak dla anten ferrytowych w systemie BLUE można zastosować 3 anteny pętlowe. Natomiast antena do składowej elektrycznej może być wykonana np. z kawałka prostego, grubego drutu miedzianego (o przekroju 2,5 – 4 mm^2) o długości od 30 cm do ok. 1 m.

Rys. 3. Po prawej nieekranowane anteny ferrytowe z przedwzmacniaczem w układzie horyzontalnym, po lewej w układzie 3D z jedną anteną ustawioną pionowo [4]

Fig. 3. On the right, unshielded ferrite antennas in a horizontal layout with a preamplifier, on left in a 3D layout with one antenna setting vertically [4]

Na rysunku 4 pokazano przykładowe wykonanie anten pętlowych. Po lewej stronie dwie anteny w kształcie okręgu w ekranie z miedzianej rurki do zastosowania na zewnątrz, natomiast po prawej o kształcie kwadratowym w postaci nawiniętej na drewniany stelaż linki lub drutu miedzianego. Instalując anteny nie ma potrzeby ustawiania ich orientacji względem stron świata – na razie nie ma takiego wymogu. Należy je tak zorientować aby uzyskać możliwie małe zakłócenia, które mogą pochodzić od pobliskich urządzeń elektrycznych.



Rys. 4. Dwie anteny pętlowe w ekranie z rurek miedzianych do zastosowania zewnętrznego oraz proste nieekranowane anteny nawinięte na ramie drewnianej [4]

Fig. 4. Two loop antennas in the shield made of copper pipes for external use and simple unshielded antennas wrapped on a wood frame [4]

Proces kalibracji, orientacji anten i ustawiania wzmocnień wymaga od użytkownika poświęcenia dużej ilości czasu, aby uzyskać możliwie optymalną konfigurację. Okazuje się czasami, że do anten dochodzą zaburzenia nieznanego pochodzenia i w związku z tym należy dokonać korekt ustawienia anten i właściwie dobrać poziomy wzmocnienia dla poszczególnych kanałów.

Pozostałe drobne elementy takie jak zasilacz, przewody antenowe i do sieci LAN użytkownik zakupuje samodzielnie. Także rozmieszczenie anten i montaż całości wykonuje samodzielnie. Wszystkie elementy systemu zasilane są tylko z jednego zasilacza wpiętego do kontrolera, a do zasilania wzmacniaczy, przedwzmacniaczy i modułu GPS wykorzystane są przewody antenowe i skrętka. Cały system pobiera tylko ok. 3-4 waty. Stacje systemu wyposażone są w odbiornik GPS pozwalający na dokładnie wyznaczenie czasu zarejestrowanego sygnału i określenie pozycji geograficznej stacji. Antenę do modułu GPS także należy umieścić w miejscu dobrego odbioru sygnałów z satelitów. System nie jest specjalnie wymagający względem parametrów łącza internetowego. Ważny jest stały dostęp do Internetu, a pasmo dla transmisji danych od stacji do serwerów (upload) powinno wynosić co najmniej 256 kbit/s.

4. Działanie systemu Blitzortung

System Blitzortung lokalizuje wyładowania z użyciem metod TOA (Time of Arrival) i TOGA (Time of Group Arrival). Każdy zarejestrowany przez stację sygnał napięciowy, którego maksymalna wartość, przekracza pewien określony poziom, wraz z dokładnym czasem z GPS i współrzędnymi geograficznymi stacji rejestrującej, wysyłany jest do jednego z głównych serwerów. Następnie system na podstawie otrzymanych danych z różnych stacji wyznacza współrzędne miejsca wyładowania. W obecnej fazie rozwoju system potrafi lokalizować jedynie wyładowania doziemne i częściowo wewnątrz chmur jednak nie są one rozpoznawane, jako tego typu. Wynika to głównie z zastosowanej techniki detekcji niskich i bardzo niskich częstotliwości. Prowadzone prace rozwojowe zmierzają jednak do rozszerzenia możliwości systemu o detekcję i rozpoznawanie wyładowań wewnątrz i pomiędzy chmurami oraz rodzaju polaryzacji (zastosowanie dodatkowych anten dla składowej elektrycznej pola) [4].

Zdolności wychwytywania sygnałów przez anteny poszczególnych stacji systemu Blitzortung są różne. Wynika to w pewnym stopniu z różnorodności zastosowanych anten, ich lokalizacji i znajdujących się w ich pobliżu źródeł zaburzeń elektromagnetycznych. Na szczęście system jest odporny na tego typu niedogodności, ponieważ daje użytkownikom duży zakres regulacji wzmocnień sygnałów, opcje automatycznej regulacji, a także kilka filtrów eliminujących zakłócenia. Filtrowanie i automatyzacja systemu jest ciągle ulepszana, gdyż do serwerów wysyłana jest bardzo duża ilość zarejestrowanych danych, które często nie są pochodzenia piorunowego. Statystycznie tylko około jedna trzecia

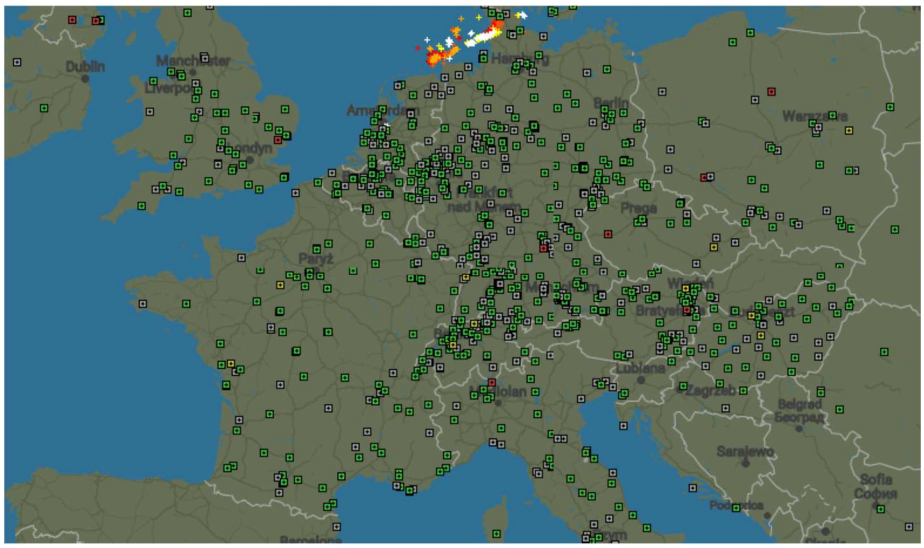
wysyłanych sygnałów jest rozpoznawana jako pochodzące od wyładowań atmosferycznych i różni się to dla poszczególnych stacji. Stosowane filtry mają na celu wyeliminowanie niepochodzących od wyładowań piorunowych sygnałów typu „szpilki” (ang. spike), sygnałów sinusoidalnych oraz serii sygnałów (ang. burst) liczących po kilkadziesiąt impulsów na sekundę (np. zakłócenia łączeniowe). Na rysunku 5 pokazano zrzut ekranu zakładki „Signals” kontrolera RED. Sygnał w kanale 1B pomimo przekroczenia poziomu wyzwalania nie został wysłany do serwera ponieważ został w nim rozpoznany nieprawidłowy kształt w postaci „szpilki” napięciowej co zostało zaznaczone w opisie kanałów „Channel” w postaci litery „S” – *spike*. Kanał 1A miał natomiast za niski poziom napięcia, aby sygnał z niego mógł być wysłany, co oznaczono literą „L” – *low*. Litery dla kanałów 1A i 1B są zaznaczone na czerwono co oznacza, że sygnały z nich nie zostały wysłane na serwery. Do pozostałych kanałów w tym kontrolerze nie są podłączone anteny i kanały są zaznaczone na szaro.

Rys. 5. Sygnały odbierane przez kontroler RED – ich parametry elektryczne i numeryczne

Fig. 5. Signals received by the RED controller – their electrical and numerical parameters

Stacje detekcji mogą pracować w opcji całkowicie automatycznej, która ustala optymalne wzmocnienie dla poszczególnych kanałów i włącza lub wyłącza filtry lub też w trybie manualnym z zadanym maksymalnym wzmocnieniem dla każdego z kanałów i włączonymi lub nie filtrami. Wzmacniacze sygnałów dołączone szeregowo do każdej z anten są kilkustopniowe oferujące maksymalne wzmocnienie na poziomie 20000. Wartość maksymalną wzmocnienia należy przeważnie ograniczyć do pewnego optymalnego poziomu. W praktyce wartości wzmocnień zmieniają się automatycznie i oscylują w granicach od kilkudziesięciu razy do kilku tysięcy razy, co zależy głównie od wielkości i parametrów zastosowanych anten i od odległości frontów burzowych od danej stacji.

Niewątpliwą zaletą systemu Blitzortung jest bardzo duża liczba stacji detekcji rozmieszczonych głównie w Europie (rys. 6), ale także w USA (rys. 7), Australii, Azji. Obecnie na całym świecie jest już ponad 1300 aktywnych stacji, z czego jednocześnie działa ok. 800. Tak duża ilość stacji pozwala w sposób ciągły pokryć swoim zasięgiem detekcji duży obszar nawet w sytuacji, gdy nie pracuje część stacji. Niestety stacje rozmieszczone są nierównomiernie, co widać na rysunkach 6 i 7, jednak bardzo duży zasięg detekcji części stacji, dochodzący do 5 tysięcy km i więcej, pozwala na skuteczne działanie systemu.

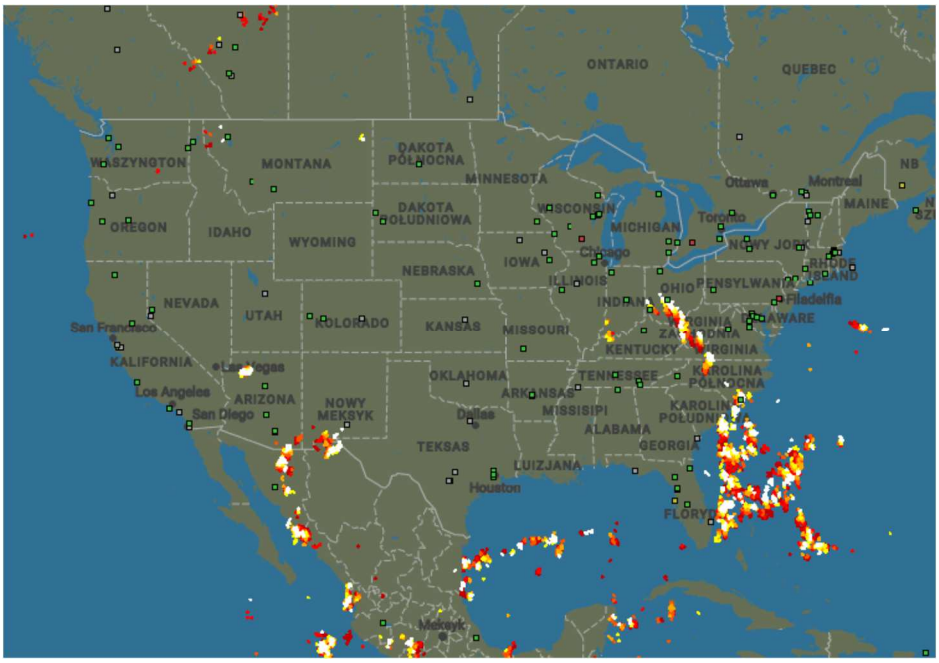


Rys. 6. Rozmieszczenie stacji detekcji systemu Blitzortung na terenie centralnej Europy

Fig. 6. Deployment of Blitzortung detection stations in central Europe

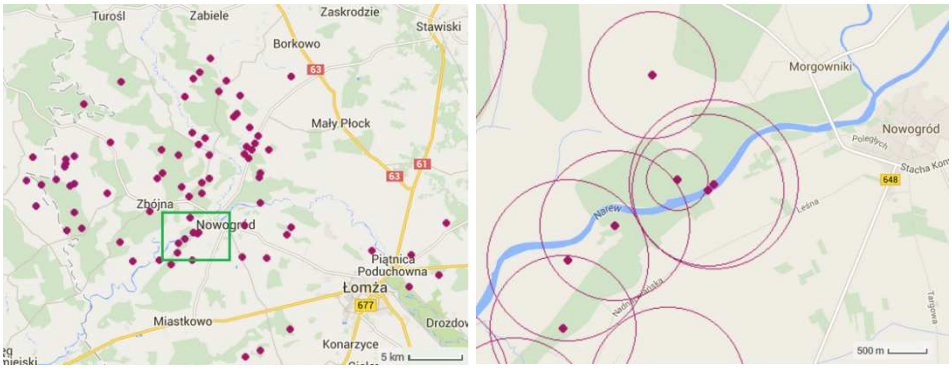
Na rysunku 8 pokazano lokalizacje wyładowań zarejestrowanych przez system detektorów Blitzortung w nocy z 15 na 16 października 2014 roku w okolicach Łomży. Rysunek po lewej przedstawia obszar o rozmiarach ok. 40x30 km natomiast po prawej powiększony prostokąt o rozmiarach ok. 5x4 km, gdzie

widać dodatkowo okręgi, których promień odpowiada dokładności lokalizacji dla poszczególnych wyładowań wynoszącej od 400 m do ok. 1 km dla tego obszaru.



