



ĆWICZENIE 1

Komunikacja między urządzeniami po protokole MODBUS

Politechnika Wroclawska – Laboratorium systemowe

Nazwa dokumentu : REF-PW-LAB_CW1
Numer referencyjny : REF/PW/LAB/2017/04/01

Wersja : B6
Data : 2017-09-12

ZATWIERDZONY PRZEZ	DATA	WERSJA	KOMENTAŻ
<i>Leszek Suchodolski</i>	<i>2017-03-28</i>	<i>A</i>	<i>Pierwsza wersja ćwiczenia</i>
<i>Kamil Sokołowski</i>	<i>2017-09-12</i>	<i>B6</i>	<i>Korekta edytorska</i>
<i>Dariusz Radomski</i>			

Schneider Electric Energy Poland Sp. z o.o.
Energy Automation Centre (REF)

ul. Strzegomska 23-27, 58-160 Swiebodzice, Poland
tel.: +48 74 854 84 10, fax: +48 74 854 85 48
ref.swiebodzice@schneider-electric.com
Environmental Register No.: E0001768WBW

schneider-electric.com/pl

Legal entity registration details:

Schneider Electric Energy Poland Sp. z o.o.
ul. Zwirki i Wigury 52, 43-190 Mikołow, Poland

Share capital: 43,031,400.00 PLN

Registry Court: Sad Rejonowy Katowice-Wschod,
VIII Wydział Gospodarczy KRS; KRS No.: 0000202164

Tax ID No.: PL 8840007793, REGON: 890006542



SPIS TREŚCI

1. zakres ćwiczenia.....	3
2. wprowadzenie teoretyczne.....	4
2.1. Stanowisko pracy - układ połączeń.....	4
2.2. Transmisja szeregową.....	5
2.3. Protokół komunikacji Modbus RTU – informacje praktyczne	7
2.4. Przykładowa analiza komunikatu cyfrowego w protokole Modbus RTU	9
3. przebieg ćwiczenia.....	12
3.1. Czynności przełączeniowe.....	12
3.2. Komunikacja w protokole Modbus cz.1	12
3.3. Komunikacja w protokole Modbus cz.2	13
3.4. Obserwacja ramki komunikacyjnej za pomocą oscyloskopu.....	14
4. spis rysunków, tabel i załączników do ćwiczenia.....	15



1. ZAKRES ĆWICZENIA

W ćwiczeniu studenci mają okazję zapoznać się z komunikacją cyfrową między zabezpieczeniem elektro-energetycznym *P116*, a sterownikiem polowym model *C264* produkcji Schneider-Electric jako elementem SSiN (Systemu Sterowania i Nadzoru).

Studenci zapoznają się z protokołem komunikacyjnym *Modbus* oraz ze sposobem parametryzacji urządzeń biorących udział w wymianie danych. Zakres ćwiczenia obejmuje obserwację wymiany komunikatów między sterownikiem, czyli urządzeniem typu RTU (ang. Remote Terminal Unit), a urządzeniem IED (ang. Intelligent Electronic Device).

Zakres prac:

- weryfikacja połączeń elektrycznych i parametrów komunikacyjnych urządzeń na stanowisku do ćwiczeń,
- wymuszanie zmian parametrów elektrycznych rejestrowanych przez IED,
- obserwacja zdarzeń na wyświetlaczu LCD sterownika oraz w dzienniku HMI (ang. Human Machine Interface),
- analiza komunikatów protokołu *Modbus* dla stanów statycznych, pomiarów i komend z wykorzystaniem oprogramowania diagnostycznego sterownika *C264*,
- wykorzystanie oprogramowania *ModbusPool* symulującego sterownik RTU, przesyłanie wirtualnych komunikatów, analiza zgromadzonych danych,
- porównanie cyfrowego komunikatu z jego postacią analogową za pomocą oscyloskopu,
- sporządzenie sprawozdania z przebiegu ćwiczenia,

Celem ćwiczenia jest zapoznanie studentów z protokołem komunikacyjnym *Modbus*. Nauczenie analizy komunikatów przesyłanych za pomocą tego protokołu oraz zapoznanie z ogólnym zastosowaniem RTU jako koncentratora danych.

