



POLITECHNIKA
LUBELSKA
WYDZIAŁ ELEKTROTECHNIKI
I INFORMATYKI

Laboratorium: Teletechnika w elektroenergetyce

Monitorowanie działania urządzeń IED

Robert Jędrychowski

Data modyfikacji: 13 grudnia 2022

Cel laboratorium:

Celem ćwiczenia jest zapoznanie się z narzędziami informatycznymi pozwalającymi na monitorowanie poprawności konfiguracji oraz wymiany danych pomiędzy urządzeniami pracującymi w standardzie IEC 61850.

Zakres tematyczny zajęć:

- ocena struktury plików konfiguracyjnych IEC 61850,
- monitorowanie obiektów danych, DataSet-ów i raportów,
- Symulacja pracy urządzeń IED.
- Monitorowanie szybkich komunikatów GOOSE.

Pytania kontrolne:

1. Z jakich elementów budujemy opis urządzenia IED?
2. Rola elementów DataSet?
3. W jaki sposób możemy kontrolować komunikację pomiędzy urządzeniami IED?
4. Jak możemy symulować działanie urządzeń IED?
5. W jaki sposób kontrolujemy ruch komunikatów GOOSE?

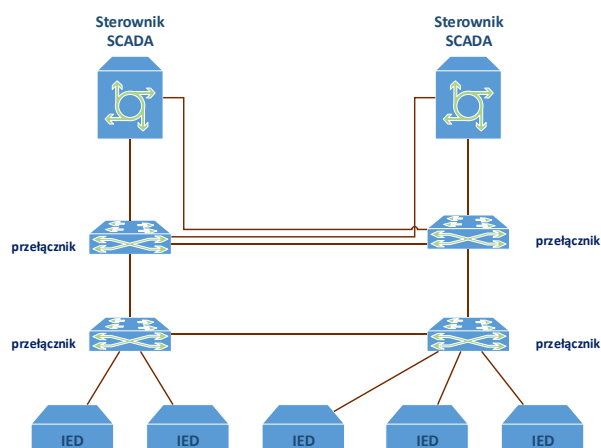
1 ZAPOZNANIE Z WYMOGAMI STANDARDU IEC 61850

Współczesne standardy komunikacji pomiędzy urządzeniami elektroenergetycznej automatyki zabezpieczeniowej (EAZ), urządzeniami telemechaniki oraz elementami lokalnych systemów sterowania i nadzoru (SSiN) wymuszają stosowanie komunikacji wykorzystującej szybki Ethernet dla sieci lokalnych. Wprowadzenie sieci LAN do nowych obiektów elektroenergetycznych odbywa się stopniowo, wraz z rozwojem nowych protokołów komunikacyjnych. Przyczyniły się do tego: wzrost szybkości działania sieci, zastosowanie nowych rozwiązań zwiększających bezpieczeństwo pracy sieci oraz porządkujących wymianę danych pomiędzy urządzeniami.

Nowe wymagania techniczne zostały zdefiniowane w standardzie IEC 61850, a następnie wprowadzone i dokładnie opisane w instrukcjach ruchu operatora sieci przesyłowej oraz operatorów sieci dystrybucyjnej. Stanowią one podstawę do projektowania i realizacji nowych stacji elektroenergetycznych oraz modernizowania już istniejących.

Wymogi stawiane sieci komunikacyjnej rozpatrywać można dla trzech warstw: sprzętowej, konfiguracyjnej oraz funkcjonalnej. Aby w pełni ocenić poprawność konfiguracji, a następnie działania sieci komunikacyjnych potrzebne są narzędzia pozwalające na testowanie zarówno pracy sieci jak i poszczególnych urządzeń do niej przyłączonych. Potrzebna jest również wiedza inżynierska pozwalająca ocenić poprawność działania sieci, urządzeń sieciowych, urządzeń telemechaniki oraz EAZ. Tworzą one wspólne środowisko automatyki stacji decydując o poprawnym realizowaniu wszystkich zadań.

Standard IEC 61850 definiując wymagania, co do formatu danych oraz szybkości ich przekazywania, precyzuje również sposób budowy sieci komunikacyjnej oraz technologie, które powinny być w niej stosowane.