Rys. 7. Rozmieszczenie stacji detekcji systemu Blitzortung na terenie USA

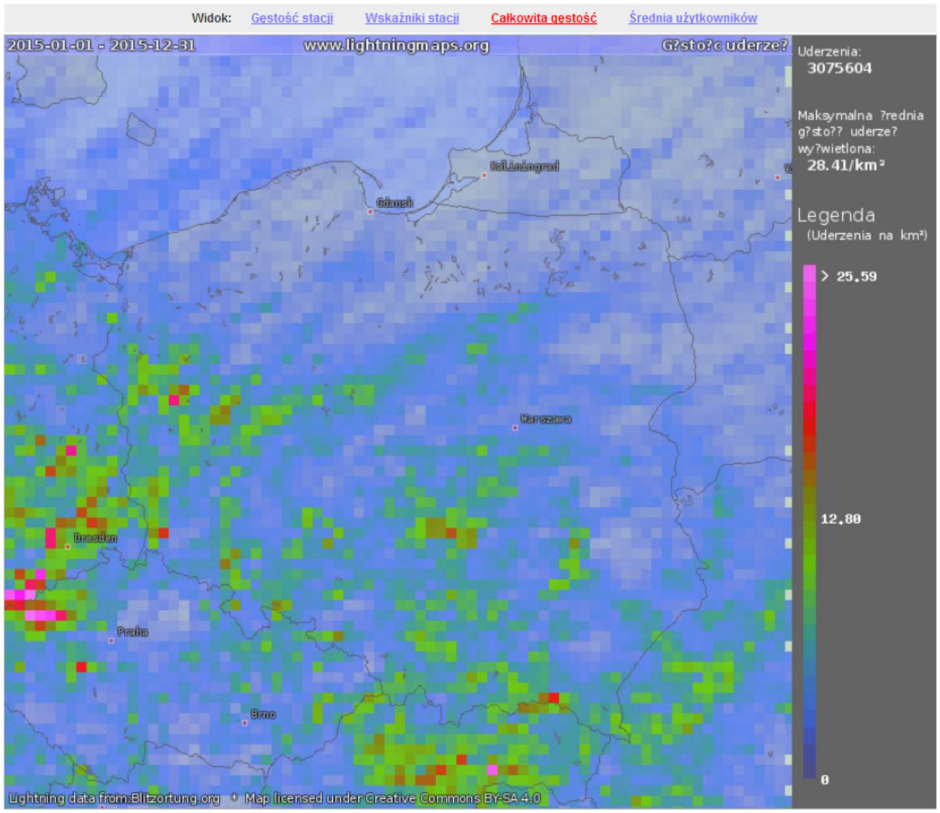
Fig. 7. Deployment of Blitzortung detection stations in USA area



Rys. 8. Wyładowania zarejestrowane przez system Blitzortung

Fig. 8. Lightning discharges detected by Blitzortung system

W odróżnieniu od systemów komercyjnych Blitzortung udostępnia publicznie dodatkowo dokładne mapy z umieszczonymi miejscami wyładowań atmosferycznych, mapy gęstości wyładowań na danym obszarze, różnego rodzaju animacje i statystyki. Dostępne są nawet mapy, które pokazują wyładowania w czasie rzeczywistym z opóźnieniem kilku sekund, czego nie ma żaden inny system. Dla aktywnych uczestników projektu są dodatkowo dostępne dane archiwalne wyładowań, jak również charakterystyki czasowe i częstotliwościowe zarejestrowanych sygnałów pochodzących od wyładowań piorunowych a także bardzo dokładne mapy z umiejscowionymi wyładowaniami (rys. 8) i różnego rodzaju rozszerzone statystyki i zestawienia. Na rysunku 9 pokazano przykładowe zestawienie statystyczne wyładowań dla obszaru Polski w roku 2015. Maksymalna gęstość wyładowań wyniosła 28,41 wył./km^2 a całkowita liczba zarejestrowanych wyładowań osiągnęła 3.075.604 (ponad trzy miliony).

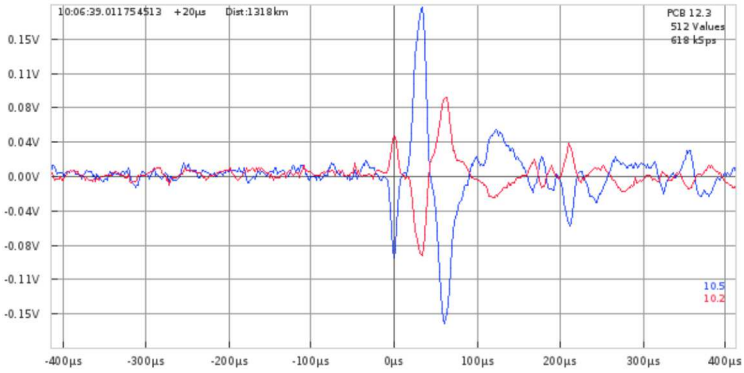


Rys. 9. Gęstość wyładowań dla obszaru Polski w roku 2015 [4]

Fig. 9. The density of discharges for the Polish territory in 2015 [4]

Mapy gęstości można wyświetlać dla 10 państw na terenie Europy, wybranych stanów USA a także dla całych kontynentów. Statystyki dostępne są dla poszczególnych miesięcy danego roku jak i dla całego roku. Mapki z ilością rejestracji są generowane także dla wszystkich stacji detekcji osobno.

Podstawowym zadaniem systemu Blitzortung jest lokalizacja wyładowań atmosferycznych. Do tego celu potrzebne są jedynie dane dotyczące czasu zarejestrowanych sygnałów i współrzędnych geograficznych stacji rejestrujących. Na tej podstawie, korzystając z metody TOA wyznaczane są współrzędne wyładowań atmosferycznych. Dodatkowo jednak do głównych serwerów przesyłane są także wszystkie przebiegi czasowe sygnałów zarejestrowanych przez stacje wchodzące w skład sieci lokalizacji. Umożliwia to wykonanie analizy poszczególnych rejestracji z różnych stacji. Dla zalogowanego użytkownika do dyspozycji są przebiegi pochodzące nawet z kilkuset różnych stacji detekcji, które zarejestrowały dane wyładowanie. Na rysunku 10 pokazano przykładową rejestrację wyładowania przez system Blitzortung, które nastąpiło 10 października 2016 roku o godzinie 10:06:39 czasu UTC w odległości 1318 km od stacji.



Rys. 10. Sygnały zarejestrowane przez anteny „magnetyczne” stacji Rzeszow-Milocin w Polsce

Fig. 10. Signals from station Rzeszow-Milocin in Poland recorded by the "magnetic" antennas

W sezonie burzowym na serwerach przechowywane są dane dla setek tysięcy przebiegów na godzinę. Niestety ze względu na bardzo dużą ilość danych potrzebnych do generowania przebiegów czasowych informacje te przechowywane są tylko przez pewien czas uzależniony od ilości wszystkich wyładowań na danym obszarze (np. na terenie Europy). W sezonie burzowym dziennie do serwerów dochodzi nawet do 1TB danych. Pełne dane (także przebiegi czasowe) przechowywane są wtedy jedynie ok. godziny i po tym czasie pozostają jedynie podstawowe dane związane z lokalizacją wyładowań oraz inne dane statystyczne. W okresie małej aktywności burzowej pełne dane pozostają dostępne nawet do 2-4 dni.

5. Wnioski

System detekcji i lokalizacji wyładowań Blitzortung dzięki małym kosztom budowy pojedynczych stacji (ok. 250-300 euro) i dużej skuteczności działania rozwija się bardzo dynamicznie. Na stronie internetowej systemu Blitzortung można zadeklarować chęć przystąpienia do projektu i zapisać się na listę oczekujących na potrzebne elementy stacji. Zarówno wykonanie i złożenie kontrolera jak i potrzebnych do detekcji anten i innych elementów jest zadaniem dość prostym. Obecnie już w każdym kontrolerze (RED, BLUE) następuje selekcja odebranych sygnałów i odrzucanie tych nie pochodzących od wyładowań atmosferycznych. Jest to ważne ponieważ do serwerów wysyłana jest bardzo duża ilość danych. Swoją wysoką skuteczność w detekcji i lokalizacji wyładowań system Blitzortung zawdzięcza dużej liczbie stacji detekcji rozmieszczonych na całym świecie. 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 pomiędzy wyładowaniem a stacja rejestrującą.

Na stronach projektu dostępne są bardzo dokładne mapy z zaznaczonymi miejscami wyładowań a także mapy pokazujące wyładowania w czasie rzeczywistym z opóźnieniem kilku sekund, mapy gęstości wyładowań na wybranych obszarach państw i kontynentów i wiele innych statystyk. Dane są dostępne zarówno dla pojedynczych stacji detekcji jak i dla całej sieci systemu Blitzortung. Można np. zobaczyć jak skutecznie pracuje dana stacja, wyświetlić charakterystykę kierunkową detekcji powiązaną także z odległością, wykresy pokazujące statystykę detekcji w czasie, w okresie do kilku dni a także wskaźniki procentowe uderzeń i lokalizacji ukazujące pracę każdej stacji.

Dodatkowo dla zalogowanych uczestników dostępne są charakterystyki czasowe i częstotliwościowe sygnałów od wyładowań zarejestrowanych przez wszystkie stacje systemu. Duża ilość dostępnych sygnałów i danych wymaga jednak odpowiedniej selekcji. Uzyskane informacje z systemu Blitzortung mogą być wartościowym uzupełnieniem podczas analizy danych z profesjonalnych systemów detekcji [5, 6] jak również przy modelowaniu matematycznym zjawisk propagacji piorunowego pola elektromagnetycznego [7, 8].

Literatura

[1] Norma 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] 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, ISSN 0033-2097, NR 7/2014, s. 97-99.
[6] 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.
[7] Gamracki M.: Modelowanie matematyczne propagacji piorunowego zaburzenia elektromagnetycznego nad ziemią, Przegląd Elektrotechniczny, ISSN 0033-2097, NR 2/2012, s. 23-25.
[8] Gamracki M.: Modelowanie propagacji piorunowego zaburzenia elektromagnetycznego nad stratną ziemią, Przegląd Elektrotechniczny, ISSN 0033-2097, NR. 7/2014, s. 171-174.

CONSTRUCTION AND OPERATION LIGHTNING DETECTION AND LOCATIONS SYSTEM BLITZORTUNG

S u m m a r y

This paper describes the structure and basis of the Blitzortung system for detection and location of lightning. The initial chapters describe the basis for the operation of such systems, frequency bands used for the detection of lightning and the most frequently used method for the detection and location used in such systems. Also mentioned other commercial systems, lightning detection and location of operating in the world. Paper show the advantages and disadvantages of detection systems operating at low and high frequencies. Described in more detail the Blitzortung system and the elements included in each detection station, the types of currently operating station (device versions named RED and BLUE), their features and functionality. Described the types and construction of antennas used to detect the magnetic and electric fields by the stations of the Blitzortung system. Shows the position of detection stations on the area of central Europe and the USA. In the next part the paper describes some of the possibilities offered by the Blitzortung system. In example the controller version RED shows the effect of the station receiving signals from the antenna and its possibilities for filtering signals which not coming from the discharge. Also describes some other features offered by the Blitzortung system and compared it with professional systems. Show some example from registration in the form of a map section with marked locations of discharge, map of density all discharges recorded by the system in 2015 on Poland area and sample time characteristics of discharge.

Keywords: lightning, lightning detection system, location of lightning, electromagnetic field

DOI: 10.7862/re.2017.3

Tekst złożono w redakcji: marzec 2017
Przyjęto do druku: maj 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (1/2017), styczeń-czerwiec 2017, s. 41-51

Tomasz ŚLIWA[1]

PROTOTYPOWY TRÓJKOŁOWY MINIROBOT LABORATORYJNY

W artykule przedstawiono budowę kołowego minirobota laboratoryjnego mogącego służyć początkowo jako platforma do badania czujników, a w przyszłości do oceny inteligentnych algorytmów nawigacyjnych w warunkach rzeczywistego przemieszczania. Przy konstrukcji robota kierowano się dostępnością elementów, łatwością montażu oraz niską ceną. Robot został wyposażony w mikrokomputer Raspberry Pi 2 z systemem operacyjnym Linux Raspbian, który wraz z oprogramowaniem aplikacyjnym stanowi zarówno system sterujący jak i platformę rozwojową umożliwiającą tworzenie i uruchamianie programów bezpośrednio w minirobocie. Do komunikacji służą usługi terminalowe, dzięki którym możliwe jest wygodne programowanie robota z dowolnego miejsca z łączem internetowym. Opisana konstrukcja została zaprezentowana na rzeszowskich zawodach ROBO~motion 2016, na potrzeby których opracowano i zaprogramowano trzy tryby pracy.

Słowa kluczowe: Robot mobilny, Raspberry Pi 2, czujniki ultradźwiękowe, IMU

1. Wprowadzenie

Rozwój autonomicznych pojazdów pociąga za sobą konieczność stosowania znacznej liczby czujników, takich jak czujniki odległości, prędkości, przyspieszenia, kursu czy pozycji. Mały trójkołowy robot mobilny jako niedroga, łatwa do skonstruowania i dalszej rozbudowy platforma, może być użyteczny w procesie testowania czujników w warunkach ruchu zbliżonych do docelowego środowiska.