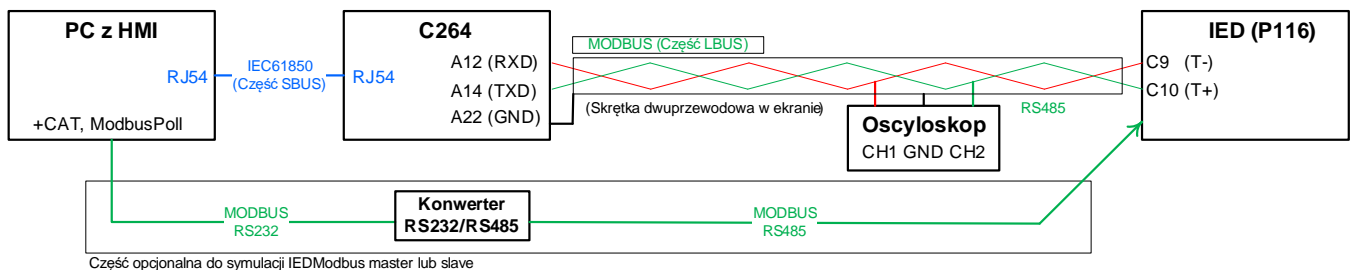
2. WPROWADZENIE TEORETYCZNE

Transmisja szeregowa to jeden z najtańszych sposobów na przesyłanie danych między dwoma urządzeniami. Zaletą transmisji szeregowej jest to, że większość urządzeń nie wymaga dodatkowych specjalistycznych modułów lub oprogramowania, a dostępne na rynku aplikacje spełniają wymogi standardów. Powszechna dostępność konwerterów pozwala na elastyczne budowanie takich aplikacji.

Modbus jest protokołem komunikacji szeregowej opracowanym w 1979 roku przez firmę *Modicon* (obecnie *Schneider-Electric*). Definiuje sposób wymiany danych między programowalnymi sterownikami oraz urządzeniami elektronicznymi. Obecnie stosowany głównie w przemyśle. Producenci urządzeń z powodzeniem stosują go również w innych aplikacjach związanych na przykład z energetyką. Umożliwia wymianę danych w sieci, w skład której wchodzi np. analizatory parametrów sieciowych instalowanych w rozdzielni energetycznej. Powstało wiele odmian tego protokołu dla komunikacji szeregowej oraz dla sieci *Ethernet*. *Modbus* jest obecnie standardem otwartym.