Rys. 1.1 Uproszczony schemat sieci światłowodowej łączącej urządzenia EAZ i telemekhaniki

Podstawę fizyczną sieci komunikacyjnej stanowi technologia szybkiego Ethernetu oparta na przełącznikach sieciowych. Ze względu na specyfikę stacji elektroenergetycznych przyjmuje się, że szkielet sieci tworzą przełączniki połączone w pierścień łącami światłowodowymi. Dla pojedynczych urządzeń możliwe jest również stosowanie połączeń miedzianych. Do portów poszczególnych przełączników dołączone są urządzenia IED wymieniające dane między sobą. Taki układ połączeń gwarantuje ich redundancję przy jednoczesnym zachowaniu wymogów związanych z logicznym przepływem danych w postaci drzewa. Aby spełnić wymagania opisane dla PICOM sieć komunikująca musi spełniać kilka podstawowych kryteriów, do których należą:

- praca z szybkością 100 Mb/s lub wyższą w trybie full duplex,
- szybka rekonfiguracja układu,
- brak pętli logicznych i eliminacja sztormów rozgłoszeniowych,
- synchronizacja czasu poprzez przełączniki i sieć z wykorzystaniem protokołu SNTP lub innych protokołów specjalistycznych,
- możliwość tworzenia sieci wirtualnych,
- określenie priorytetów dla poszczególnych rodzajów komunikacji,
- możliwość stosowania również starszych protokołów komunikacyjnych np. DNP3 dla urządzeń niespełniających wymagań IED.

Zależnie od rodzaju informacji przesyłanych pomiędzy urządzeniami IED stosowane są trzy tryby transmisji danych: unicast, multicast i broadcast.

PICOM opisuje wymagania jakościowe stawiane procesowi przekazywania informacji pomiędzy poszczególnymi LN tworzącymi funkcje logiczne. Wymagania te dotyczą czasu i opóźnień w przesyłaniu informacji, integralności danych oraz sposobu obliczania wydajności komunikacji.

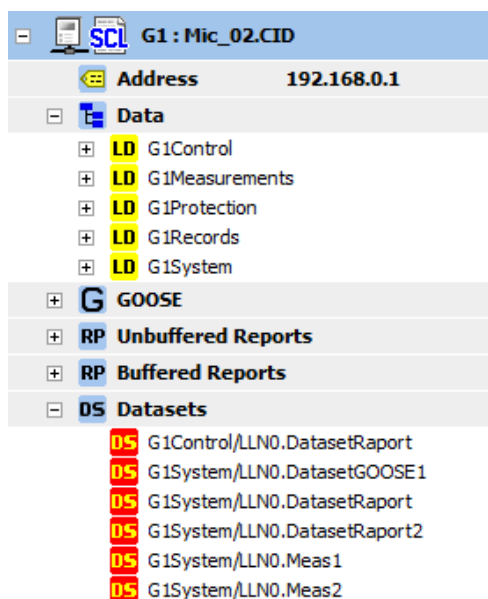
Określenie czasu zdarzenia zależy od jego charakteru. Jeśli zdarzenie jest generowane w wyniku obliczeń, alokacja (znakowanie) czasu powinna nastąpić w obrębie rozdzielczości zegara. Jeżeli zdarzenie jest wynikiem zmiany wejścia binarnego należy uwzględnić migotanie styku. Dla zdarzeń określonych jako zmiana wejścia analogowego uwzględniamy proces filtrowania sygnału. Całkowity czas transferu komunikatu liczy się od chwili, kiedy nadawca umieszcza zawartość danych na górze stosu transmisji, aż do chwili, kiedy odbiorca odzyskuje dane ze stosu transmisji.

Wymagania zawarte w PICOM określone zostały w dwóch grupach klasy wydajności. Pierwsza dotyczy sterowania i zabezpieczeń, są to klasy P1 – P3. Druga przewidziana została dla pomiarów i jakości energii, klasy M1 – M3. Wyszczególniono siedem typów komunikatów

różniących się czasem, który może wynosić od 3 ms dla szybkiego komunikatu P3 do nawet 1000 ms dla transferu plików lub bloków danych.

Sieć zbudowana według takich założeń będzie również spełniać wymogi stawiane dla starszych rozwiązań takich jak IEC 60870 czy DNP3.

Język konfiguracji opisany w części IEC 61850 – 6 stanowi istotny element modelowania systemu, co pozwala na precyzyjne definiowanie wszystkich elementów SAS. Do konfiguracji wykorzystano rozszerzalny język znaczników XML, a stworzony język określa się, jako język konfiguracji systemu (SCL). Głównym celem tego formatu wymiany jest zapewnienie możliwości opisu systemu stacji oraz stworzenie narzędzi inżynierii IED zgodnych dla systemów różnych producentów. Języku SCL zawiera informacje związane z opisem komunikacji pomiędzy IED, konfiguracji parametrów IED oraz konfiguracji SAS. Model systemu i komunikacji IED w SCL uwzględnia wymagania zdefiniowane w IEC 61850-5 i IEC 61850-7-x.



Rys. 1.2 Sposób grupowania danych dla zabezpieczenia generatora

W drugiej wersji dokumentu IEC 61850 – 6 opisane zostało sześć różnych typów plików wykorzystywanych w procesie konfiguracji, pliki te różnią się przeznaczeniem oraz szczegółowością zawartych w nich informacji. Zawartość języka SCL w pliku opisującym stację można określić w kilku charakterystycznych punktach:

1. Część opisująca podstawową strukturę systemu opisującą urządzenia i sposób ich podłączenia.
2. Część komunikacji: opisuje jak dane są grupowane do wysłania, co powoduje ich wysyłanie i jakie dane są potrzebne z do pobrania z innych IED.
3. Część prezentująca skonkretyzowany typ dla LN; opcjonalne dane i usługi, dla których ustawiono parametry.
4. Ostatnią część stanowią relacje pomiędzy LN.

Poprawność komunikacji pomiędzy poszczególnymi IED zależy również od prawidłowo zdefiniowanych relacji w pliku konfiguracyjnym SAS.

W standardzie szczegółowo opisane zostały różne rodzaje informacji wymienianych pomiędzy urządzeniami. Przekazywane mogą być dane o różnej strukturze i znaczeniu, należą do nich:

- zmienne wartości próbkowane z CTs (przekładnik prądowy) i VTs (przekładnik napięciowy),
- szybka wymiana I/O, dane zabezpieczeń i sterowanie,
- sygnały sterujące,
- sygnały regulacji,
- zarządzanie i konfiguracja,
- monitorowanie i nadzór,
- retransmisja danych do centrum,
- synchronizacja czasu.

```

<Communication>
  <SubNetwork name="EOiR" type="8-MMS">
    <ConnectedAP iedName="G1" apName="AP1">
      <Address>
        <P type="IP">192.168.67.20</P>
        <P type="IP-SUBNET">255.255.255.128</P>
        <P type="IP-GATEWAY">192.168.67.1</P>
        <P type="OSI-PSEL">00000001</P>
        <P type="OSI-SSEL">0001</P>
        <P type="OSI-TSEL">0001</P>
      </Address>
      <GSE ldInst="System" cbName="gcb01">
        <Address>
          <P type="MAC-Address">01-0C-CD-01-AC-E0</P>
          <P type="APPID">0001</P>
          <P type="VLAN-ID">008</P>
          <P type="VLAN-PRIORITY">4</P>
        </Address>
        <MinTime unit="s" multiplier="m">10</MinTime>
        <MaxTime unit="s" multiplier="m">1000</MaxTime>
      </GSE>
    </ConnectedAP>
  </SubNetwork>
</Communication>

```

Rys. 1.3 Fragment pliku konfiguracyjnego opisujący parametry komunikacji

Wszystkie te dane przechowywane są w odpowiedniej strukturze przedstawianej na rys. 1.2. Wszystkie struktury danych opisuje sekcja *Data*, a sposób ich przekazywania lub udostępniania innym urządzeniom IED opisują sekcje *GOOSE*, *Buffered* i *Unbuffered Reports*, które wymagają odpowiedniej konfiguracji.

Ważna jest również poprawna konfiguracja parametrów komunikacyjnych samego urządzenia IED. Parametry te opisane są w sekcji *Communication* (i uwzględniają: konfiguracje IP urządzeń, strukturę logiczną sieci oraz transmisje danych multicastowych i rozgłoszeniowych. Informacje zawarte w tej sekcji rzutują na poprawność komunikacji oraz są niezbędne do późniejszego testowania działania urządzeń.

Monitorowanie poprawności działania sieci LAN nie gwarantuje jeszcze braku błędów w transmisji poszczególnych typów danych. Posługiwanie się typowymi aplikacjami informatycznymi śledzącymi ruch pakietów pomiędzy wybranymi urządzeniami nie daje możliwości oceny, czy poszczególne informacje są odbierane lub transmitowane poprawnie.

LN PriFouMMXU1	
Name	Value
▶ DO Mod	on
▶ DO Beh	on
▶ DO Health	Ok
▶ DO NamPit	MiCOM
▶ DO Hz	49,998 Hz
▶ DO PPV	404,011 V; 401,108 V; 404,021 V
▶ DO A	0 A; 0 A; 0 A
▶ DO A2	
▶ DO W	0 Watts; 0 Watts; 0 Watts
▶ DO VA	0 VA; 0 VA; 0 VA
▶ DO PF	0; 0; 0
▶ DO AngA	0 phi; 0 phi; 0 phi
▶ DO AngPPV	29,845 deg; -90,156 deg; 150,107 deg
▶ DO AvgPF	0
▶ DO AngV	0 deg; -120,163 deg; 119,959 deg
▶ DO AvgWatts	0 Watts
▶ DO AvgVAr	0 VAr
▶ DO AvgVA	0 VA
▶ DO V	233,461 V; 232,674 V; 231,502 V
▶ DO VAr	0 VAr; 0 VAr; 0 VAr
▶ DO VN	

Rys. 1.4 Węzeł logiczny MMUX oraz wartości jego atrybutów

Dlatego też konieczne jest stosowanie narzędzi posiadających zdolność do analizowania struktury i zawartości transmitowanych danych zgodnych z architekturą standardu IEC 61850. Narzędzia te posiadają różne funkcjonalności. Najprostsze pozwalają na przeglądanie zawartości plików konfiguracyjnych dla poszczególnych urządzeń IED oraz ich ocenę pod względem zgodności ze standardem. Programy zaawansowane pozwalają nie tylko na ocenę plików SCL, ale przede wszystkim na śledzenie pracy poszczególnych urządzeń w czasie rzeczywistym.

Specjalistyczne programy diagnostyczne umożliwiają śledzenie ruchu wybranych danych dla aktualnej konfiguracji urządzenia. Używają do tego celu różnych metod. Na przykładzie aplikacji IEDScout firmy Omicron można określić te metody, jako:

1. Analiza danych bieżących realizowana poprzez odpytywanie (*polling*) dla:
 - obiektów danych,
 - atrybutów danych,
 - raportów,
 - obiektów *DataSets*,
 - obiektów *GOOSE*.
2. Generowanie komunikatów wymuszonych (np. *GOOSE*).
3. Zastosowanie modułu przechwytywania *Sniffer* w celu:
 - monitorowania przepływu komunikatów w czasie rzeczywistym,
 - monitorowania komunikatów *GOOSE*,
 - filtrowania obserwowanych komunikatów,
 - analizowania zawartości komunikatów,
 - wyszukiwania błędów w przebieg komunikacji.

Przedstawione na rys. 12.4 dane dla węzła logicznego MMUX odpowiadającego za pomiar wielkości elektrycznych uzyskano poprzez zastosowanie metody odpytywania. Uzyskane dane mogą być analizowane na poziomie LN lub poszczególnych atrybutów. Możliwe jest również wymuszanie zmiany wartości dla poszczególnych atrybutów.

Rysunek 12.5 prezentuje dane przechwycone przy zmianie wartości atrybutów dla tego samego węzła. Szczegółowo zaprezentowane zostały ścieżki do odpytanych atrybutów oraz odpowiedź wygenerowana w wyniku zapytania. Oba komunikaty opatrzone zostały cechą

czasu, co również daje możliwość oceny przebiegu komunikacji. Podobne informacje można uzyskać dla innych danych przesyłanych na zasadzie klient-serwer.

Request	
Success:	true
Timestamp:	2015-01-19 13:23:52.629
Paths:	
	Path: G1Measurements/PriFouMMXU1.AvgPF.units.multiplier [CF]
	Path: G1Measurements/PriFouMMXU1.AvgPF.mag.f [MX]
	Path: G1Measurements/PriFouMMXU1.AngV.phsA.units.SIUnit [CF]
	Path: G1Measurements/PriFouMMXU1.AngV.phsA.units.multiplier [CF]
	Path: G1Measurements/PriFouMMXU1.AngV.phsA.cVal.mag.f [MX]
	Path: G1Measurements/PriFouMMXU1.AngV.phsB.units.SIUnit [CF]
	Path: G1Measurements/PriFouMMXU1.AngV.phsB.units.multiplier [CF]
	Path: G1Measurements/PriFouMMXU1.AngV.phsB.cVal.mag.f [MX]
	Path: G1Measurements/PriFouMMXU1.AngV.phsC.units.SIUnit [CF]
	Path: G1Measurements/PriFouMMXU1.AngV.phsC.units.multiplier [CF]
Response	
Success:	true
Timestamp:	2015-01-19 13:23:52.652
Values:	
	Integer: 0
	Float: 0
	Integer: 9
	Integer: 0
	Float: 0
	Integer: 9
	Integer: 0
	Float: -120,1634
	Integer: 9
	Integer: 0

Rys. 1.5 Widok okna śledzenia danych pomiarowych opisanych atrybutami węzła logicznego MMXU

2 WYKORZYSTANIE NARZĘDZI INFORMATYCZNYCH DO ŚLEDZENIA RUCHU W SIECI

- Na początku zajęć należy uruchomić program monitorujący w sieci z urządzeniami IED, może to być program WireShark lub Colasoft Copsa.
- Narzędzia te są programami informatycznymi niebędącym oprogramowaniem specjalistycznym, ale wykorzystywanymi przez informatyków do śledzenia ruchu w sieciach komputerowych.
- Należy uruchomić nasłuch. Wyniki działania programu należy sprawdzić na końcu ćwiczenia.

2.1 Analiza konfiguracji urządzenia IED, odczyt danych wymuszonych

Należy uruchomić program IEDScut firmy Omicron. Pozwala on na przeglądanie zawartości plików konfiguracyjnych urządzeń IED, podsłuchiwanie pracy urządzeń IED oraz kontrolę poprawności komunikacji.

Program IEDScout podzielony jest na trzy zakładki: *File*, *Home*, *Sniffer*. Interfejs programu w zakładce *Home* tworzą elementy w postaci okienek, takie jak: pasek tytułu (zawiera informacje odnośnie nazwy programu oraz licencji), pasek menu (zawiera dostępne polecenia programu) oraz pasek narzędzi (zawierają ikony dostępu do poleceń). W prawej dolnej części okna programu znajduje się pasek trybu pracy *Test Mode/Simulation* umożliwiający przejście z trybu tworzenia i edycji IED do trybu badań. Okno nawigacji (*Navigation Pane*) znajduje się po lewej stronie ekranu, wyświetla strukturę danych badanego urządzenia IED w postaci drzewa znanego z eksploratora Windows. Drzewo zawiera wpisy:

- GOOSE – zorientowane obiektowo zdarzenie stacyjne;

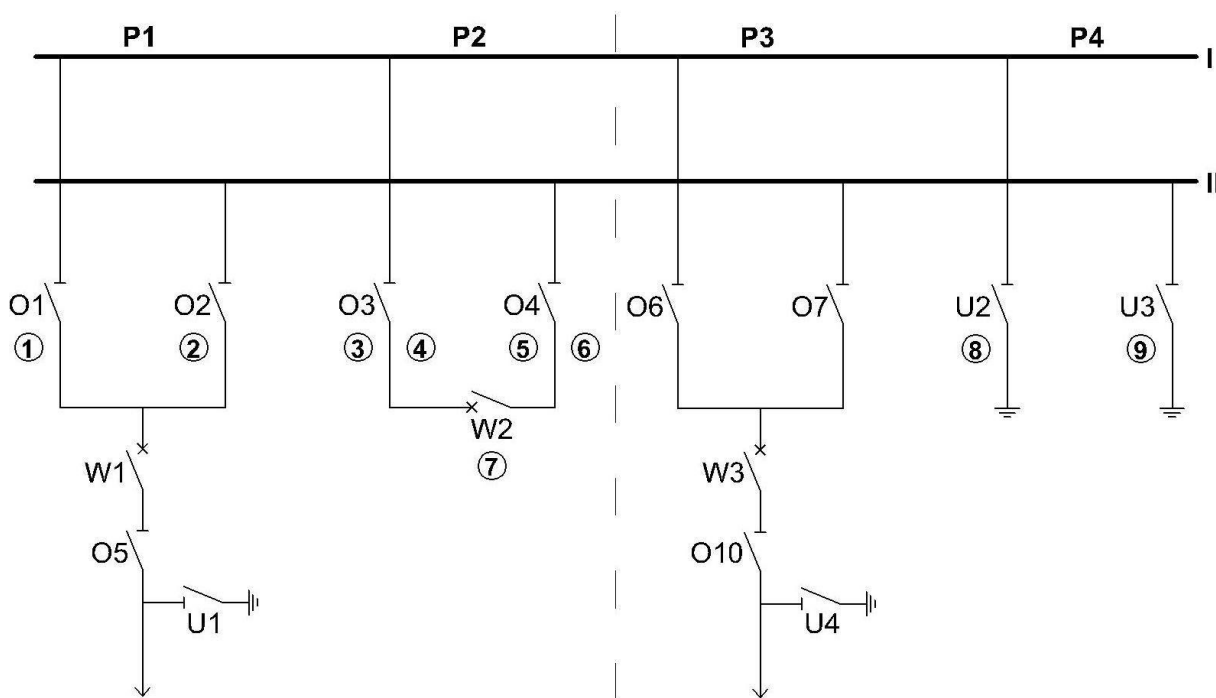
- Reports – raporty;
- DataSets – zestawy danych;
- Data Model – modele danych.

Należy wykonać następujące zadania:

- Dokonać oceny zawartości pliku .ICD wskazanego przez prowadzącego.
- Wykonać analiza danych bieżących realizowana poprzez odpytywanie (*polling*) dla:
 - obiektów danych,
 - atrybutów danych,
 - raportów,
 - obiektów DataSets,
 - obiektów GOOSE.

2.2 Analiza operacji łączeniowych

Program IEDScout umożliwia obserwację zmian stanów poszczególnych urządzeń w stacji elektroenergetycznej. W badaniu wykorzystano zabezpieczenia odległościowe linii REL650 oraz REL670. Panele przednie urządzeń pozwalają na sterowanie poszczególnymi polami. Pola P1 oraz P2 obsługiwane są przez REL670, natomiast pola P3 i P4 przez REL650. Zmiana stanu łączników opisanych numerami umieszczonymi, w kółkach odpowiadają numerom poszczególnych komunikatów obiektów danych *Ind* pochodzących z węzłów logicznych GGIO.



Rys. 12.2.1. Schemat badanego układu

W tym celu posługujemy się panelami przekaźników odległościowych w celu dokonania zmiany stanu poszczególnych łączników. Obserwowane dane GOOSE podzielone są na część definicji i część wartości wiadomości. Górna część definicji opisuje statyczne definicje atrybutów, które zawarto w tabeli.

Tabela 1. Statyczne definicje danych GOOSE

Nazwa definicji	Skrót definicji	Opis definicji
<i>GOOSE control block reference</i>	GoCBRef	Blok kontrolujący informacje GOOSE.
<i>Destination MAC address</i>	DstAddress	Docelowy adres MAC wiadomości GOOSE.
<i>Source MAC address</i>	SrcAddress	Źródłowy adres MAC urządzenia nadającego.
<i>Application ID</i>	AppID	Identyfikator aplikacji. Prawidłowy zakres wynosi 0000 ... FFFF w liczbach szesnastkowych. Wartość domyślna to 0000.
<i>GOOSE ID</i>	GoID	GOOSE ID; musi być unikalna w obrębie systemu.
<i>DataSet name</i>	DataSet	Nazwa zestawu danych.
<i>VLAN ID</i>	VLANID (VID)	Wirtualny identyfikator sieci LAN. Prawidłowy zakres wynosi 000 ... FFF w liczbach szesnastkowych. Wartość domyślna to 000.
<i>VLAN priority</i>	VLAN priority	Priorytet wiadomości wychodzących. Prawidłowy zakres 0 ... 7, gdzie 0 jest najniższy i 7 jest najwyższym priorytetem. Wartość domyślna dla GOOSE jest 4.
<i>Needs commissioning</i>	NdsCom	Wymaganie uruchomienia. Pokazuje, czy to GOOSE musi zostać uruchomione.
<i>Configuration revision</i>	ConfRev	Weryfikacja konfiguracji.

Część dolna definicji przedstawia wartość wiadomości, która zawiera atrybuty mogące zmieniać się z każdą otrzymaną wiadomością. Dokładny opis zmiennych wartości wiadomości przedstawiono w tabeli poniżej.

Tabela 2. Zmienne wartości wiadomości danych GOOSE

Nazwa definicji	Skrót definicji	Opis definicji
<i>Simulation/Test</i>	-	Wskazuje, czy GOOSE jest symulowany.
<i>Timestamp</i>	-	Znacznik czasu ostatniego wystąpienia zmiany danych.
<i>Status Number</i>	StNum	Numer stanu jest zwiększany przy każdej zmianie danych.
<i>Sequence number</i>	SqNum	Numer sekwencji jest ustawiony na zero przy każdej zmianie danych, a zwiększany przy każdej retransmisji.
<i>Time allowed to live</i>	timeAllowedtoLive	Maksymalny czas, aż GOOSE zostanie retransmitowany. Jeśli GOOSE nie zostanie odebrany w tym przedziale czasowym, to limit czasu jest przekroczony.

W celu realizacji zadania należy:

- Zapoznać się ze sposobem pracy przekaźników REL i układem ich połączeń;

- Wykonać załączyć lub wyłączyć wybrane łączniki i zaobserwować, co zmienia się na wyświetlaczach przełączników.
- Zaobserwować, zmiany w programie IEDScout.

2.3 Symulacja GOOSE

Program jest w stanie symulować albo pojedynczy GOOSE lub całe IED (model danych i usługi) z wykorzystaniem definicji GOOSE załadowanych z pliku SCL lub wykrytych w sieci. Pakiety GOOSE zawierają oznakowanie symulacji (GOOSE Simulation Flag), które umożliwia abonentowi odróżnić GOOSE używane do testowania i normalnych GOOSE generowanych w trakcie działania system.

Aby rozpocząć symulację należy wybrać z paska narzędzi (część *Services*) polecenie *Simulate* GOOSE. Pojawi się okno ustawień symulacji (GOOSE Simulation Settings). Ustawienia symulacji GOOSE podzielone są na dwie części po lewej stronie znajdują się:

- GCB attributes – wyświetla atrybuty GOOSE zaczerpnięte z GOOSE Control Block (GCB);
- Advanced GCB attributes – wyświetla zaawansowane atrybuty GCB;
- Simulation intervals – przedziały symulacyjne:
 - Initial (początkowy) (ms) retransmisja GOOSE zaczyna się w przedziale określonym w milisekundach przy Initial.
 - Multiplier (mnożnik) retransmisja zostaje zwiększona poprzez pomnożenie przedziału Initial od wartości Multiplier aż do czasu równego lub większego niż Final (w ms) przedział zostanie osiągnięty.
 - Final (końcowy) (ms) odtąd przedział Final jest używany do momentu aż nastąpi zmiana stanu. Zmiana stanu następuje za każdym razem, gdy wartości przesyłanego GOOSE są modyfikowane.

2.4 Modułu przechwytywania Sniffer

Program pozwala również na przechwytywanie wysyłanych pomiędzy urządzeniami komunikatów, służy do tego zakładka *Sniffer*. Opcja ta pozwala na:

- monitorowania przepływu komunikatów w czasie rzeczywistym,
- monitorowania komunikatów GOOSE,
- filtrowania obserwowanych komunikatów,
- analizowania zawartości komunikatów,
- wyszukiwania błędów w przebieg komunikacji.

Aby móc wykonać powyższe zadania i widzieć zmianę wartości należy wykorzystać dostępne wymuszalniki.