Od pewnego czasu powstaje wiele różnorodnych konstrukcji robotów mobilnych. Budowane są zarówno małe, hobbystyczne jednostki przeznaczone do udziału w zawodach [3, 5], nieco bardziej skomplikowane roboty edukacyjne m.in. z wizyjnym sprzężeniem zwrotnym zapewnianym przez zewnętrzną kamerę [2] jak i jeszcze bardziej skomplikowane, wielokołowe konstrukcje z manipulatorem [1]. Istnieją także gotowe zestawy edukacyjne takie jak robot Khepera [7, 12] czy Lego Mindstorms [6, 13]. Nawet małe konstrukcje bywają skompli-

[1] Tomasz Śliwa, Politechnika Rzeszowska, Wydział Elektrotechniki i Informatyki, Katedra Informatyki i Automatyki, al. Powstańców Warszawy 12 35-959 Rzeszów, 17 865 1490, tomeks@kia.prz.edu.pl

kowane i kosztowne, dlatego w proponowanym rozwiązaniu postawiono na prostotę i dostępność części.

W artykule opisano pierwszą fazę budowy minirobota konstruowanego w oparciu o uniwersalne, trójkołowe podwozie napędzane dwoma silnikami prądu stałego (DC). Moc oraz kierunek obrotów ustawiana jest indywidualnie dla każdego z silników, co zapewnia dobrą manewrowość. Jako modułu obliczeniowego użyto popularnego mikrokomputera Raspberry Pi 2 Model B [8] (w skrócie RPi2), którego zasoby sprzętowe i moc obliczeniowa zapewniają obsługę algorytmów sterujących, środowiska programowania oraz usług pomocniczych, np. zdalnego dostępu. Do wykrywania przeszkód w otoczeniu robota użyto czujników ultradźwiękowych. Całość oprogramowania niezbędnego do działania i obsługi zlokalizowano w samym robocie. Dostęp do zasobów robota możliwy jest ze zdalnego terminala, dzięki czemu nad rozwojem robota może pracować jednocześnie cały zespół współpracujących użytkowników. Po wstępnych testach sprzętu i oprogramowaniu minirobota, zaprezentowano go na rzeszowskich Międzynarodowych Zawodach Robotów ROBO~motion 2016.

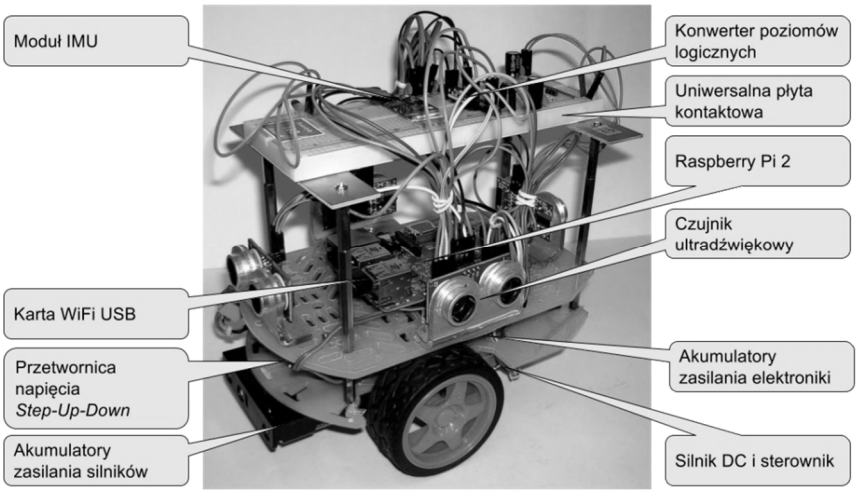
2. Budowa robota

Robot zbudowany został na bazie uniwersalnego, trójkołowego podwozia wyposażonego w dwa koła napędzane silnikami DC i jedno koło wsporcze. Komputer steruje kierunkiem obrotów oraz mocą silników DC [4] za pomocą sterownika - *drivera* kontrolowanego sygnałem PWM (*Pulse-Width Modulation*). Do pomiaru odległości od przeszkód na pokładzie zainstalowano cztery czujniki ultradźwiękowe. Znalazł się tam także układ IMU (*Inertial Measurement Unit*) zawierający żyroskop, magnetometr (kompas), akcelerometr, barometr i termometr. Ze względu na różnice w poziomach sygnałów cyfrowych poszczególnych modułów zastosowano konwerter poziomów logicznych. Do zasilania układów elektronicznych robota użyto 4 szeregowo połączone akumulatory NiMH, których napięcie stabilizuje przetwornica *Step-Up-Down*. W celu eliminacji zakłóceń wprowadzanych przez silniki DC sterowane sygnałem PWM, zastosowano osobne zasilanie silników z kolejnych 4 szeregowo połączonych akumulatorów NiMH. Zmontowany robot jest pokazany na rysunku 1.

Silniki DC DG01D 48:1 zamontowane w podwoziu zasilane są napięciem 5V, a do ich sterowania służy zintegrowany moduł drivera DRV8835. Umożliwia on za pomocą sygnałów PWM sterowanie mocą i kierunkiem obrotów. Wykorzystano także dodatkowe wejście zasilania *drivera*, aby doprowadzić napięcie do silników z osobnego zestawu akumulatorów.

Zastosowany mikrokomputer Raspberry Pi 2 posiada 40-pinowe złącze GPIO (*General Purpose Input/Output*), na które wyprowadzono standardowe sygnały magistral komunikacyjnych I2C, SPI, UART, linie zasilania +5V

i +3,3V oraz uniwersalne piny GPIO umożliwiające sterowanie urządzeniami peryferyjnymi. Wejścia/wyjścia GPIO pracują na poziomie logicznym 3,3V.



Rys. 1. Zmontowany robot mobilny

Fig. 1. Full-featured mobile robot

Zastosowany mikrokomputer Raspberry Pi 2 posiada 40-pinowe złącze GPIO (*General Purpose Input/Output*), na które wyprowadzono standardowe sygnały magistral komunikacyjnych I2C, SPI, UART, linie zasilania +5V i +3,3V oraz uniwersalne piny GPIO umożliwiające sterowanie urządzeniami peryferyjnymi. Wejścia/wyjścia GPIO pracują na poziomie logicznym 3,3V. Podanie 5V na wejście RPi2 może spowodować uszkodzenie. Jako układ IMU zastosowano moduł GY-80 z interfejsem I2C, zawierający układy:

- akcelerometr ADXL245B,
- żyroskop L3H4200D,
- magnetometr HMC5883L,
- barometr i termometr BMP085.

Do pomiaru odległości służą 4 czujniki ultradźwiękowe HC-SR04 o zasięgu 2m umieszczone z przodu, z tyłu i na bokach robota. Do komunikacji z czujnikiem HC-SR04 wymagane jest użycie dwóch linii, jednej do wyzwolenia pomiaru, drugiej do pomiaru czasu odpowiedzi, proporcjonalnego do odległości obiektu od czujnika. Ponieważ czujnik pracuje z zasilaniem i poziomami logicznymi 5V, dlatego pomiędzy wyjściami czujników a wejściami mikrokomputera RPi2 zainstalowano konwerter poziomów logicznych z tranzystorami BSS138. Do połączenia wszystkich modułów wykorzystano uniwersalną płytę kontaktową umieszczoną w górnej części robota.

Komunikacja robota z użytkownikiem-programistą odbywa się za pomocą małej karty sieciowej WiFi TL-WN725N podłączonej do jednego z czterech portów USB mikrokomputera RPi2.

3. Raspberry Pi 2 jako komputer pokładowy

W punkcie tym krótko przedstawiono relatywnie mocny mikrokomputer Raspberry Pi 2 (rys. 2) jako główny moduł obliczeniowy robota, pracujący pod kontrolą systemu operacyjnego Linux Raspbian, a także jego oprogramowanie oraz możliwości techniczne. Ten stosunkowo niewielki moduł elektroniczny jest wyposażony w:

- procesor ARM Cortex-A7 (900MHz, cztery rdzenie, 32bit),
- 1 GB pamięci RAM (współdzielona z GPU),

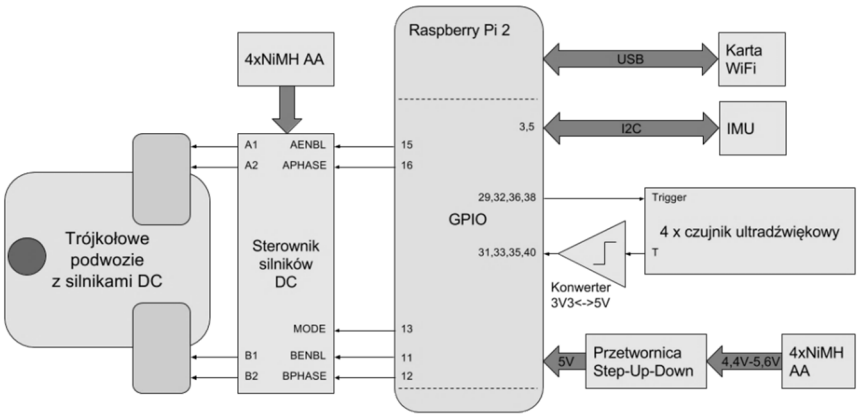
oraz SoC (*System on Chip*) i dedykowaną jednostkę GPU (*Graphics Processing Unit*). Komunikację z otoczeniem zapewnia szereg wejść i wyjść, spośród których w opisywanym zastosowaniu najważniejsze są:

- 40 pinowe złącze GPIO z interfejsami UART, I2C, SPI, PWM,
- cztery złącza USB 2.0,
- gniazdo microSD do podłączenia karty z systemem operacyjnym,
- Ethernet 10/100Mbps.

Ponadto na płytce znajduje się wyjście HDMI (*High-Definition Multimedia Interface*), wyjście analogowe audio/wideo (czteropolowy *jack* 3.5mm), interfejs kamery CSI (*Camera Serial Interface*), interfejs wyświetlacza dotykowego DSI (*Display Serial Interface*) oraz microUSB jako wejście zasilania. Na karcie pamięci SD (*Secure Digital*) zainstalowano system operacyjny Linux Raspbian oparty na popularnej dystrybucji Linux Debian. Dzięki 4 rdzeniom procesora oraz 1 GB pamięci RAM możliwe jest uruchomienie nie tylko procesów obsługujących układy peryferyjne robota, ale także bezpośrednie uruchomienie zaawansowanych środowisk programistycznych, tekstowych i graficznych usług terminalowych do bezpośredniego łączenia się z pulpitem robota, a ponadto usług plikowych i bazodanowych.

Dla modułu RPi2 jest dostępna biblioteka *wiringPi* [9] napisana w języku C zawierająca szereg funkcji umożliwiających m.in. konfigurację i bezpośredni dostęp do GPIO oraz magistral komunikacyjnych. Biblioteka wspiera:

- podstawowe operacje IO, t.j. tryb I/O pinu, rezystor „podciągający”, zapis i odczyt, zapis PWM,
- operacje czasowe (funkcje opóźniające, czas pracy procesu),
- obsługa magistral UART, I2C, SPI,
- programowy kontroler PWM,
- pseudo-przerwania, wątki, priorytet procesu,
- programowy generator prostych dźwięków.



Rys. 2. Schemat blokowy systemu robota mobilnego sterowanego przez Raspberry Pi 2

Fig. 2. System diagram of mobile robot controlled by Raspberry Pi 2

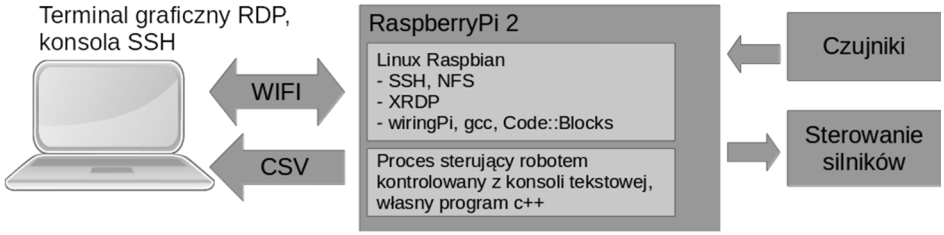
Wraz z bibliotekami programistycznymi dostarczane są narzędzia konsolowe umożliwiające dostęp do funkcji GPIO z poziomu powłoki systemu. Bibliotekę *wiringPi* przeportowano także dla innych języków programowania (Python, Ruby, PHP).

Instalacja systemu operacyjnego Raspbian polega na imporcie jego obrazu ze strony https://www.raspberrypi.org/downloads/raspbian/ i umieszczeniu go na karcie SD za pomocą zalecanego przez opiekunów systemu Raspbian oprogramowania *Win32DiskImager* [11] dla systemu Windows, *Etcher* [10] dla Mac OS lub *dd* dla systemu Linux. Podczas pierwszego uruchomienia modułu RPi2 konieczne jest podłączenie monitora i klawiatury. Dzięki wyprowadzonym złączom HDMI oraz USB nie jest to jednak trudnością. Wstępna konfiguracja polega m.in. na wyborze trybu pracy (GUI, linia poleceń), powiększeniu systemu plików do rozmiarów karty SD oraz konfiguracji połączeń internetowych. Następnie należy doinstalować pakiety wspomagające pracę (np.: *mc, htop, iftop*), kompilatory i środowiska programistyczne (*gcc, g++, Code::Blocks, Geany*), połączenie zdalne (*SSH, xrdp*), itd.

Po skonfigurowaniu i uruchomieniu połączeń zdalnych klawiatura i monitor nie są już potrzebne, ponieważ praca z modułem będzie możliwa z dowolnego komputera z zainstalowanym klientem SSH (np. *putty* dla Windows, *open-ssh* dla Linux) lub/i klientem usług terminalowych RDP (*Remote Desktop Protocol, mstsc „Podłączenie pulpitu zdalnego”* w systemie Windows, *rdesktop* lub *remmina* w systemie Linux).

4. Technika pracy z robotem

Poniżej przedstawiono technikę pracy z robotem, w tym sposób tworzenia oprogramowania i analizy wyników udostępnianych w formie pliku tekstowego CSV (*Comma-Separated Values*). Na rys. 3 pokazano ogólny schemat techniki pracy. Terminal graficzny umożliwia bezpośredni dostęp do pulpitu systemu operacyjnego zainstalowanego w RPi2 oraz uruchomienie środowiska programistycznego dla tworzenia oprogramowania przetwarzającego dane z czujników i sterującego silnikami zgodnie z określonym algorytmem. Oprogramowanie to uruchamia się bezpośrednio na RPi2, a wyniki pracy obserwuje w czasie rzeczywistym na konsoli tekstowej oraz zapisuje do tekstowego pliku CSV. Pliki CSV zawierające dane o stanie robota mogą być udostępnione do dalszej analizy za pomocą usług *nfs* (*Network File System*), *sshfs (SSH File System*, jako klienta pod systemem Windows można użyć programu *WinSCP),* FTP (*File Transfer Protocol*) lub HTTP (*Hypertext Transfer Protocol*).

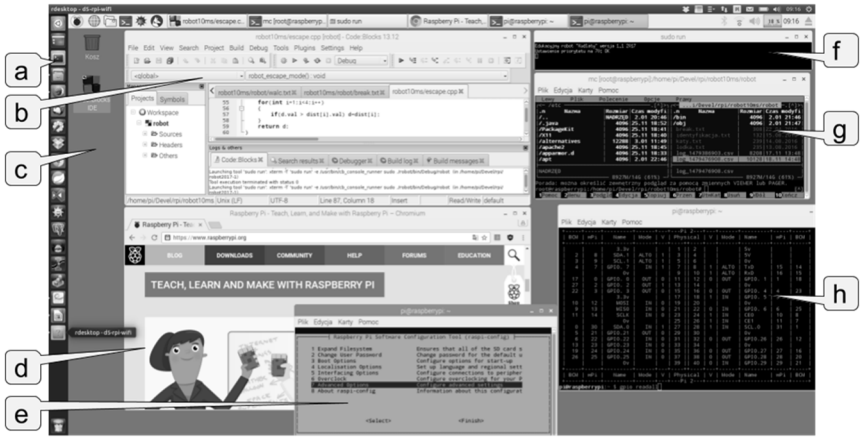


Rys. 3. Schemat blokowy techniki pracy z systemem robota

Fig. 3. Block diagram of working technique with robot system

Do tworzenia oprogramowania wykorzystano środowisko *Code::Blocks.* Jest to wieloplatformowe zintegrowane środowisko programistyczne napisane w C++ wspierające głównie języki C i C++. Funkcjonalność *Code::Blocks* opiera się na wtyczkach (*plugin*), dzięki czemu może być stosunkowo łatwo rozszerzane. *Code::Blocks* umożliwia tworzenie wieloplikowych projektów odciążając programistę od tworzenia własnych skryptów kompilacyjnych (*makefile*), posiada system podpowiedzi kodu (*intellisense*) oraz możliwość dodawania własnych poleceń. Przydaje się to np. w celu uruchomienia kompilowanego programu z wyższymi uprawnieniami wynikającymi z konieczności dostępu do urządzeń peryferyjnych, czy zmiany priorytetu wykonania procesu.

Na rysunku 4 pokazano przykładowy pulpit graficzny RPi2 z systemem Raspbian.



Rys. 4. Pulpit graficzny systemu Raspbian uruchomiony w systemie Ubuntu za pomocą terminala *rdesktop*

Fig. 4. Raspbian graphical desktop running on Ubuntu using the *rdesktop* terminal

Na rysunku 4 widoczne są następujące elementy:

a) pasek boczny systemu Ubuntu, tj. lokalnego pulpitu użytkownika,
b) zintegrowane środowisko programistyczne *Code::Blocks* uruchomione na RPi2,
c) pulpit zdalny procesora RPi2,
d) przeglądarka internetowa,
e) oprogramowanie *raspi-config* służące do podstawowej konfiguracji RPi2,
f) program sterujący robotem uruchomiony poprzez *sudo*,
g) menedżer plików *mc (Midnight Commander)*, umożliwiający m.in. szybki podgląd logów,
h) wynik polecenia *gpio readall* wyświetlający stan pinów GPIO.

Zastosowanie modelu pracy terminalowej umożliwia dostęp do robota z różnych komputerów i praktycznie z każdego miejsca, gdzie dostępne jest połączenie internetowe. Dzięki temu, że programista tworzy oprogramowanie bezpośrednio w systemie operacyjnym robota, jest ono dostępne w całości i w najnowszej wersji przy każdym połączeniu.

5. Zawody robotów 2016

Poniżej krótko scharakteryzowano pierwszą publiczną demonstrację opisywanego robota, która odbyła się na Międzynarodowych Zawodach Robotów

ROBO~motion w dniu 23 kwietnia 2016 roku na Politechnice Rzeszowskiej. Robot został zaprezentowany w konkurencji *Free Style* pod nazwą „Kudłaty". Na potrzeby zawodów zostały zaprogramowane trzy tryby działania:

1. Sterowanie ręczne, gdzie ruchem sterowano bezpośrednio za pomocą klawiatury komputera, na którym uruchomiony był terminal graficzny. Tryb ten umożliwiał sterowanie szybkością robota (klawisze +,-), kierunkiem ruchu przód/tył (W, S), wykonywaniem skrętów lewo/prawo (A, D) oraz szybkich obrotów lewo/prawo w miejscu (Z, X).
2. Ucieczka od przeszkody, w której robot wykorzystywał dane z ultradźwiękowych czujników odległości. Jeżeli poniżej danej odległości (30 cm) od przedniego lub tylnego czujnika pojawiła się przeszkoda, robot oddalał się od niej na bezpieczną odległość (50 cm) i zatrzymywał. Jeśli przeszkoda pojawiła się w zasięgu czujnika bocznego, wówczas robot wykonywał obrót w taki sposób, aby przeszkoda znalazła się w zasięgu czujnika tylnego i odjeżdżał na bezpieczną odległość. Okazało się, że mimo tak prostego algorytmu robot potrafi znaleźć bezpieczny punkt nawet w dość skomplikowanym otoczeniu (np. stoliki, inne roboty, bandy reklamowe), a szukanie bezpiecznego punktu wyglądało atrakcyjnie dla publiczności.
3. Odtwarzanie sekwencji ruchu zapisanej w postaci prostego programu w pliku tekstowym. W tym celu opracowano prosty język skryptowy obsługujący deklaracje zmiennych, proste bezparametrowe procedury i bezwarunkowe pętle. Dzięki wykorzystaniu stosu, pętle i procedury mogły być zagnieżdżone. Każda elementarna instrukcja znajdowała się w osobnej linii. Program wykonywany był z góry na dół, wielkość znaków słów kluczowych musiała zostać zachowana, możliwe były wcięcia spacjami i puste linie. Program sekwencji ruchu składał się z trzech części: deklaracja zmiennych (VARIABLES … VARIABLES_END), deklaracja procedur (PROCEDURES … PROCEDURES) oraz program główny (PROGRAM … PROGRAM_END). W tabeli 1 przedstawiono słowa kluczowe i polecenia języka skryptowego, gdzie w nawiasach kwadratowych ([ ]) wpisano parametry podawane przez użytkownika nie będące częścią języka.

Tabela 1. Słowa kluczowe języka skryptowego

Table 1. Script language keywords

Słowo kluczowe	Opis
VARIABLES	Początek bloku deklaracji zmiennych
VARIABLES_END	Koniec bloku deklaracji zmiennych
PROCEDURES	Początek bloku deklaracji procedur
PROCEDURES_END	Koniec bloku deklaracji procedur
PROGRAM	Początek bloku programu („punkt wejścia”)
PROGRAM_END	Koniec programu
$[*nazwa*]	Deklaracja i użycie zmiennej, np. $krok = 100
proc [*nazwa*]	Początek procedury *nazwa*, np.: proc circle
end_proc	Koniec definicji procedury
call [*nazwa*]	Wywołanie procedury, np.: call circle
loop [N]	Początek bloku pętli, gdzie N jest liczbą powtórzeń. Parametr N może być liczbą wpisaną bezpośrednio lub zmienną zadeklarowaną wcześniej, np.: loop 20, loop $circ_count
end_loop	Koniec bloku pętli
set [L] [R] [T]	Polecenie elementarne ustawiające procent mocy nominalnej na kołach robota przez podany czas, gdzie: • L - moc na kole lewym w zakresie -100 do 100 [%] • R - moc na kole prawym w takim samym zakresie • T - minimalny czas wykonania polecenia [ms]
cor [L] [R] [T]	Polecenie elementarne wykonujące korektę aktualnej mocy na kołach robota przez podany czas, gdzie: • L - korekta mocy na kole lewym w zakresie -100 do 100 [%] • R - korekta mocy na kole prawym w takim samym zakresie • T - minimalny czas wykonania polecenia [ms]

Krótki program rozpędzający robota od 0 do 100% w czasie 10 sekund (100 x 100 milisekund), a następnie wprowadzający go w ruch obrotowy trwający 5 sekund z 50% mocy na kołach ma postać:

```
VARIABLES
  $l_circ=50
  $r_circ=-50
VARIABLES_END
PROCEDURES
  proc circle
    set $l_circ $r_circ 5000
  end_proc
PROCEDURES_END
```

```
PROGRAM
  set 0 0 0
  loop 100
    cor 1 1 100
  end_loop

  call circle
  set 0 0 0
PROGRAM_END
```

Cały kod interpretera skryptu zajmuje około 300 linii tekstu. Podczas publicznej prezentacji w trakcie zawodów ROBO~motion 2016 korzystając z programu napisanego w tym języku skryptowym robot wykonał symulację ruchów walca wiedeńskiego w takt klasycznego utworu *Fale Dunaju* Josefa Ivanovicia.

6. Podsumowanie

W pierwszej fazie prac autora nad algorytmami nawigacji w czasie rzeczywistym udało się wykonać prototyp pełnosprawnego minirobota oraz przygotowano i przetestowano zestaw narzędzi oraz technik pracy nad rozwojem jego funkcjonalności. Dotychczasowe algorytmy były realizowane bez sprzężeń zwrotnych i czujników innych niż ultradźwiękowe.

W artykule zaprezentowano minirobot laboratoryjny skonstruowany dla przyszłych badań. Przedstawiono jego budowę mechaniczną, komputer sterujący wraz z zestawem oprogramowania użytkowego, charakterystykę i technikę zdalnej pracy z robotem. Zostały przeprowadzone pierwsze testy w ruchu, robot został także zaprezentowany na Międzynarodowych Zawodach Robotów ROBO~motion 2016. Zbudowany minirobot wydaje się spełniać oczekiwania oraz być solidną platformą rozwojową dla dalszych badań.

W ciągu następnych kilku miesięcy od zawodów ROBO~motion 2016 przygotowano kolejne elementy oprogramowania użytkowego, takie jak:

- kompensacja tarcia statycznego
- utrzymanie stałego kursu geograficznego
- utrzymanie stałej odległości od poruszającego się „przewodnika”
- obrót tworzący mapę odległości od przeszkód w otoczeniu robota

Elementy te wykorzystują dane z ultradźwiękowych czujników odległości oraz z magnetometru. Do sterowania zastosowano typowe mechanizmy ze sprzężeniem zwrotnym (regulatory PI) oraz filtry cyfrowe. Badania nawigacyjne o krótkim zasięgu w czasie rzeczywistym będą wykonywane na prostokątnej arenie. Planuje się także dodanie obsługi akcelerometru oraz kamery, jednej na robocie, a drugiej zewnętrznej. Celem następnego etapu prac jest uzupełnianie oprogramowania o algorytmy nawigacyjne, testowanie cyfrowej filtracji sygnałów, dobór parametrów algorytmów oraz zastosowanie metod inteligencji obliczeniowej (sieci neuronowe) do lokalizacji robota.

Literatura

[1] Dudek D., Kazała R., Strączyński P.: Mobilny robot manipulacyjny wykorzystujący technologie Internetu Rzeczy w systemie sterowania i monitorowania, Pomiary Automatyka Robotyka, nr 4/2016, s. 37-45.

[2] Figurowski D., Brasel M., Kubicki M.: Stanowisko laboratoryjne do badań algorytmów sterowania robotami mobilnymi z wizyjnym sprzężeniem zwrotnym, Pomiary Automatyka Robotyka, nr 3/2016, s. 71-76.

[3] Kalisch M., Panfil W.: System sterowania grupą robotów ligi Small Size Robot League, Pomiary Automatyka Robotyka, nr 11/2014, s. 90-95.
[4] Leniowski R.: Podstawy robotyki, Uniwersytet Rzeszowski, Rzeszów 2013
[5] Węgierek M., Świstak B., Winiarski T.: Modularne środowisko do rywalizacji robotów sportowych śledzących linię, Pomiary Automatyka Robotyka, nr 3/2015, s. 61-66.
[6] http://eti.pg.edu.pl/katedra-systemow-decyzyjnych-i-robotyki/aktualnosci/-/asset_publisher/Km3ylDPmIIDZ/content/roboty-mobilne
[7] http://rab.ict.pwr.wroc.pl/lab_010/stanowiska/khepera.php
[8] http://raspberrypi.org
[9] http://wiringpi.com
[10] https://etcher.io/
[11] https://sourceforge.net/projects/win32diskimager/
[12] https://www.k-team.com/khepera-iv
[13] https://www.lego.com/pl-pl/mindstorms

PROTOTYPE THREE-WHEEL LAB MINIROBOT

S u m m a r y

The paper presents construction of a three-wheel lab minirobot used initially as a sensor testing platform, and in future for evaluation of intelligent navigation algorithms in real motion environment. Availability of elements, easy assembling, and low price have been construction guidelines. The robot is equipped with Raspberry Pi 2 microcomputer and Linux Raspbian operating system. Together with application programs, it operates both as a control system and development platform allowing to prepare and run programs directly in the robot. Communication is provided by terminal services, so easy programming the robot from any place with internet access is possible. The construction described here was presented at Rzeszow Robo~motion 2016 competition. Three operating modes were available at that time.

Keywords: Mobile robot, Raspberry Pi 2, ultrasonic sensors, IMU

DOI: 10.7862/re.2017.4

Tekst złożono w redakcji: marzec 2017
Przyjęto do druku: maj 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (1/2017), styczeń-czerwiec 2017, s. 53-65

Mariusz SZAREK [1]
Mariusz NYCZ[2]
Sara NIENAJADŁO[3]

THE ANALYSIS OF EFFCIENCY AND PERFORMANCE OF INTRUSION PREVENTION SYSTEMS

This article aims at presenting a comparative analysis of two intrusion detection and prevention systems, namely Snort and Suricata, run in the af-packet mode in the context of the efficiency of their protection against the denial of service attacks. The paper sets out, in statistical terms, the denial of service attacks and distributed denial-of-service attacks occurring around the world. In the further part of the research, penetration tests were conducted in order to assess comparatively analysis of the efficiency of IDS/IPS systems was carried out in the context of starting various numbers of network connected devices as well as in the case of sending packets with different sizes. This article is addressed to security systems administrators as well as to people involved in security systems implementation.

Keywords: security, network, test, protection, detection, service, denial, intrusion, system, DDoS, DoS, attack

1. Introduction

Recent years were marked by the significant progress in the field of devices and ICT technologies in the case of their access to the World Wide Web. This phenomenon is getting more and more dynamic in the last months and years. It has become a regular occurrence that devices such as TV sets, smartphones, tablets and computers are equipped with solutions which enable their users to access the network. The scope of the phenomenon and the research are so significant that the designing and producing have been started of prototypes of other television, radio and household electrical appliances with the capability of network communication. As a consequence of such a widespread digitalization risks and dangers resulting from the use of network devices are growing. These dan-

[1] Mariusz Szarek, Politechnika Rzeszowska, 783535006, 132887@stud.prz.edu.pl
[2] Autor do korespondencji: Mariusz Nycz, Politechnika Rzeszowska, Zakład Systemów Złożonych, mnycz@prz.edu.pl
[3] Sara Nienajadło, Politechnika Rzeszowska, sara.n@op.pl

gers are cyber attacks such as worms, viruses and Trojan horses. They are based on the use of incorrectly programmed or designed applications and devices with security gaps in source codes. These attacks aim at, among others, stealing sensitive information such as personal data of a user/ a company/ an institution as well as at deleting or replacing that data, requesting access to and taking control over the given application/ device/ account/ system or creating the situation when the access to a given service/ assistance is denied. Protection against these types of dangers enhanced to the most is possible thanks to the use of a wide scope of security measures. The advancement, the range and the kind of safety technology used should be determined by the importance and the value of resources and data which are to be protected [17].

Systems, programs, applications and devices developed have security gaps in software and a source code, mainly as a result of an insufficient number of operational tests. The scope of these gaps depends on the type and the advancement of the technology applied. Hackers use these gaps in order to conduct various kinds of cyber attacks. Assistance, support and the automatic update of a code do not provide the comprehensive solution to the problem because the time span between the moment of identifying the weak point in the software and then working out as well as sending a patch by the programmer is long enough to carry out the attack. Together with the growing number of dangers a broad range of solutions is getting more and more available, which not only reduce significantly the risk but also happen to eliminate it completely from time to time.

At present, Denial-of-Service attacks (DoS) and Distributed Denial-of-Service attacks (DDoS) are extremely popular. The attacks are intended to block the possibility to use and administer web servers of various types of companies and institution, namely websites of non-governmental organizations, self-governing and scientific bodies, and websites of banks, shops and web portals. Attacks result in the huge increase of delay times of particular sites or, in the worst case, in the complete standstill. Successful attack on a given web site can cause the loss of trust of customers and users connected with this institution, which can in turn considerably affect the financial performance. DoS attacks are used for political and terrorist reasons in order to block systems and web sites which a crucial for a state.

There is a wide variety of solutions which protect the respective network's and information systems' components against DoS and DDoS attacks. It is recommended for instance to use only essential and necessary programs, applications and services. Access lists at routers and firewalls are created and configured. The use and accessibility of hardware and computational resources as well as CPU utilization are monitored on a continuous basis. Network capacity limits are introduced. Administrators and users are forced to write long and complex passwords which include capital and lower case letters, digits and special cha-

racters. They are also obliged to change passwords very often. Frequent, regular and automatic firmware updates are performed in order to eliminate gaps in the software. Frequent and systematic backup copies of company's data are made. In the case of the attack tools are used which enable to target a type and source of this attack and, furthermore, cause the immediate cut-off of a network and devices from the source.

Intrusion Detection Systems and Intrusion Prevention Systems are among the most modern, the most efficient and the most common tools used to protect against Denial-of-Service attacks and Distributed Denial-of-Service attacks. There are two of IDS/IPS systems – physical (hardware) and logical (software). They are used to detect and also react to attack attempts on networks, systems, and network devices in the case of IPS systems. Many global companies from the IT security and computer network branch produce physical solutions, which are expensive to buy and to operate and for this reason used only in the largest companies and institutions. Free programming solutions, which base their operations on packet lines, are used widely.

2. The Presentation of Denial-of-Service attacks

2.1. Definition and Types of Denial-of-Service Attacks

Denial-of-Service attacks are specified as cyber attacks which aim at making a given service or a computer system stop working as a result of a saturation of hardware or computational resources. These are the most frequent, the most productive and the most effective cyber attacks. There is a high variety of techniques, solutions and ways of denial-of-service attacks, which are used by hackers according to the objective pursued, and its advancement and complexity. As an example, the Denial-of-Service attack is the transmission of an enormous number of packets to the victim's environment in order to occupy all the resources available and as a result to cause the device or a system malfunction due to overload. The use of security loopholes in particular protocols of ISO/OIS model layers is one the other way employed by attackers. Denial-of-Service attacks are characterized by the fact one does not need huge financial push, extraordinary amount of time or expensive devices in order to conduct them and, what is more, the structure of the attack is not complicated as well. Due to the aforementioned factors, Denial-of-Service attacks are growing in frequency, complexity and advancement. Hackers draw up and create new, innovative and increasingly complex forms, ways, types, techniques and methods of these attacks. The fowing diagram presents Denial-of-Service attacks which occurred [1][2] (Fig. 1).

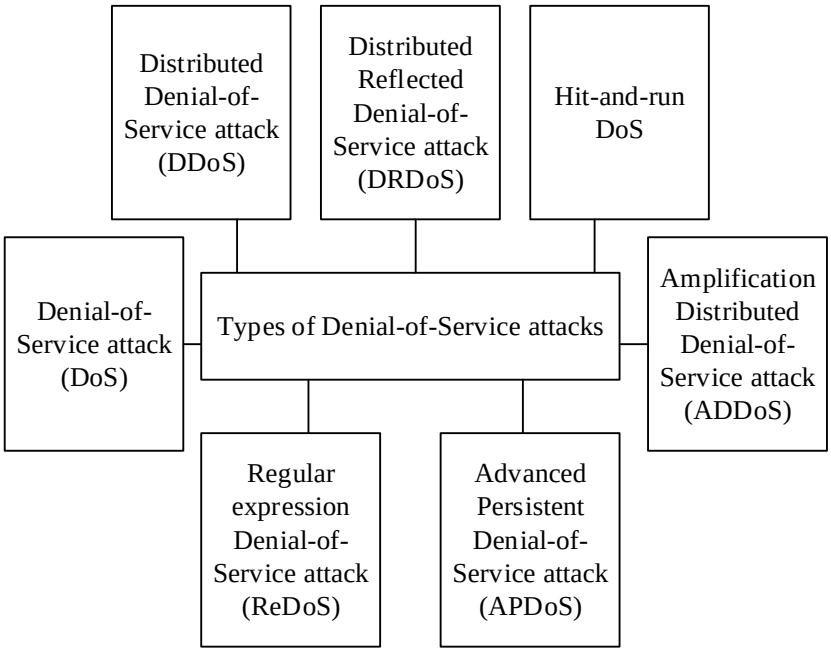


Fig. 1. Types of existing Denial-of-Service attacks [1] [2]

2.2. The statistics of existing Denial-of-Service attacks around the world in the fourth quater of 2016 and first quarter of 2017

Companies, which produce solutions to protect data, resources, servers, devices and network services against cyber threats, conduct research and compile statistics that enable them to evaluate existing dangers more efficiently and also fight with these threats. The aggregated results of research and statistics define the trends of existing dangers in the event of cyber attacks which will make it possible to create new hardware and software solutions for ensuring protection as well as improve the existing ones.

Each quarter, Akamai company presents results of research devoted to the occurrence of Denial-of-Service attacks around the world. According to the report from the first quarter of 2017 the fragmentation of UDP packets was the most frequent cause of Denial-of-Service attacks around the world since it adds up to 29% of all the dispersed Denial-of-Service attacks conducted in the first quarter of 2017. Among other frequent attacks are those directed at protocols NTP, DNS, SYN segment as well as UDP flood. The graph below shows the frequency of particular targets of DoS and DDoS attacks in the first quarter of 2017 [3] (Fig. 2).

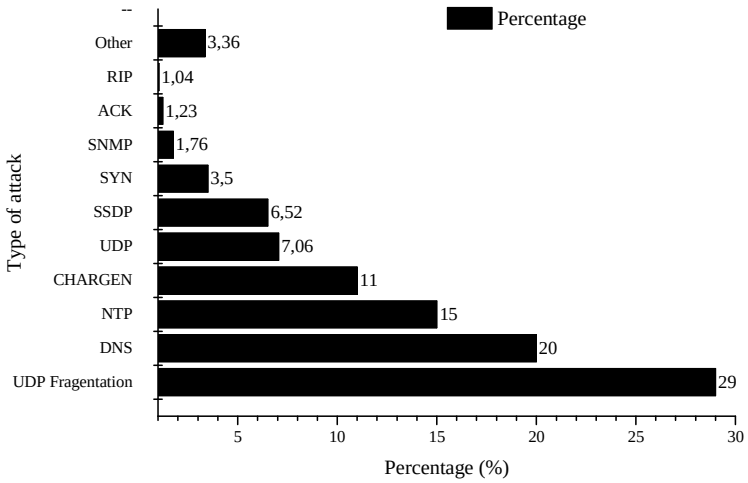


Fig. 2. Percentage summary of the types of DoS and DDoS attacks which took place around the world in Q1 2017 [3]

Furthermore, the report of Akamai company presents a league of countries where web application attacks took place most often in the first quarter of 2017. U.S. has been ranked first in this evaluation. 221 million of the attacks happening in the first quarter of 2017. Countries such as Brazil, U.K., Japan and Germany noted much less of the web application attacks. The graph below shows a league table of countries where web application attacks were most frequent in the first quarter of 2017 [3] (Fig. 3).

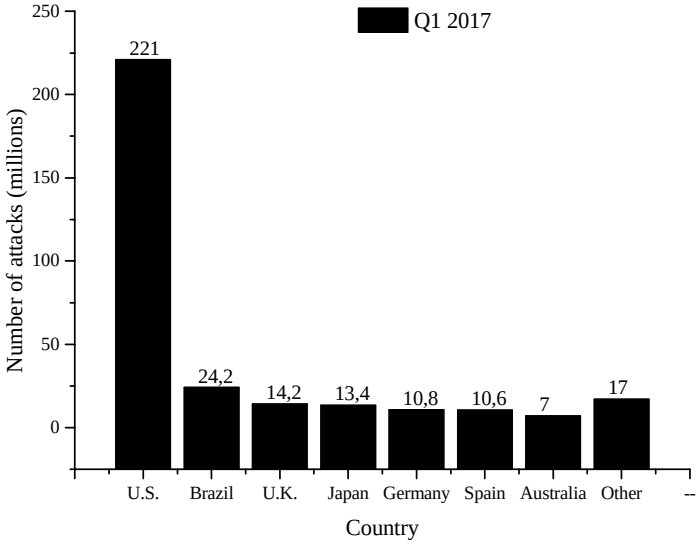


Fig. 3. Top Source Countries for web application Attacks, Q1 2017 [3]

The following graph presents frequency of web application attacks which took place in first quarter of 2017 (Fig. 4). The most popular type of attack is SQL injection, with 44% of all attacks. On the second place is LFi taking up 39% of web application attacks. The third place occupies XSS with 10% of all web application attacks [3].

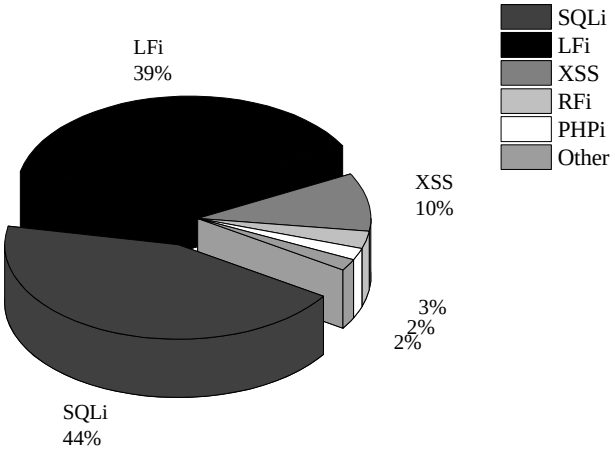


Fig. 4. Web Application Attack Frequency, Q1 2017 [3]

3. The Analysis of Efficiency nad Productivity of IDS/IPS Snort and Suricata Systems run in the af-packet mode when faced with DoS AND DDoS attacks

Intrusion Detection Systems and their extension, namely Intrusion Prevention Systems are an efficient and widely used way of fighting against threats connected with Denial-of-Service attacks and other cyber-attacks. Their objective is to maximalise in real time the safety of administrators and users of particular systems, applications and Web services against attacks through the implementation of specifically designed physical (hardware) and logical (software) solutions [4].

Intrusion Detection Systems are used to identify unauthorized and unwanted system or computer network invasion. They are highly specialized tools such as devices, applications and services executed on electronic equipment connected with the network. These systems monitor the network in real time in order to detect possible risks, dangerous elements, components, events and in order to break security policy rules of a given electronic system. Founding this dangerous element result in creating the message stored in a database or in a source file. The most important in the process of working out the intrusion detection system is the implementation of solutions which enable system to operate automatically

without the constant control of an administrator, a user. Such solutions make it possible to modify in real time options and properties of a firewall. These solutions allow to eliminate almost completely the occurrence of the attack which use vulnerabilities in a source code [4-6].

Intrusion Prevention Systems are extensions of IDS systems with mechanisms which prevent breaking into by rejecting packets with malware sent to a victim of an attack. These mechanisms are added to properties, functions and features of IPS systems. Appropriate library must be added to a system and this system must be placed on the packet line so that system IDS will be able to work efficiency as IPS system [4].

The effectiveness analysis of IDS/IPS systems in the context of the protection against Denial-of-Service attacks was conducted with the example of two free-of-charge programming systems IDS/IPS Snort and Suricata which run in the af-packet mode.

3.1. The description of configured and used test environment

IDS/IPS Snort and Suricata systems which are run in the af-packet mode were analyzed in terms of their effectiveness concerning the protection against dispersed Denial-of-Service attacks: SYN-Flood and Land [7-10].

The test environment comprising of three virtual machines with Debian system and IDS/IPS Snort and Suricata systems were prepared to cater the needs of simulation and research. These machines carried out the functions of machines under attack. Moreover, the test configuration comprises of attacking environment, namely the virtual machine with Kali Linux system installed. Open source packets generator hping3 was installed on this system, which was used to simulate attacks. Apart from attacking machines and the machines under attack there was also a router in the network which provided connection between virtual machines and Internet [11-16].

3.2. Research and comparison of the effectiveness of IDS/IPS systems run in the af-packet mode in the context of the protection against Denial-of-Service attacks concerning SYN-Flood and Land

Initially, tests were conducted on the machine of a victim in the situation when there was no IDS/IPS system operating in the environment of the victim. Research was conducted with various numbers of terminals switched on when SYN-Flood attack was up and running in the attacking environment. This graph below shows response time during communications between different network entities in case of SYN-Flood attack on the Network without any of the IDS/IPS systems operating (Fig. 5).

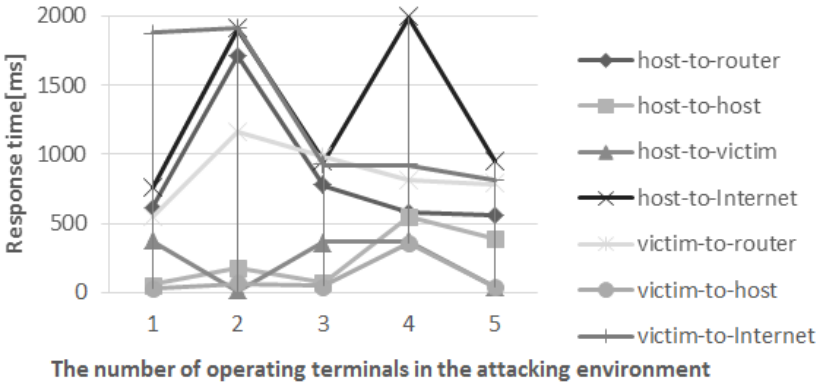


Fig. 5. Response time during communication between respective network entities in case of Land attack on the system without any of the IDS/IPS systems operating

Next testing phase was based on researching the response time of particular network entities in situation when IDS/IPS Snort and Suricata systems run in the af-packet mode. The research was conducted with various numbers of switched on terminals when SYN-Flood attack was conducted in the attacking environment. The graph below shows response time during communication between different network entities in case of SYN-Flood attack on the network with Snort system run in the af-packet mode (Fig. 6).

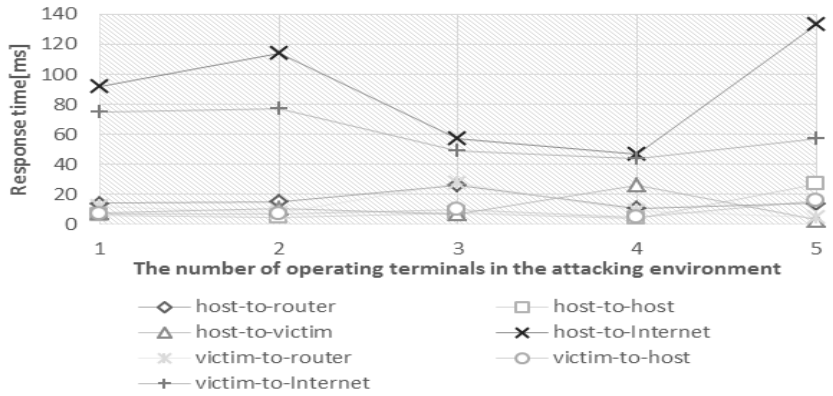


Fig. 6. Response time during communications between different network entities in case of SYN-Flood attack on the network with Snort system run in the af-packet mode

The graph below shows response time during communication between different network entities in case of SYN-Flood attack on the network with Suricata system run in the af-packet mode (Fig. 7).

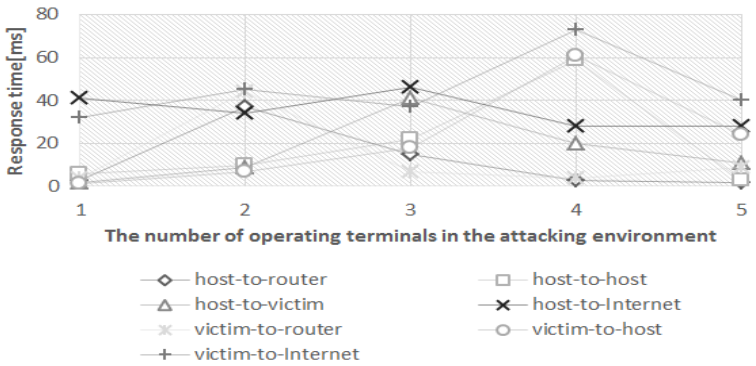


Fig. 7. Response time during communications between different network entities in case of SYN-Flood attack on the network with Suricata system run in the af-packet mode

Land attack was the second Distributed Denial-of-Service attack which was examined in the research. As in the case of SYN-Flood attack, first one examined delay time during communications between particular network entities in case when there was no IDS/IPS system operating. Research was conducted with various numbers of terminals switched on when Land attack was up and running in the attacking environment. This graph shows response time during communications between different network entities in case of Land attack on the network without any of the IDS/IPS systems operating (Fig. 8).

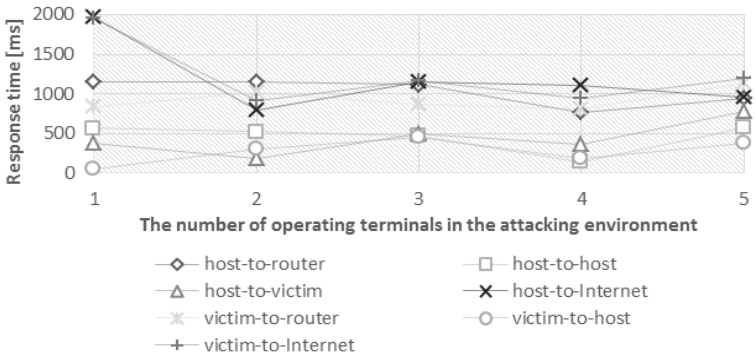


Fig. 8. Response time during communications between different network entities in case of Land attack on the network without any of the IDS/IPS systems operating

Similarly to SYN-Flood attack, next testing phase was based on researching the response time of particular network entities in situation when IDS/IPS Snort and Suricata systems run in the af-packet mode. Research was conducted with various numbers of terminals switched on when Land attack was up and running

in the attacking environment. The graph below shows response time during communication between different network entities in case of Land attack on the network with Snort system run in the af-packet mode (Fig. 9).

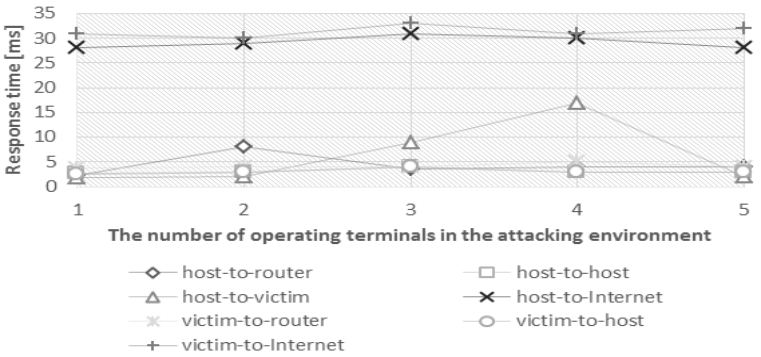


Fig. 9. Response time during communications between different network entities in case of Land attack on the network with Snort system running in the af-packet mode

The graph below shows response time during communication between different network entities in case of Land attack on the network with Suricata system run in the af-packet mode (Fig. 10).

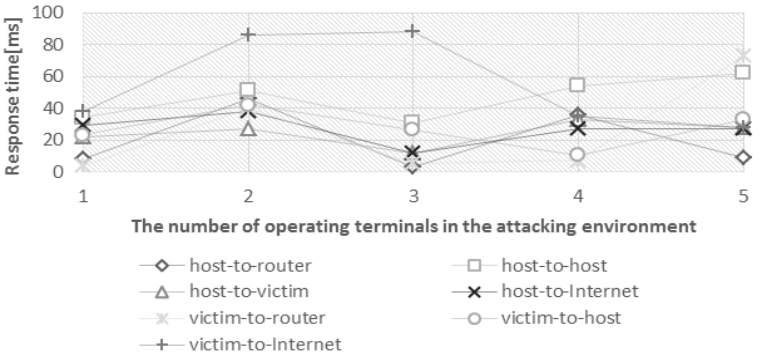


Fig. 10. Response time during communications between different network entities in case of Land attack on the network with Suricata system run in the af-packet mode

3.3. The efficiency tests of IDS/IPS Snort and Suricata systems with regard to response time depending on the number of served hosts and on the size of transmitted packets

A part from the tests of IDS/IPS systems in the context of the efficiency of their protection against Denial-of-Service attacks and Distributed Denial-of-

Service attacks, the productivity analysis of these systems was also carried out. To this end, delay time was examined during packet transmission on a line host-router in case of various numbers of hosts served by IDS/IPS system. The graph bellow shows delay time in communication between a host and a router with Snort and Suricata system running in the af-packet mode when these systems serve various number of network devices (Fig. 11).

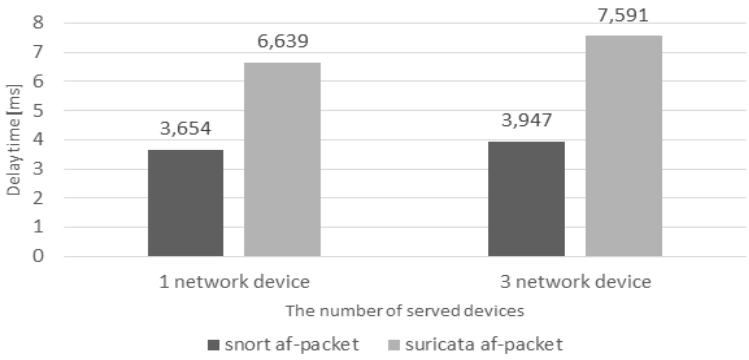


Fig. 11. Delay time in communication between a host and a router with Snort and Suricata system running in the af-packet mode when these systems serve various number of network devices

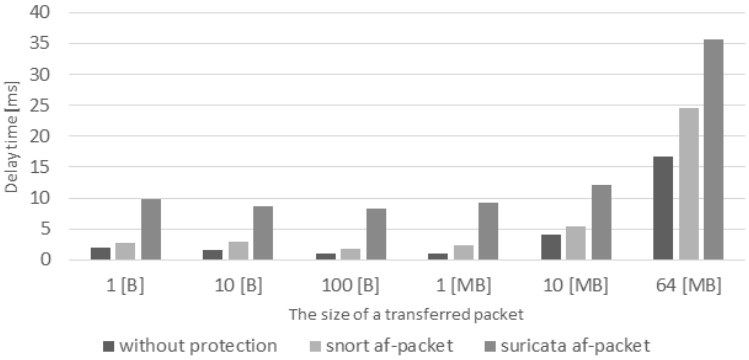


Fig. 12. The comparison between delay time during the transmission of packets having various sizes between a host and a router when there is no IDS/IPS system operating, when Snort system is running in the af-packet mode, when Suricata system is running in the af-packet mode

The second efficiency test of IDS/IPS Snort and Suricata systems consisted in the observation of delay time during the transmission of packets having various sizes between a host and a router when the systems were switched on. The graph below presents delay time during the transmission of packets having va-

rious sizes between a host and a router when there is no IDS/IPS system operating, when Snort system is running in the af-packet mode, when Suricata system is running in the af-packet (Fig. 12).

4. Summary

The research conducted proved that IDS/IPS Snort and Suricata systems run in the af-packet mode are efficient in protecting devices, resources and network entities against Land attack which belongs to the group of Denial-of-Service attacks. The start of both these systems causes the significant reduction in response time during communications between various network entities, which leads to the uninterrupted use of network services. As far as SYN-Flood is concerned, Suricata is slightly more efficient with delay time not exceeding 80 [ms], but in case of Land attack Snort system is more efficient with response time not exceeding 35 [ms]. On the basis of results obtained one can claim that both Snort and Suricata run in the af-packet mode are protecting the network effectively against Denial-of-Service attacks and Distributed Denial-of-Service attacks. The productivity tests show that Snort system is more productive than Suricata system, because regardless of the number of hosts of the size of transmitted packets, response time when this system is operating is lower than response time when Suricata system is switched on. Both is case of Snort and Suricata system the increase in the number of hosts served does not cause the significant increase in response time. The size of transmitted packets is of almost no importance to the efficiency of IDS/IPS systems on condition that packets transmitted are of low (up to 1[MB]). The transmission of huge packets (more than 1[MB]) cause the significant increase in responses during communication between particular network elements when IDS/IPS systems are operating.

References

[1] https://dataspace.pl/dos-rodzaje-atakow-cz-1/[Access: 24.08.2015]

[2] https://dataspace.pl/dos-rodzaje-atakow-cz-2/[Access: 3.09.2015]

[3] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-security-executive-summary.pdf [Access: 19.05.2017]

[4] K. Scarfone, P. Mell: Guide to Intrusion Detection and Prevention Systems (IDPS)

[5] http://students.mimuw.edu.pl/SO/Projekt04-05/temat5-g2/sikora-kobylinski/idsips.html [Access: 23.12.2015]

[6] http://sekurak.pl/wprowadzenie-do-systemow-ids/[Access: 23.03.2015]

[7] http://insecure.org/sploits/land.ip.DOS.html[Access: 20.11.1997]

[8] http://www.computerworld.pl/news/291980/Atak.na.sieci.IP.html [Access: 29.12.1997]

[9] https://www.incapsula.com/ddos/attack-glossary/http-flood.html [Access: 18.10. 2015]
[10] https://www.incapsula.com/ddos/attack-glossary/syn-flood.html [Access: 18.10. 2015]
[11] https://www.debian.org/doc/ [Access: 7.04.2015]
[12] https://www.snort.org/documents/snort-ips-tutorial [Access: 25.08.2015]
[13] https//www.snort.org/documents [Access: 25.08.2015]
[14] https://www.kali.org/kali-linux-documentation/ [Access: 2.01.2016]
[15] http://wiki.hping.org [Access: 30.09.2009]
[16] http://suricata-ids.org/docs/ [Access: 6.08.2014]
[17] Ch. Chapman: Network Performance and Security: Testing and Analyzing Using Open Source and Low-Cost Tools

BADANIE SPRAWNOŚCI SYSTEMÓW IDS/IPS PRZED ATAKAMI DOS I DDOS

S t r e s z c z e n i e

Tematem artykułu jest analiza sprawności systemów wykrywania i zapobiegania włamaniom przed atakami odmowy usługi. W początkowej cześć artykuł w oparciu o wynik analiz, zaprezentowano skalę problemu omawianych zagrożeń. W kolejnych paragrafach przedstawiono metodykę badań określenia podatności na ataki odmowy usługi. Następnie przeprowadzono symulacje wydajności i skuteczności obrony przed atakami dwóch sieciowych systemów wykrywania włamań w segmencie open-source Snort i Suricata. Analizowano rozwiązania pracując w trybach nfqueue i af-packet, przy zestawie tych samych reguł. Przeprowadzone testy porównawcze z wykorzystaniem dwóch najpopularniejszy zagrożeń tj. Land i SYN Flood, wykazały przewagę rozwiązania Suricata w skuteczności wykrywania analizowanych ataków. Artykuł jest adresowany do osób zajmujących się wdrażaniem i administracją systemów zabezpieczeń.

Słowa kluczowe: sieci, bezpieczeństwo, ochrona, testy, odmowa, usługi, wykrywanie, wtargnięcie, przeciwdziałanie

DOI: 10.7862/re.2017.5

Tekst złożono w redakcji: maj 2017
Przyjęto do druku: czerwiec 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 294, Elektrotechnika 36
RUTJEE, z. 36 (1/2017), styczeń-czerwiec 2017, s. 67-76

Mariusz NYCZ[1]
Tomasz SZELIGA[2]
Piotr HAJDER[3]

ASSESSMENT OF THE VULNERABILITY OF THE APACHE SERVER TO DDOS ATTACKS

The article presents an analysis of the vulnerability of the Apache server with regard to common DDoS attacks. The paper begins with presenting the statistical overview of the issue of denial-of-service attacks. We also discuss the methods used for performing DDoS attacks. Working with the virtual systems, the authors designed a test environment, where the assessment was conducted of the vulnerability of selected WWW systems. At the end of the article, actions are proposed to implement effective methods of defending against the denial-of-service attacks. The paper is written for the specialists in the field of web systems security.

Keywords: DDoS Attack; security; the Apache; web server

1. Introduction

With every passing year, ensuring the reliability of the operation of WWW servers is becoming a more and more important issue. The high requirements set for the web services, such as e-banking, e-transaction systems or electronic trading result in setting the accessibility at 99.9%. Along with the increase of the importance of the web systems, we can now observe a dynamic development of new threats and techniques aimed at lowering or even paralyzing the accessibility to the system. Properly performed dispersed denial of service attacks (DDoS) pose a serious threat to all the services on the Internet. The main idea of the denial-of-service attacks is to use up all the WWW server resources, which results in the implemented WWW services being inaccessible, which in turn leads to serious financial losses. We can expect the number of the attacks to increase in the next couple of years, and the methods of attacking to become more and more advanced. Currently used mechanisms of detection and protection against this kind of threats are not fully sufficient.

[1] Autor do korespondencji: Mariusz Nycz, Politechnika Rzeszowska, Zakład Systemów Złożonych, mnycz@prz.edu.pl
[2] Tomasz Szeliga, Politechnika Rzeszowska
[3] Piotr Hajder, Akademia Górniczo-Hutnicza w Krakowie

2. Denial-of-service attacks – a statistical overview

The presented results were formulated on the basis of analysing 459 web-sites belonging to multiple owners from the Subcarpatian voivodeship. Fig. 1 presents the market share of each web server software program. Achieved results were compared with data provided by Netcraft (world) and amudom (Poland). Results show overrepresentation of the Apache server on the Polish market.

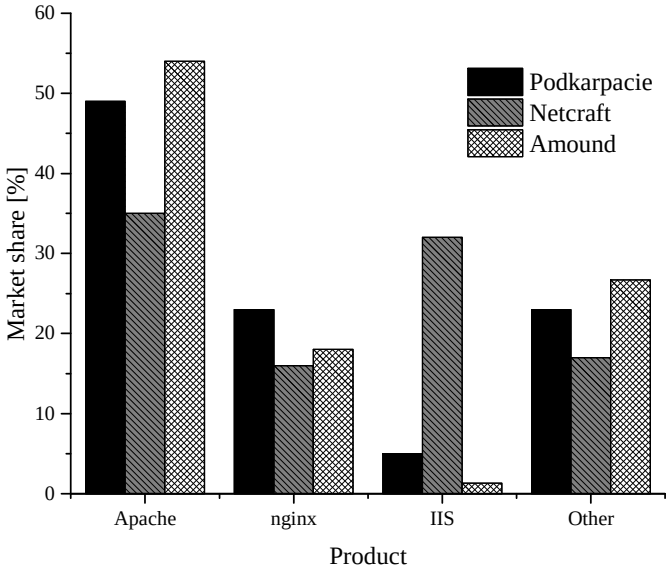


Fig. 1. Web-server software market in 2016 [1, 2]

According to DDoS Attack Report by Prolexic, sales and financial services were the most popular targets for the attacks in the area of web applications [3]. Akamai organization published a report about denial of service attacks. Fig. 2 presents the statistical data on the percentage of different types of attacks. This kind of attacks is performed usually for financial gain. According to the report [3], one of the purpose of this kind of attacks is to buy valuable goods at lower prices.

The attacks began to be aimed also at the financial services provided by the e-banking companies. Denial-of-service attacks are usually performed to steal the records from the existing databases of the banking institutions, which results in making their market situation worse. According to the report [3], DDoS attacks aimed at the sales industry make up 40% of all the application-layer attacks. By comparison, most of the attacks at the web layer are aimed at the game industry, where the protection against the application-layer attacks is very often weaker.

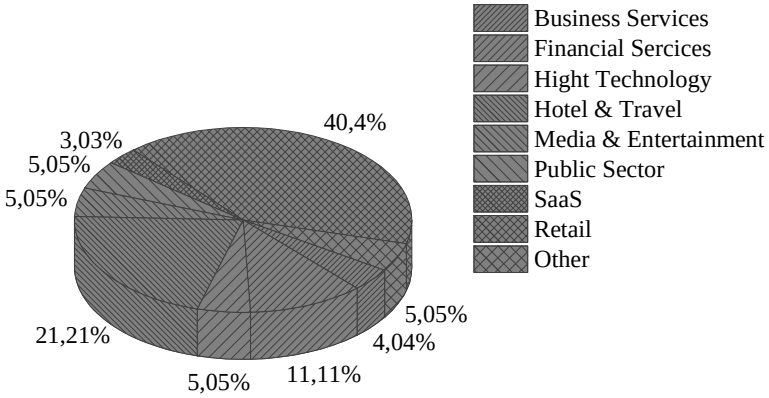


Fig. 2. Percentage of the application-layer attacks in the industry [3]

The number of the attacks increases along with the development in the field of technology. The report [3] includes statistical data regarding the direction of DDoS attacks in the recent years. Fig. 3 presents the data regarding 4rd quarter of 2016.

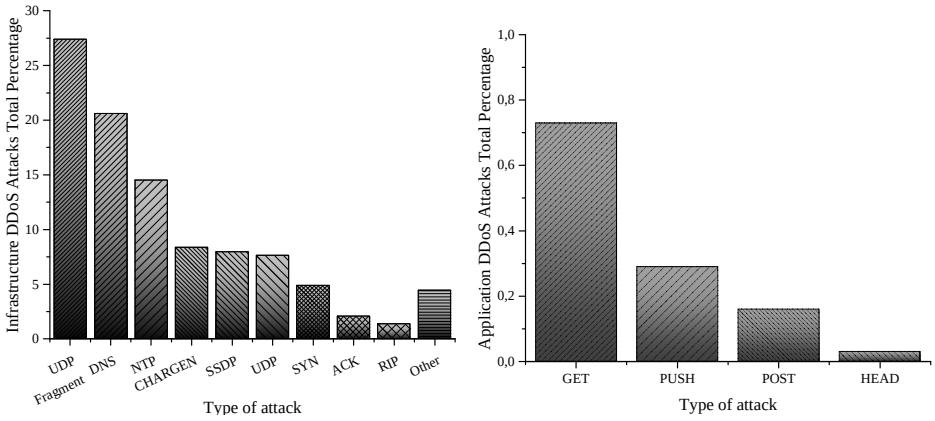


Fig. 3. Directions of denial-of-service attacks [3]

3. The types of DDoS attacks

The analysis performed allowed for the assessment of the effectiveness of different methods of the attack. Slowloris and R.U.Dead.Yet scripts were tested, as well as Syn Flood attack [2, 5]. Below you can find the description of the types of the attacks used for the tests:

- Slowloris – attack with HTTP Get queries. The main task of the script it to maintain the connection by completing the fragments of the header.

The maximum time for sending a package which maintains the connection is 300 sec. Slowloris does not destroy the hardware or the data of the server. It is impossible to detect the attacker by the Apache server logs only [10]. The attack was performed with the following request:

perl slowloris.pl –dns 192.168.0.109 –port 8080 –time 50 –num 1000 (1)

Where: dns is the destination address for the attack, port is the HTTP port number, time is the delay between the requests sent and num is the number of threads used during a single attempt at connecting [16].

- R.U.Dead.Yet – a free script using HTTP Post queries. The attack is performed by sending incomplete but justified headers. Every time, the fragments of the header body are sent, 1 byte each, at a very low speed. The task of every server is to compare the number of the bytes received with the value of the Content-Length field. Adding new information to the header body continuously results in the server being unable to complete the connection, which makes it use more and more of its resources to perform the operation of checking the number of the bytes of the received information. The post header is not being buffered [12]. The authors used Slowhttptest application to generate HTTP Post traffic (2).

Slowhttptest –c 600 –B –i 1 –t POST –g –o Slowhttptest -r 300 –l 400 –u http://192.168.0.101/ -x 20 (2)

Where: c is the total number of connections, -B is the type of attack, -i is the time between the connections, -t is the type of the response, -g -o indicate the parameters used to generate the charts, -r is the number of connections per second, -l is the target length of the text in a second, -u is the address of the victim and –x determines the maximum length of the bits.

- Syn Flood – takes advantage of TCP/IP protocol weaknesses. During the attack, a number of half-open connections with the server is maintained. Each of the connections can be maintained from 3 up to 4 minutes, depending on the used configuration. At the beginning, the client assigns a port for TCP/IP and sends SYN message to WWW server, requesting a connection. The resources are “booked” by the system, which responds by sending a SYN-ACK package to the encrypted IP of the client. During the test, it was necessary to generate a traffic like one during a Syn Flood attack. The authors used Scapy packet generator for that purpose (3).

```
IP= IP(dst="192.168.0.101")
IP= IP(src="192.168.0.111")
t=TCP()                                    (3)
t.sport=(RandNum(1024, 6565)
send((IP/t), loop=1)
```

Where: dst – target address for the attack, src – encrypted source address for the attack, t – TCP traffic variable and sport – setting pseudorandom port numbers. The last request makes the TCP requests being sent continuously [14].

4. WWW server defense mechanisms

Proper choice of the attack mechanisms made it possible to discover the weaknesses of the Apache server. Each of the implemented defence mechanisms is a free tool for protecting against the violations of safety protocols [4, 7-9, 11].

- mod_security module – a complex firewall for the web applications. Responsible for the monitoring and analysis of the HTTP traffic. Allows using the existing firewall rules and creating the new ones. The model also enables to block the access to the rest of the Apache server configuration files. The rules used while performing the analysis of the vulnerability of the WWW server filtered the traffic by: checking the number of the requests sent from one IP address, limiting the number of loggings-on to one per minute, checking the number of active connections for one IP address and checking the request paths. Every time any of the defined values is exceeded, the task of the module is to add the address of the potential attacker to the blacklist. After 5 minutes, the blocked address will be removed from the turn-on list.
- mod_qos module – introduces a mechanism reducing the speed of sending the fragments of the headers of the requests. Activating mod_qos module makes performing a Slow HTTP attack effectively impossible, as well as any other attacks using large bandwidth. Mod_qos module architecture makes it possible to add a new functionality in the form of a separate module, gathering information regarding the operation of the Apache server in real-time. After the installation of mod_status module, the access to the data can be gained through a browser, by providing the address of the server. Moreover, it is possible to generate a report including basic information on the number of the connected addresses or the maximum number of the addresses from where the connection request may be sent. Many other parameters are also displayed. Combining mod_qos and mod_status modules allows controlling the safety of the Apache

server more effectively. A detailed description of the parameters is given in Tab. 1.

Table 1. Mod_qos module setup parameters

Parameter	Description
QS_ClientEntries	Maximum number of clients
QS_ClientEvent RequestLimit	Maximum number of simultaneous requests for a single IP address
QS_SrvMaxConn PerIP	Maximum number of connections for a server address
MaxClients	Maximum number of active TCP connections
QS_SrvMaxConn Close	Maximum number of keep-alive connections. If the limit is exceeded, the connection is closed for every request.
QS_SrvMinData Rate	Minimum bandwidth: the number of bytes sent per second / the number of bytes received per second
QS_LimitRequestBody	Maximum size of the body of the request
LimitRequestFields	Maximum size of the header of the request

- mod_evasive module – module responsible for monitoring of the number of incoming HTTP connections. The architecture of this solution allows communication with ipchains, routers, and complex firewalls. Every client attempting to connect is checked for the number of the requests incoming for one website, as well as for the number of simultaneous requests for a single process or thread of the server. The module also blocks the attempts to establish a connection for the IP addresses included in the blacklist.

5. Assessment of the vulnerability of the Apache server

The main task of the server is to process the requests of the HTTP communication protocol. Web servers are used for websites, e-mail accounts, databases and many other web services [9], [11], [15]. A free tool, the Apache server is used by many companies. The server may operate in one of the two modes: MPM Prefork and MPM Worker. The main difference between the two is the manner of processing the request. The server working in MPM mode uses child processes to accomplish the task. Processing every incoming request is performed with a new child process. This kind of architecture ensures the safety of the rest of the requests processed. The main drawback of this method of request processing is that the resources of the server are limited. The second mode in which the Apache server can operate is MPM Worker. The server creates a sepa-

rate child thread for every request. This solution makes it possible to process a higher number of clients with smaller hardware resources [6], [13]. A properly designed DDoS attack is capable of making the server deny a service irrespective of the mode in which the Apache server has been operating.

Failure to ensure a proper level of securing the Apache server may result in the attacker's being able to use the server for a denial-of-service very soon after the attack is commenced. Three kinds of attack were used for the analysis. Each of them was to show a different security gap in the Apache server. The vulnerability tests of the Apache server proved that an unsecured server cannot filter out a dangerous action. The default WWW server configuration does not allow using any mechanisms of detecting DDoS attacks [6], [15]. Therefore, installing some protective tools is necessary to ensure safety in case of any attempts to violate the safety protocols. The vulnerability tests of the Apache server indicated that the server in its default configuration is vulnerable to all the used mechanisms of attack. During the test conducted with R.U.Dead. type traffic-generating tool, a denial of service occurred. A website activated on the server did not respond to a request by the user. In case of the rest of the other types attacks aimed at an unsecured server, the websites loaded longer than usual. Moreover, the server did not always respond to the requests sent by the user. Fig. 4 presents the results of conducted analysis.

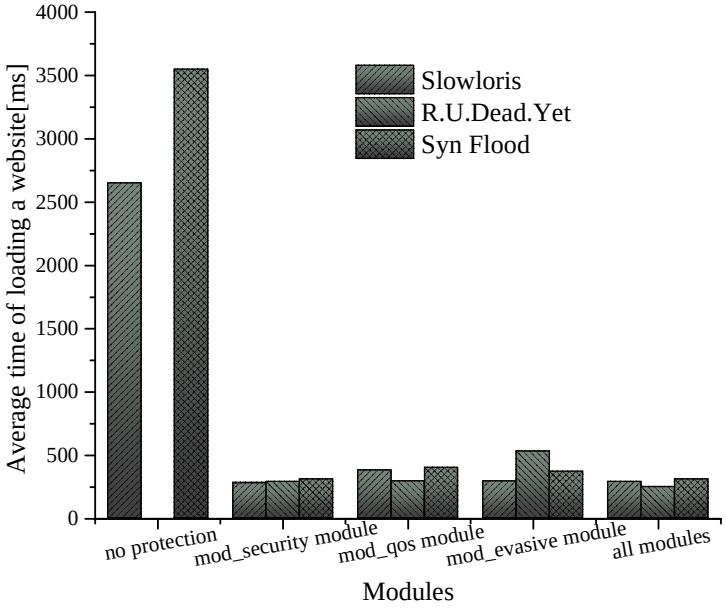


Fig. 4. Analysis of the time of loading pages during DDoS attack for different defence mechanisms

It should be remembered that the testing and analysis of Apache was carried out in a virtual test environment. To carry out the previously mentioned analysis has been used 2 virtual machines, on each of which had been installed Kali Linux. For a virtual machine performing the role of the web server has been set the RAM to 2GB of value, created a virtual SCSI drive size 40GB. In addition, the network card is set to bridge mode. The server at all time has at his disposal two core processor. Apache server the whole duration of the test was operated MPM Prefork which allowed for the safe close requests classified as a probable attack. Use MPM Prefork mode that caused the server can only handle 375 active connections at the same time. Apache also had set up parameters with values: Timeout 200 s, KeepAive On, MaxKeepAliveRequests 400, Max Clients 150.

Using proper mechanisms of protecting against DDoS attacks made WWW server resistant to some extent to the denial-of-service attacks. Unfortunately, the mechanisms implemented did not protect the server in 100%. Additional configurations have to be introduced in the configuration files of the Apache server in order to increase the protection of WWW server.

Summary

Performed vulnerability tests of the Apache server indicated that an unsecured WWW server is not equipped with any mechanisms limiting the effects a DDoS attack. During the stress tests, the server was incapable of executing any of the actions generated, being exceptionally vulnerable to HTTP Post, Get or Syn Flood attacks. Implementing only three protective mechanisms ensured proper operation of the server and the access to the services.

The analysis was not performed to indicate which of the chosen protective mechanisms is the best, but to show the difficulties regarding the protection against denial-of-service type of attacks.

References

[1] Web Server Survey - Web server developers: Market share of active sites. Available: https://www.netcraft.com/internet-data-mining/ [Access: 10.03.2017]

[2] W. Stallings: „Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji", Helion, Gliwice 2012.

[3] Akamai's [state of the internet] / security – Q4 2016 report. Available: https://www.stateoftheinternet.com/downloads/pdfs/2015-cloud-security-report-q3.pdf [Access: 15.03.2017]

[4] S.T. Zargar, J. Joshi, D. Tipper: "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE communications surveys & tutorials, vol. 15, no. 4, fourth quarter 2013.

[5] Ch. Douligeris, A. Mitrokotsa: “DDoS attacks and defense mechanisms a classification”, Department of Informatics University of Piraeus, Piraeus, Greece.

[6] M. Poongothai, M. Sathyakala: “Simulation and Analysis of DDoS Attacks”, International Conference on Emerging Trends in Science, Engineering and Technology, 2012.

[7] Security Labs: How to Protect Against Slow HTTP Attacks [Online]. Available: https://blog.qualys.com/securitylabs/2011/11/02/how-to-protect-against-slow-http-attacks [Access: 30.03.2017]

[8] cunetix: How To Mitigate Slow HTTP DoS Attacks in the Apache HTTP Server [Online]. Available: https://www.acunetix.com/blog/[Access: 30.03.2017]

[9] Apache Security: Denial of Service Attacks [Online]. Available: https://www.feistyduck.com/library/apache-security/online/apachesc-CHP-5.html [Access: 01.04.2017]

[10] Ataki Slow HTTP DoS (cz. 1.) – Slowloris, [Online]. Available: http://sekurak.pl/ataki-slow-http-dos-cz-1-slowloris/ [Access: 01.04.2017]

[11] Securing the Apache, Part 8: DoS & DDoS Attacks, [Online]. Available: http://opensourceforu.efytimes.com/2011/04/securing-apache-part-8-dos-ddos-attacks/ [Access: 10.04.2017]

[12] R.U.D.Y. (R-U-Dead-Yet): DDoS Attack Glossary [Online]. Available: https://www.incapsula.com/ddos/attack-glossary/rudy-r-u-dead-yet.html [Access: 10.04.2017]

[13] Understanding the Apache 2 MPM (worker vs prefork) [Online]. Available: https://www.garron.me/en/blog/apache2-mpm-worker-prefork-php.html [Access: 06.04.2017]

[14] K. Geetha: SYN flooding attack — “Identification and analysis”, Information Communication and Embedded Systems (ICICES), 2014 International Conference on, 2014.

[15] N. Shipilov, K. Borisenko, A. Shorov: “Simulation of DDoS-attacks and protection mechanisms against them”, Young Researchers in Electrical and Electronic Engineering Conference 2015 IEEE NW Russia, 2015.

[16] J. Brynielsson: “Detectability of low-rate HTTP server DoS attacks using spectral analysis”, International Conference on Advances in Social Networks Analysis and Mining, 2015.

BADANIE PODATNOŚCI SERWERA APACHE NA ATAKI ODMOWY USŁUGI

Streszczenie

W artykule przedstawiono analizę podatności serwera Apache w odniesieniu do popularnych ataków DDoS. Praca rozpoczyna się od przedstawienia statystycznego ujęcia problemu, jakim są ataki odmowy usług. Ponadto przedstawiony został problem rozpowszechniania metod wykorzystywanych do przeprowadzania ataków DDoS. Autorzy, bazując na systemach wirtualnych opracowali środowisko testowe, na którym zrealizowano badania podatności wybranych systemów WWW. Publikację kończą propozycje działań mających na celu zaimplementowanie efektywnych

metod obrony przed atakami odmowy usługi. Artykuł jest adresowany do osób zajmujących się bezpieczeństwem systemów webowych.

Słowa kluczowe: bezpieczeństwo, Apache, ataki DDoS

DOI: 10.7862/re.2017.6

Tekst złożono w redakcji: maj 2017
Przyjęto do druku: czerwiec 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. 4,10. Ark. druk. 5,0. Papier offset. 80g B1.
Oddano do druku w lipcu 2017 r. Wydrukowano w lipcu 2017 r.
Drukarnia Oficyny Wydawniczej, al. Powstańców Warszawy 12, 35-959 Rzeszów
Zam. nr 85/17