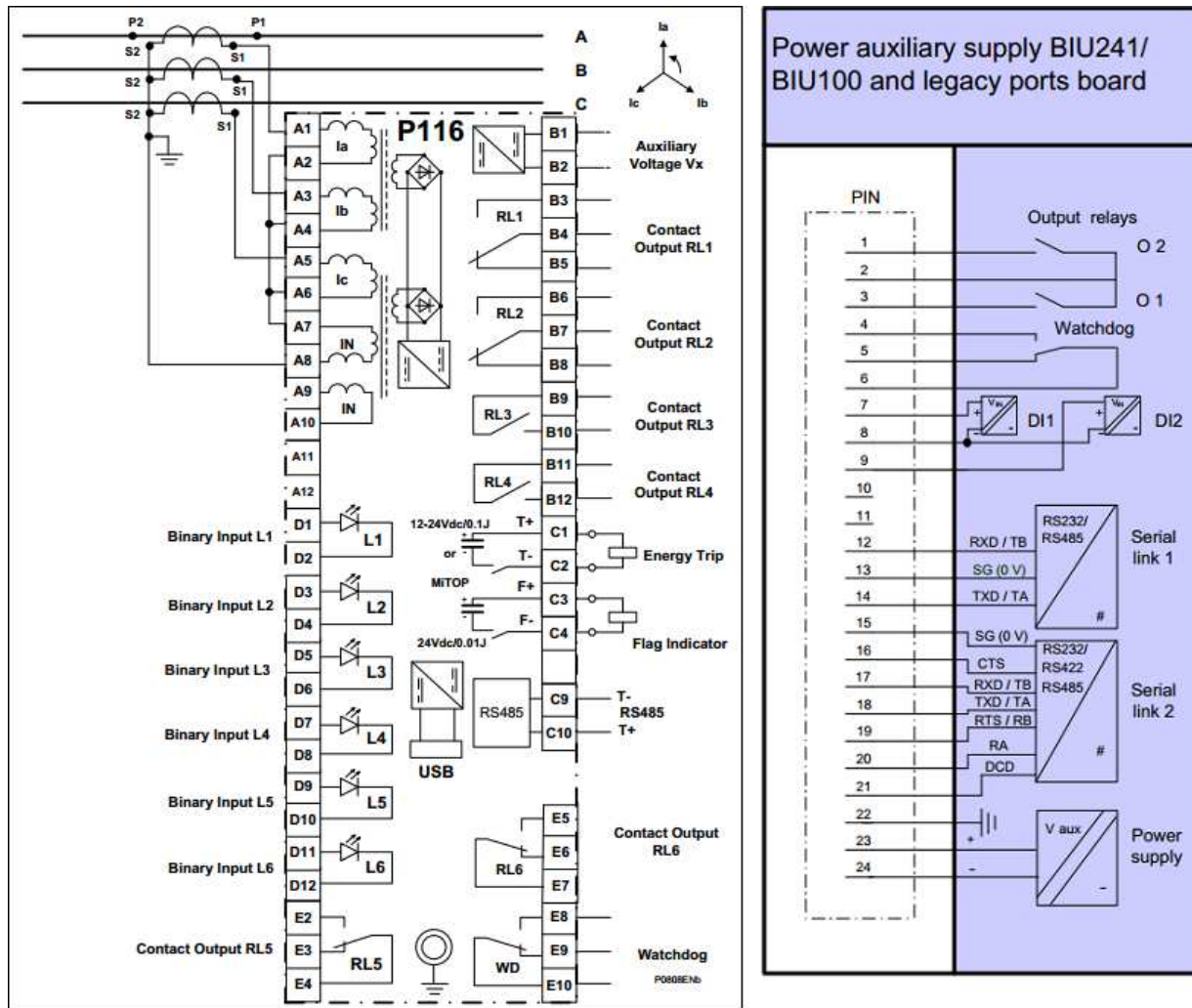
2.1. Stanowisko pracy - układ połączeń

Stanowisko laboratoryjne składa się kompletu zabezpieczeń elektro-energetycznych wyposażonych w moduł komunikacji szeregowej, sterownika, oscyloskopu oraz komputera wyposażonego w oprogramowanie diagnostyczne. Na rysunku Rys.1 przedstawiono schemat prawidłowego połączenia pomiędzy urządzeniami.



Rys. 1 Układ laboratoryjny - schemat połączeń

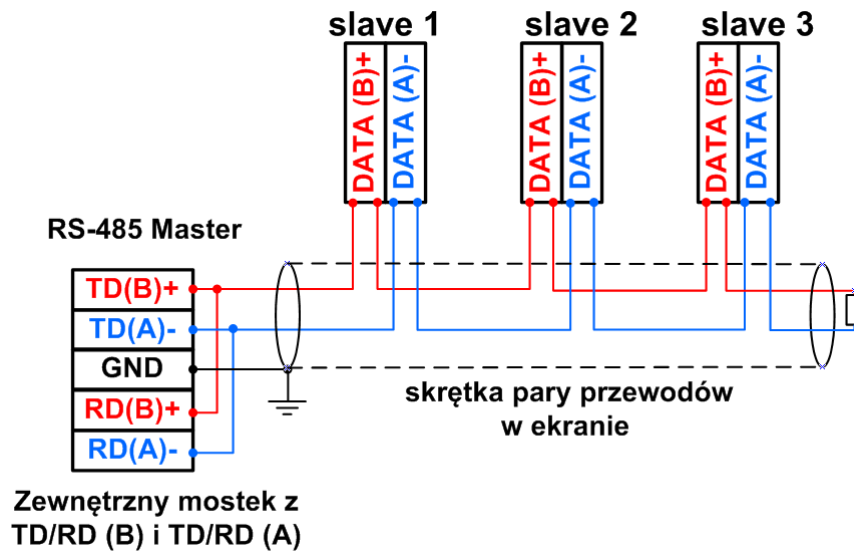
Na rysunku Rys.2 znajduje się fragment DTR (Dokumentacji Techniczno-Ruchowej) dla urządzeń *P116* oraz *C264*. Za jego pomocą można zweryfikować połączenia elektryczne między elementami ćwiczenia.



Rys. 2 Wycinek DTR dla wybranych urządzeń

2.2. Transmisja szeregowa

W rzeczywistych rozwiązaniach obiektowych połączenie między urządzeniami realizowane jest zazwyczaj zgodnie ze standardem RS-485 (ang. Recommended Standard). Prawidłowe połączenie elektryczne zaprezentowano na Rys.3. Urządzenie pracujące w charakterze RTU określane jest jako *Master*, a pozostałe urządzenia to *Slave*.



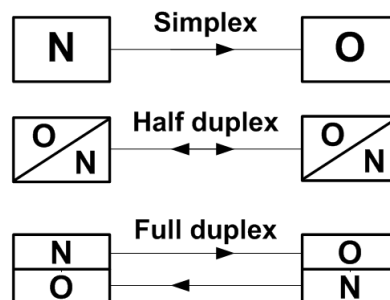
Rys. 3 RS-485 układ dwuprzewodowy z wieloma odbiornikami

W tak zaproponowanym układzie należy zdecydować o wymianie danych między nadajnikiem, a odbiornikiem. Rozróżniamy typy transmisji:

Simplex – transmisja realizowana w jednym kierunku,

Halfduplex – transmisja realizowana w obu kierunkach ale nie jednocześnie, dane mogą być przesłane w jednym kierunku, a następnie w drugim,

Fullduplex – czyli transmisja w obu kierunkach. Może ona być realizowana poprzez zastosowanie oddzielnej pary przewodów dla każdego z kierunków. Możliwe jednoczesne przesyłanie i odbieranie informacji.



Rys. 4 Typ transmisji

Zanim nastąpi wymiana danych w układzie połączonych ze sobą urządzeń, ustala się jednoznaczne parametry transmisji, wspólne zarówno dla *Master* jak i *Slave*.

Parametry transmisji:

- szybkość transmisji – urządzenia nadawcze i odbiorcze muszą pracować z jednakową szybkością (to znaczy wiedzieć ile czasu trwa transmisja pojedynczego bitu). Szybkość podawana jest w bitach na sekundę, *bps* (ang. bits per second). Wartości jakie przyjmuje ten parametr to np.: 75, 110, 150, 300, 600, 1200,

- 2400, 4800, 9600, 19200, 38400, 57600 oraz 115200 bps.
- ilość danych – przez ten parametr należy rozumieć ilość bitów odpowiedzialnych za dane. Zazwyczaj parametr przyjmuje wartość 7 lub 8 bitów z danymi.
 - bity synchronizacji – są to bit startu oraz jeden lub dwa bity stopu. Wprowadza się je, by urządzenia nadawcze i odbiorcy potrafiły rozpoznać początek i koniec porcji danych podczas realizowanej transmisji.
 - kontrola parzystości – parametr ten określany jest też jako bit kontrolny. Wybierany jako Parzysty, Nieparzysty, Brak (ang. Even, Odd, None). Ustawienie Brak oznacza brak kontroli, a przesłana porcja danych nie zawiera bitu kontroli. Kontrola na tak niskim poziomie zakłada sprawdzenie czy w przesłanej porcji danych znajduje się parzysta, czy też nieparzysta ilość bitów w stanie wysokim. Można to zaobserwować na przykładzie Tab.1.

8 bitów danych	Ile bitów w stanie „1”	Stan bitu parzystości	
		even	odd
00000000	0	0	1
10001001	3	1	0
11001101	5	1	0
11111111	8	0	1

Tab. 1 Kontrola parzystości

Ważnym czynnikiem zapewniającym spójność przesyłanych danych jest decyzja o sposobie ich przesyłania, rozróżniamy dwa.

Synchroniczna transmisja – przesyłanie danych poprzedza specyficzna informacja wstępna, za jej pomocą nadawca i odbiorca synchronizują się. Po tej operacji następuje przesłanie danych w takt sygnału synchronizującego. Preambuła synchronizująca jest powtarzana między innymi gdy urządzenia stwierdzą wzrost ilości błędów w transmisji.

Asynchroniczna transmisja – sposób ten nie wymaga stosowania dodatkowego sygnału taktującego. Transmisja rozpoczyna się od przesłania bitu startu, następnie przesyłane są bity danych, opcjonalny bit parzystości, transmisję kończą bity stopu. Po czasie martwym procedura jest powtarzana. Transmisja nazywana jest asynchroniczną gdyż zakłada się, że dane mogą pojawiać się w dowolnej chwili i będą natychmiast transmitowane do odbiorcy.

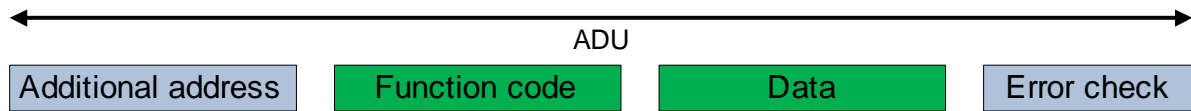
2.3. Protokół komunikacji *Modbus RTU* – informacje praktyczne

Pełna specyfikacja protokołu udostępniona jest w *Internecie*.¹ Rozdział ten przybliży jedynie podstawowe dane na temat protokołu i jego praktycznego zastosowania w ćwiczeniu. Omawiana jest jedynie implementacja rozpoznawana jako *Modbus RTU*.

Informacja pomiędzy urządzeniami przesyłana jest w postaci jednostek protokołu ADU (ang. Application Data Unit) potocznie zwanych ramkami. Zawierają one adres

¹ Przykładowa lokalizacja: Modbus Protocol Specification - <http://www.modbus.org/>

urządzenia, kod funkcji, dane i pole kontrolne. Rys.5 przybliża graficzną postać takiej ramki.



Rys. 5 Budowa ramki Modbus

Adres (ang. additional address) – reprezentowany jako liczba z zakresu od 0 do 255.
 Kod funkcji (ang. Function code) – reprezentowany jako liczba z zakresu od 1 do 255,
 Dane (ang. Data) – fragment przeznaczony na dane,
 Kontrola błędów (ang. error check) – reprezentowana jako suma kontrolna, w skrócie CRC (ang. Cyclical Redundancy Check) zawiera informacje umożliwiające sprawdzenie poprawności ramki, wyliczana jest za pomocą specjalnego algorytmu.

Warto wiedzieć, że:

- Protokół umożliwia wymianę danych między wieloma urządzeniami na tym samym łączu danych,
- Dla większości urządzeń należy wybrać tryb protokołu: *ASCII* lub *RTU*,
- *Master*, to urządzenie kontrolujące wymianę informacji, na jednym łączu danych występuje tylko jeden *Master*,
- *Slave* to urządzenie posiadające dane, potrafi ono reagować na rozkazy przesłane przez urządzenie *Master*,
- Najbardziej znaczący bajt dla adresu i danych przesyłany jest jako pierwszy,
- Najdłuższa ramka (ADU) może zawierać 256 bajtów,
- Dane czy też zmienne w *Modbus* to wartości binarne wejść lub wyjść oraz rejestry,
- Podczas wymiany komunikatów mogą pojawić się błędy, *Slave* odpowiada wówczas do urządzenia *Master* w miejsce funkcji pojawia się wartość funkcji którą wywołał *Master* plus wartość 128. Odpowiedź zawiera jeden bajt danych, a w nim kod błędu – wyjątek (ang. exception code),
- Wartości zapisane są w pojedynczych rejestrach (2 bajty), niektóre dane mogą być zapisane na dwóch rejestrach, zależy to od producenta urządzenia.
- Znamienita większość aplikacji prezentuje dane w zapisie szesnastkowym,

Typ	Rodzaj zmiennej	Możliwość zapisu
Discreet Input Wejścia dwustanowe	Single bit Jedno-bitowy	Read Tylko odczyt
Coils Cewka, przekaźnik	Single bit Jedno-bitowy	Read / Write Odczyt / zapis
Input registers Rejestry wejściowe	16-bit Word Słowo 16-bitowe	Read Tylko odczyt
Holding registers Rejestry pamiętające	16-bit Word Słowo 16-bitowe	Read / Write Odczyt / zapis

Tab. 2 Typy i rodzaje zmiennych w Modbus RTU

Opis funkcji	Kod funkcji (dziesiętnie)	Kod funkcji (szesnastkowo)
Read Coils Odczyt stanów wyjść przekaźnikowych	01	0x01
Read Discreet Inputs Odczyt stanów wejść dwustanowych	02	0x02
Read Holding Registers Odczyt rejestrów pamiętających	03	0x03
Read Input Registers Odczyt rejestrów wejściowych (np. wejścia analogowe)	04	0x04
Write Single Coils Zapis jednego wyjścia, ustawienie przekaźnika	05	0x05
Write Single Register Zapis do jednego rejestru pamięci	06	0x06
Write Multiple Coils Zapis wielu wyjść, ustawienie przekaźników	15	0x0F
Write Multiple registers Zapis wielu rejestrów	16	0x10

Tab. 3 Podstawowe funkcje dostępne w Modbus RTU

Code	Text	Details
1	Illegal Function	Function code received in the query is not recognized or allowed by slave
2	Illegal Data Address	Data address of some or all the required entities are not allowed or do not exist in slave
3	Illegal Data Value	Value is not accepted by slave
4	Slave Device Failure	Unrecoverable error occurred while slave was attempting to perform requested action
5	Acknowledge	Slave has accepted request and is processing it, but a long duration of time is required. This response is returned to prevent a timeout error from occurring in the master. Master can next issue a Poll Program Complete message to determine if processing is completed
6	Slave Device Busy	Slave is engaged in processing a long-duration command. Master should retry later
7	Negative Acknowledge	Slave cannot perform the programming functions. Master should request diagnostic or error information from slave
8	Memory Parity Error	Slave detected a parity error in memory. Master can retry the request, but service may be required on the slave device

Tab. 4 Standardowe kody błędów w Modbus RTU

2.4. Przykładowa analiza komunikatu cyfrowego w protokole Modbus RTU

Przykład 1:

Ramka pochodząca od urządzenia *Master*

[TX P=1 8 bytes : 03 03 00 06 00 02 25 E8]

to 8 bajtów w postaci szesnastkowej,

03 – Adres urządzenia wynosi 3,

03 – Funkcja o kodzie 3, czyli odczyt rejestrów,

00 06 00 02 – Sekcja Dane zawiera 4 bajty, dwa pierwsze to adres rejestru, który wynosi 6, kolejne dwa bajty to ilość rejestrów do odczytu równa 2,

25 E8 – Ostatnia sekcja to suma kontrolna CRC,



Ramka odpowiedzi od *Slave*

[RX P=1 9 bytes : 03 03 04 41 BC 6D AA A0 C4]

to 9 bajtów w postaci szesnastkowej,

03 – Adres urządzenia wynosi 3,

03 – Funkcja o kodzie 3, czyli odpowiedź na odczyt rejestrów,

04 41 BC 6D AA – Sekcja Dane zawiera 5 bajtów, pierwszy oznacza ilość bajtów danych czyli 4, dwa kolejne to rejestry, każdy na dwóch bajtach. Dla tego przykładu można przyjąć, że reprezentują one wartość zmiennoprzecinkową zapisaną na dwóch rejestrach, zakodowaną według standardu *IEEE-754*². Przesłana wartość to liczba rzeczywista, w zaokrągleniu wynosi 23,55.

A0 C4 – suma kontrolna CRC,

Przykładowe formatowania liczb to:

- *unsigned short int(16b)*, *unsigned int(32b)* – liczby całkowite bez znaku;
- *signed short int(16b)*, *signed int(32b)* – liczby całkowite ze znakiem (najstarszy bit to znak)
- *float(32b)* – liczby zmiennoprzecinkowe

Przykład 2:

Ramka pochodząca od urządzenia *Master*

[TX: 01 03 00 01 00 01 D5 CA]

Zapytanie urządzenia o adresie 1, o jeden rejestr (funkcja 3) o adresie 1,

Ramka odpowiedzi od *Slave*

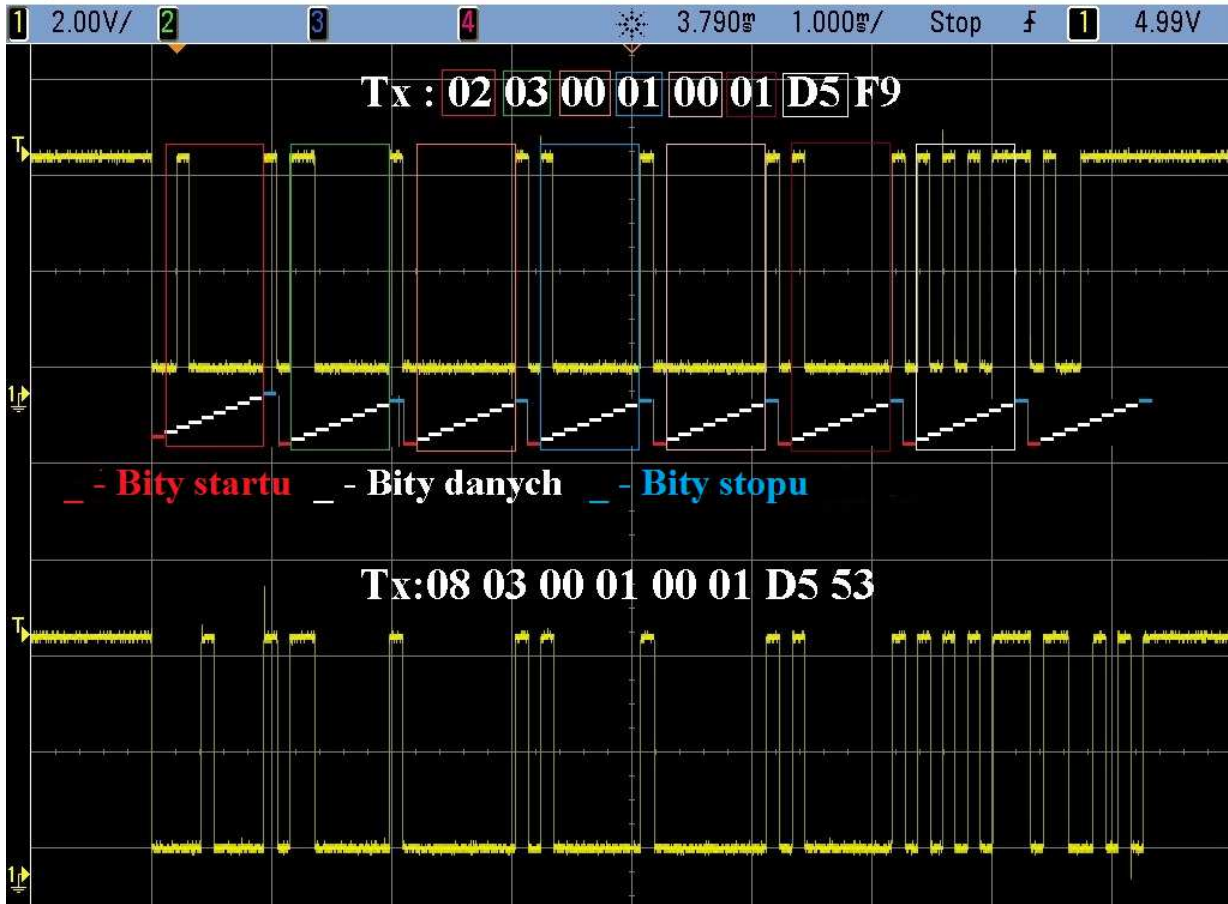
[RX: 01 83 02 A0 C4]

Funkcja 131 (128 plus 3) oznacza wystąpienie wyjątku podczas próby odpowiedzi na zapytanie funkcją 3, kod błędu wynosi 2, czyli żądany adres nie jest dostępny.

Przykład 3:

Na Rys.6 zaprezentowano postać analogową ramki przesłanej przez urządzenie *Master*.

² Format liczb zapisanych w rejestrach zdefiniowany jest przez producentów urządzeń



Rys. 6 Ramki Modbus w postaci analogowej



3. PRZEBIEG ĆWICZENIA

3.1. Czynności przełączeniowe

W tej części ćwiczenia należy zaobserwować poprawność odwzorowania stanów pracy urządzeń. Wartości elektryczne rejestrowane przez przekaźnik *P116* powinny odpowiadać tym, które odwzorowane są na urządzeniu *C264* oraz na stacji operatorskiej HMI. Warto zanotować obserwacje i rozbieżności.

Weryfikacja stanu komunikacji:

Za pomocą oprogramowania diagnostycznego *CAT* należy sprawdzić poprawność stanu komunikacji między *C264*, a *P116*. W tym celu należy posłużyć się schematem poruszania po oprogramowaniu *CAT* (Załącznik 1). Za pomocą schematu poruszania się po konfiguracji *P116* (Załącznik 2) zweryfikować poprawność parametrów komunikacyjnych.

Parametry transmisji:

adres *Slave 1*,
prędkość 9600 bps,
8 bitów danych, brak parzystości, 1 bit stopu (w skrócie 8n1).

Dokonać odpowiednich korekt jeżeli jest to konieczne. Zanotować obserwacje.

Sterowanie wyłącznikiem w polu:

W polu nr.5 (P05) sekcji 15kV na wyświetlaczu LCD *C264* (lub z poziomu stacji operatorskiej HMI) zmienić stan wyłącznika *Q1*. Należy skorzystać z załącznika 3.

Zaobserwować stan wyjść przekaźnikowych *RL5* (odpowiada „cb close”) i *RL6* (odpowiada „cb trip”) w urządzeniu *P116*.

Zmiana stanu wyłącznika *Q1*:

Zmienić stan wejścia *L6* przekaźnika *P116*. Zaobserwować czy zmienia się położenie wyłącznika na odpowiednim widoku w *C264* oraz na stacji operatorskiej HMI. W dzienniku zdarzeń *C264* i na widoku HMI sprawdzić i zanotować czas pojawienia się zdarzeń, porównać je (Załącznik 4).

Odczyt wartości prądu w polu:

Zmienić wartość prądu fazy *L1* rejestrowanego przez przekaźnik *P116*. Porównać jego wartość z dostępną na wyświetlaczu LCD *C264* oraz na stacji operatorskiej HMI. Zanotować obserwacje dla przynajmniej dwóch różnych wartości prądu.

3.2. Komunikacja w protokole *Modbus* cz.1

Ta część ćwiczenia polega na obserwacji i diagnostyce komunikacji pomiędzy urządzeniami w sieci *Modbus*. Poprzez powtórzenie czynności przełączeniowych



opisanych w punkcie 3.1 oraz przechwycenie i późniejszą analizę komunikatów cyfrowych, należy zweryfikować poprawności przesyłanych stanów statycznych, pomiarów i sterowań. Należy zanotować obserwacje.

W oprogramowaniu CAT lub z wiersza poleceń Windows uruchomić monitor portu szeregowego (Załącznik 5). