

## BADANIA KOMUNIKACJI POMIĘDZY URZĄDZENIAMI AUTOMATYKI ZABEZPIECZENIOWEJ ZGODNIE ZE STANDARDEM IEC 61850

Tomasz BEDNARCZYK<sup>1</sup>, Jakub BARTZ<sup>2</sup>, Kacper CHYŁA<sup>2</sup>, Michał GAŁĄZKA<sup>2</sup>, Damian TORUŃCZAK<sup>2</sup>, Filip PANKOWIAK<sup>2</sup>, Mirosław WŁAS<sup>2</sup>, Kamil ZAWACKI<sup>2</sup>

1. OMICRON Energy Solutions Polska Sp. z o.o., ul. Kosynierów 44, 41-219 Sosnowiec  
tel: +48 32 621 1028, kom: +48 882 803 661, e-mail: tomasz.bednarczyk@omiconenergy.com
2. Politechnika Gdańska, Wydział Elektrotechniki i Automatyki, ul. Narutowicza 11/12, 80-233 Gdańsk  
tel: +48 58 347 23 37 fax: +48 58 341 08 80 e-mail: miroslaw.wlas@pg.edu.pl

**Streszczenie:** W artykule opisano badania modelu sieci SN wyposażonego w przekaźniki REF615 Serii Relion firmy ABB oraz tester zabezpieczeń CMC 256-6 firmy OMICRON. Na stanowisku badawczym na Wydziale Elektrotechniki i Automatyki Politechniki Gdańskiej przeprowadzono badania czasu przesyłania komunikatów GOOSE oraz retransmisji danych za pomocą testera zabezpieczeń CMC 256-6. Wyniki potwierdziły niezawodność oraz powtarzalność czasów przesyłu danych.

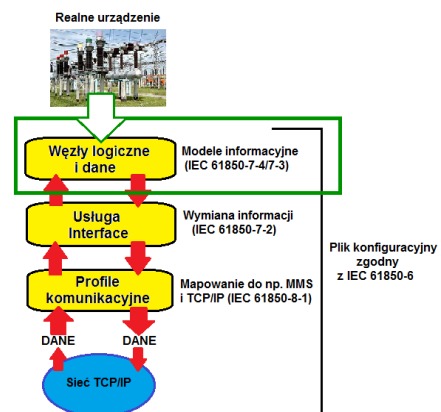
**Słowa kluczowe:** przekaźniki zabezpieczeniowe, sieci inteligentne, IEC 61850, komunikaty GOOSE.

### 1. WPROWADZENIE

W ostatnich latach obserwujemy w przemyśle, ale także w energetyce, bardzo dynamiczny rozwój technologii komunikacyjnych opartych na sieci Ethernet. Pociąga to za sobą konieczność opracowania rozwiązań gwarantujących niezawodną wymianę danych pomiędzy urządzeniami na stacji elektroenergetycznej, ale także w sieci SN, niezależnie od ich producenta i wykorzystanego sposobu komunikacji [1]. Rozwiązania te ujęto w standardzie IEC 61850 [2], stawiając przed producentami i projektantami nowoczesnych systemów sterowania i nadzoru wyzwanie zapewnienia zgodności istniejących SSiN (System Sterowania i Nadzoru) z normą [3]. Podejmuje się próby przesyłania sygnału także z wykorzystaniem radia [4]. Niniejszy artykuł przedstawia możliwości przystosowania przekaźnika zabezpieczeniowego do pracy jako inteligentnego urządzenia IED na stacji elektroenergetycznej i w sieci SN. Celem pracy jest nawiązanie komunikacji między urządzeniami IED, zgodnej ze standardem IEC 61850, oraz przeprowadzanie badań mających na celu sprawdzenie zgodności utworzonej komunikacji ze standardem IEC 61850, m.in. zbadanie czasu przesyłania komunikatów GOOSE oraz zbadanie poprawności retransmisji tych komunikatów. Zdecydowano się na skomunikowanie urządzeń za pośrednictwem transmisji przewodowej. Takie rozwiązanie ma na celu sprawdzenie czasu przesyłania komunikatów GOOSE drogą przewodową i porównanie tych czasów z pomiarami wykonanymi podczas przesyłania drogą radiową. Pomiary czasów przesyłania komunikatów GOOSE drogą radiową zostały opisane w pracy [4]. Praca ta ma na celu wykazać, że zastosowanie transmisji przewodowej nie tylko w obrębie stacji, ale także

na obszarze całego GPZ, daje ogromne możliwości szybkiej komunikacji i ograniczenia przerw w dostawie energii elektrycznej.

Standard IEC 61850 definiuje mechanizm wymiany informacji, w którym można wydzielić cztery podstawowe aspekty przedstawione na rys. 1: modele informacji, interfejsy serwisowy, mapowanie do protokołów oraz konfigurację systemu. Powyższy mechanizm wymiany informacji polega na zdefiniowanych modelach danych. IEC 61850 korzysta z koncepcji wirtualizacji w tworzeniu modelu danych. Ten model danych dostarcza systemowi automatyki stacyjnej obraz fizycznego świata.



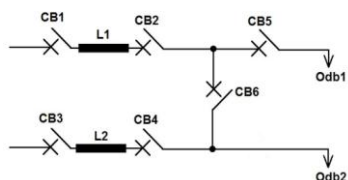
Rys. 1. Fundamentalne aspekty standardu IEC 61850

### 2. STANOWISKO BADAWCZE

Stanowisko składa się z sześciu przekaźników zabezpieczeniowych REF615 firmy ABB [5], testera zabezpieczeń CMC 256-6 firmy Omicron oraz siedmiu kompaktowych wyłączników niskonapięciowych XT2N, reprezentujących wyłączniki średniego napięcia (rys. 2). Urządzenia tworzą jedną sieć, połączono je przewodem Ethernet kat. 5e za pośrednictwem switcha AFS660 firmy ABB. W ramach przygotowania badań utworzono komunikację między urządzeniami zgodną ze standardem IEC 61850. Zamodelowano warstwę komunikacyjną na przykładowym modelu sieci średniego napięcia (rys. 3) i na jej podstawie przeprowadzono badania.



Rys. 2. Widok stanowiska badawczego



Rys. 3. Uproszczony schemat zamodelowanej sieci SN

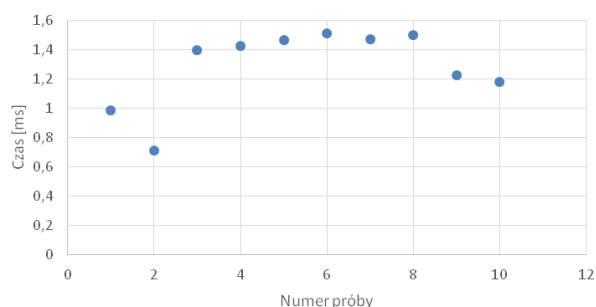
### 3. BADANIA

#### 3.1. Badania opóźnień przesyłania informacji GOOSE

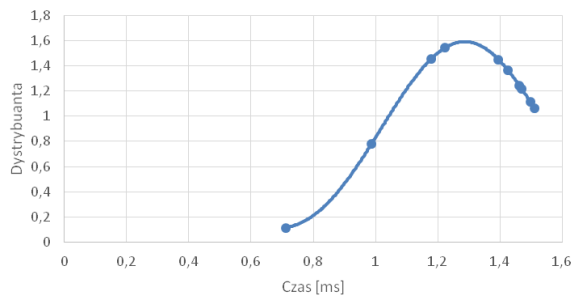
Na zasymulowanym modelu sieci 15kV przekaźniki zabezpieczeniowe przesyłają między sobą dwie podstawowe informacje, jakimi są: zadziałanie urządzenia nadrzędnego TRPPTRC1 (trip) oraz pozycja wyłącznika CBXCBR1. Informacja typu trip jest najczęściej badanym komunikatem i zgodnie z wymogami normy [2] zaliczana jest do szybkich wiadomości typu 1A (ang. *Type 1 – Fast messages „Protection”*).

Zastosowano dwa sposoby pomiarów czasu opóźnienia informacji trip. Pierwszym z nich było porównanie stempli czasowych, wystawianych przez przekaźniki w chwili wysłania i odebrania wiadomości. Drugim sposobem był pomiar czasu dla dwóch wiadomości przy użyciu oprogramowania, które zaczynało mierzyć czas w chwili wysłania wiadomości oraz kończyło pomiar w chwili odebrania wiadomości zwrotnej. Oba sposoby pomiarów dały zbliżone wyniki, co można uznać za potwierdzenie słuszności tych wyników. W ramach pomiarów przeprowadzono dwa eksperymenty. Pierwszym z nich był pomiar czasu na modelu sieci średniego napięcia. W ramach stworzonej komunikacji na modelu badano czas przesyłania wiadomości GOOSE zawierającej informację trip, przesyłaną z przekaźnika CB1 do przekaźnika CB2. Przekaźnik CB1 był wyzwalany przez zadziałanie funkcji nadprądowej (wymuszenie prądowe zapewnione przez tester zabezpieczeń CMC 256-6 firmy OMICRON powodowało jej uruchomienie), a następnie przesyłał informację trip do przekaźnika CB2. Dla tego eksperymentu zastosowano metodę pomiarową wykorzystującą stemple czasowe. Aby tak podejście do badań było możliwe, przed ich rozpoczęciem konieczna była synchronizacja wszystkich urządzeń z zewnętrznym wzorcem czasu.

Synchronizacji dokonano za pośrednictwem protokołu SNTP. Wzorcem czasu dla przekaźników był komputer (z dostępem do Internetu), który z kolei był synchronizowany z zegarem GPS. Taki sposób synchronizacji czasu również został uwarunkowany technicznymi możliwościami przekaźników zabezpieczeniowych. W trakcie badań analizowano ramki ethernetowe, zawierające wysłane komunikaty GOOSE (za pomocą programu Wireshark), oraz analizowano rejestrator zakłóceń (za pomocą programu Wavewin ABB), rejestrujący odebrane GOOSE. Porównanie stempla czasu odbioru i wysłania wiadomości pozwoliło na poznanie czasu przesłania komunikatu GOOSE. Przeprowadzono 10 pomiarów, które obrazowo przedstawiono na rysunku 4. Na rysunku 5 zaprezentowano rozkład normalny uzyskanych wyników.

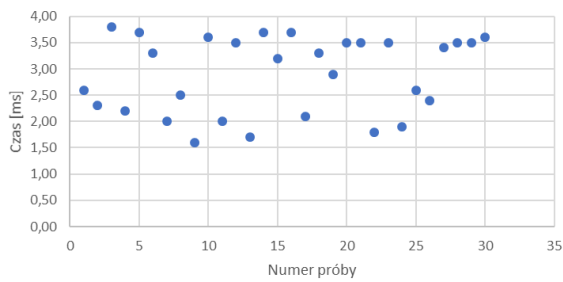


Rys. 4. Czasy GOOSE dla modelu sieci w zależności od numeru próby

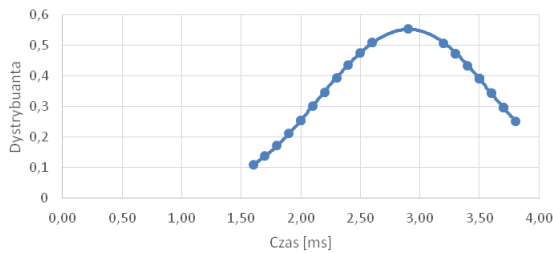


Rys. 5. Rozkład normalny wyników dla badań na modelu sieci

Drugim eksperymentem była symulacja przekaźnika zabezpieczeniowego REF615 za pomocą testera zabezpieczeń CMC 256-6 firmy OMICRON. Symulowany przekaźnik poprzez zewnętrzne wymuszenie użytkownika wysyłał komunikat GOOSE typu trip do sześciu przekaźników zabezpieczeniowych, powodując otwarcie ich wyłączników. Po otwarciu wyłącznika przekaźnik zabezpieczeniowy wysyłał informację zwrotną o wyzwoleniu wyłącznika (również typu trip) do testera CMC 256-6. Tester zabezpieczeń wysyłał i odbierał komunikaty GOOSE. Przy użyciu oprogramowania State Sequencer mierzono czas od momentu zasymulowania komunikatu GOOSE typu trip, wysłanego do przekaźników, do chwili odebrania subskrybowanej wiadomości od przekaźników o wyzwoleniu. Warto podkreślić, że użyty w badaniu tester zabezpieczeń CMC 256-6 daje możliwość symulacji przekaźników różnych firm, poprzez zaimplementowanie do niego odpowiedniego pliku SCL. W trakcie badań użyto pliku SCL opisującego przekaźnik REF615. Przeprowadzono 30 pomiarów, a wyniki pokazano graficznie na rysunku 6 oraz przedstawiono rozkład normalny wyników na rysunku 7. Wyniki dotyczą przekaźnika CB1, dla pozostałych przekaźników, wyniki są zbliżone.



Rys. 6. Czasy round-trip dla przełącznika CB1



Rys. 7. Rozkład normalny czasów round-trip dla przełącznika CB1

Uzyskane wyniki przesyłania jednego komunikatu trip są zadowalające. Należy jednak pamiętać, że uzyskany czas 1,5 ms dotyczy przełączników jednej firmy – ABB. Sytuacja może wyglądać zdecydowanie gorzej w pomiarach czasu komunikatów wysyłanych przez przełączniki różnych firm. Wszystkie przesyłane komunikaty odnoszą się do zadziałania funkcji zabezpieczeniowych oraz pozycji wyłączników, każdy z komunikatów GOOSE został przesłany wraz z atrybutami odpowiedzialnymi za jakość. We wszystkich przełącznikach zabezpieczeniowych pracujących w stworzonym układzie został dodany blok funkcjonalny SCHLCC1. Blok ten jest wykorzystywany w celu nadzoru komunikacji Ethernet. Jeżeli komunikacja została przerwana (co może nastąpić z różnych powodów, np. na skutek przerwania przewodów wykorzystywanych do komunikacji), natychmiast informacja ta została wyświetlona na przełącznikach zabezpieczeniowych REF615 użytych w układzie. Wyjście CH1LIV wyżej wymienionego bloku jest ustawiane w stan logiczny „prawda”, jeżeli przełącznik zabezpieczeniowy otrzymuje ramki Ethernet. Dodatkowo ze wszystkich bloków funkcjonalnych, służących do łączenia danych wejściowych z aplikacją, w celu sprawdzenia poprawności przesyłanych danych zostało wyprowadzone wyjście VALID, które sprawdza, czy komunikacja dla konkretnej przesyłanej wiadomości działa poprawnie. Wszystkie wyjścia VALID zostały logicznie połączone w programie PCM600 i wyprowadzone na dziewiątą programowalną diodę każdego z przełączników zabezpieczeniowych użytych na stanowisku, w celu sygnalizacji poprawności działania komunikacji. Poniżej została przedstawiona przykładowa macierz komunikatów GOOSE, jakie są przesyłane w układzie. W tym przypadku jest to macierz sygnałów (rys. 8), jakie odbiera trzeci przełącznik zabezpieczeniowy. Przedstawia ona realizację przesyłania informacji o pozycji wyłączników pierwszego, drugiego, czwartego, piątego oraz szóstego użytych w układzie. Podobna funkcjonalność została stworzona w pozostałych przełącznikach zabezpieczeniowych, dodatkowo w niektórych przesyłane są również informacje dotyczące zadziałania funkcji zabezpieczeniowych, które były niezbędne, aby przeprowadzić rekonfigurację modelu sieci.

	IED, Logical Device	REF615_C B1, CTRL	REF615_C B2, CTRL	REF615_C B4, CTRL	REF615_C B5, CTRL	REF615_C B6, CTRL
		CBXCBR1 Pos stVal	CBXCBR1 Pos stVal	CBXCBR1 Pos stVal	CBXCBR1 Pos stVal	CBXCBR1 Pos stVal
- Wyl_1_pozycja:GOOSERCV_INTL:0	IN	X				
- Wyl_2_pozycja:GOOSERCV_INTL:1	IN		X			
- Wyl_4_pozycja:GOOSERCV_INTL:2	IN			X		
- Wyl_5_pozycja:GOOSERCV_INTL:3	IN				X	
- Wyl_6_pozycja:GOOSERCV_INTL:4	IN					X

Rys. 8. Macierz komunikatów otrzymywanych przez CB3

### 3.2. Badania retransmisji przesyłania informacji GOOSE

W celu przeprowadzenia badania w programie PCM600 zostały zdefiniowane kolejno trzy niezależne komunikaty GOOSE, każdy z komunikatów zawierał pojedynczy atrybut danych odnoszący się do zadziałania funkcji zabezpieczeniowych 3-fazowych bezkierunkowych zabezpieczeń nadprądowych. Odpowiednio :

- GOOSE\_1: funkcja zabezpieczeniowa PHLPTOC 3-fazowe bezkierunkowe zabezpieczenie nadprądowe, stopień zabezpieczeniowy niski,
- GOOSE\_2: funkcja zabezpieczeniowa PHHPTOC 3-fazowe bezkierunkowe zabezpieczenie nadprądowe, stopień zabezpieczeniowy wysoki,
- GOOSE\_3: funkcja zabezpieczeniowa PHIPTOC 3-fazowe bezkierunkowe zabezpieczenie nadprądowe, stopień bezzwłoczny.

Każdy z wyżej wymienionych komunikatów został przesłany w 20 próbach. W celu wymuszenia zadziałania funkcji zabezpieczeniowych i w konsekwencji wymuszenia komunikatu GOOSE, mówiącego o zadziałaniu tych funkcji, został wykorzystany tester zabezpieczeń CMC 256-6 firmy Omicron. Wyjścia prądowe CMC 256-6 zostały połączone z wejściami pomiarowymi przełącznika zabezpieczeniowego REF615. W oprogramowaniu QuickCMC została skonfigurowana wartość prądu na tyle duża, aby pobudzić zadziałanie funkcji zabezpieczeniowej. Przesłany komunikat GOOSE oraz jego retransmisja została zbadana dzięki oprogramowaniu do testera zabezpieczeń o nazwie IEDScout, w którym zostały zmierzone czasy pierwszych sześciu retransmisji przesyłanej wiadomości GOOSE (tab. 1). Poniżej został przedstawiony opis oznaczeń użytych w tabelach zawierających wyniki, jakie otrzymano po przeliczeniu otrzymanych pomiarów czasu:

- **nr ret.** – numer retransmisji komunikatu GOOSE,
- **t<sub>min</sub>** – minimalny czas retransmisji komunikatu GOOSE liczony od przesłania nowego komunikatu GOOSE [ms],
- **t<sub>max</sub>** – maksymalny czas retransmisji komunikatu GOOSE liczony od przesłania nowego komunikatu GOOSE [ms],
- **t<sub>sr</sub>** – średni czas retransmisji komunikatu GOOSE liczony od przesłania nowego komunikatu GOOSE [ms],
- **t'<sub>min</sub>** – minimalny czas retransmisji komunikatu GOOSE liczony od poprzedniej retransmisji komunikatu [ms],
- **t'<sub>max</sub>** – maksymalny czas retransmisji komunikatu GOOSE liczony od poprzedniej retransmisji [ms],
- **t'<sub>sr</sub>** – średni czas retransmisji komunikatu GOOSE liczony od poprzedniej retransmisji komunikatu [ms].

Tablica 1. Wyniki badań uzyskane z 20 transmisji funkcji zabezpieczeniowej PHLPTOC

Nr ret.	$t_{\min}$ [ms]	$t_{\max}$ [ms]	$t_{\text{sr}}$ [ms]	$t'_{\min}$ [ms]	$t'_{\max}$ [ms]	$t'_{\text{sr}}$ [ms]
1.	0,106	0,209	0,160	0,106	0,209	0,160
2.	2,399	5,048	2,586	2,235	4,914	2,426
3.	5,018	7,563	5,181	2,515	2,639	2,595
4.	105,06	107,59	107,22	100,03	102,44	102,04
5.	10005,6	10010,3	10008,4	9900,3	9902,9	9901,2
6.	19906,3	19912,9	19909,2	9900,2	9902,6	9900,8

Niezależnie od tego, jaka funkcja zabezpieczeniowa jest przesyłana, wyniki pomiarów są na zbliżonym poziomie. Wniosek płynący z tej zależności wskazuje, że niezależnie od stopnia zabezpieczeniowego danej funkcji, a co za tym idzie niezależnie od prędkości działania danej funkcji, retransmisja komunikatów GOOSE jest realizowana w ten sam sposób. Innymi słowy, retransmisja komunikatów odbywa się w bardzo zbliżonych odstępach czasowych niezależnie od prędkości działania funkcji zabezpieczeniowych.

Z otrzymanych wyników badań wynika, że pierwsza retransmisja komunikatu GOOSE odbywa się w czasie nieprzekraczającym  $t_{\max} = 0,215 \text{ ms}$ . Czas ten jest bardzo krótki, może to świadczyć o tym, że pierwszy komunikat retransmisyjny jest nadawany od razu po przesłaniu komunikatu GOOSE, a czas opóźnienia wynika tylko z ograniczeń możliwości reakcji przekaźników zabezpieczeniowych użytych podczas badania. Kolejnym faktem potwierdzającym tę tezę jest przebadany czas przesyłu komunikatu GOOSE, liczony od momentu wysłania do momentu odebrania: jest on kilkukrotnie dłuższy od czasu pierwszej retransmisji. Wyżej przytoczona analiza porównująca czas pierwszej retransmisji z czasem przejścia komunikatu GOOSE między przekaźnikami zabezpieczeniowymi potwierdza, że komunikaty GOOSE w standardzie IEC 61850 są przesyłane bez potwierdzenia odebrania poprzedniego komunikatu. Analizując czasy średnie pomiędzy retransmisjami, warto zauważyć, że pierwsza retransmisja odbywa się najszybciej, gdyż jest ona najważniejsza. Jeżeli z jakichś powodów komunikat GOOSE nie dociera do przekaźnika zabezpieczeniowego, pierwsza retransmisja odbywa się w tak krótkim czasie, że nie ma to wpływu na działanie układu sieci SN. Czas drugiej oraz trzeciej retransmisji ustala się na poziomie oscylującym w okolicach  $2,5 \text{ ms}$ . Czwarta retransmisja zostaje przesyłana po ok.  $100 \text{ ms}$  od trzeciej retransmisji komunikatu GOOSE. Natomiast piąta retransmisja i kolejne ustalają się na poziomie nie przekraczającym  $10 \text{ s}$ . Retransmisja odbywa się w sposób uporządkowany. Czasy minimalne oraz maksymalne przesyłanych retransmisji komunikatu GOOSE nie odbiegają znacząco od siebie, co może świadczyć o poprawności działania komunikacji na stanowisku badawczym.

## 4. WNIOSKI KOŃCOWE

W artykule przedstawiono badania opóźnień i retransmisji komunikatów GOOSE, które są niezbędne do zapewnienia odpowiedniego poziomu bezpieczeństwa w rzeczywistych układach sterujących siecią elektroenergetyczną. Ponieważ komunikaty GOOSE są wysyłane bez odpytania urządzenia przesyłającego i bez konieczności potwierdzenia przyjęcia wiadomości przez urządzenie odbierające, komunikacja jest bardzo szybka, zaś czasy opóźnień wynoszą średnio  $1,5 \text{ ms}$ .

Przyszłością systemu elektroenergetycznego jest budowanie systemów komunikacji opartych na szybkiej komunikacji przewodowej lub radiowej i wdrożenie systemów zarządzania dystrybucją DMS. Istnieje kilka powodów takiego stanu rzeczy: dynamiczny rozwój źródeł energii odnawialnej i rozproszonej oraz powstanie wirtualnych elektrowni (VPP), klastrów energetycznych, magazynów energii i infrastruktury dla pojazdów elektrycznych, konieczność rekonfiguracji sieci ze względu na optymalizację poziomu napięć, rozplywu mocy biernej, konieczność optymalizacji układu sieci w celu równoważenia obciążenia i generacji energii, zarządzanie rozplywami, lokalizacja zwarć, izolacja i przywrócenie zasilania, konieczność zarządzania wahaniami napięcia oraz monitorowanie jakości energii. Dlatego też konieczne jest rozszerzenie liczby urządzeń działających w systemie dystrybucyjnym w całej sieci SN. Konieczne jest zainstalowanie rozłączników (sekcjonalizery) i wylączników (reklozery) wyposażonych w przekaźniki zabezpieczeniowe, które umożliwiają przeprowadzenie szybkich rekonfiguracji sieci i zapewniają adaptację zabezpieczeń do warunków panujących w sieci.

## 5. BIBLIOGRAFIA

1. Krakowski M.: Implementacja standardu IEC 61850 w zabezpieczeniach i rozdzielnicach JM-TRONIK, Urządzenia dla Energetyki 2013, nr 4.
2. IEC 61850, Edition 2.0: Communication networks and systems for power utility automation – Part 1 – 10.
3. Babś A. i in.: Rozbudowa urządzeń automatyki elektroenergetycznej w celu uzyskania zgodności z normą IEC 61850 [online], <http://www.i.en.gda.pl> (dostęp: 12.09.2018)
4. Chang J. i in., Application of a multifunctional distance protective IED in a 15KV distribution network, 66<sup>th</sup> Annual Conference for Protective Relay Engineers, College Station, TX, USA, 2013, s. 150–171.
5. Zabezpieczenie i sterowanie pola REF615 – Zabezpieczenie i sterowanie pól liniowych [online], <https://new.abb.com/medium-voltage/pl/produkty-i-rozwiazania-automatyki-sieciowej/przekazniki-numeryczne/zabezpieczenie-i-sterowanie-pol-liniowych/relion/ref615> (dostęp: 12.09.2018).

## RESEARCH ON COMMUNICATION BETWEEN IED IN ACCORDANCE WITH THE IEC 61850 STANDARD

The article describes the research of the SN network model equipped with REF615 relays of the ABB Relion Series and the CMC 256-6 security tester of the OMICRON company. The time of GOOSE messaging and data retransmission was tested using the CMC256-6 security tester. The results confirmed the reliability and repeatability of data transfer times.

**Keywords:** protection relay, smart grid, IEC 61850, GOOSE.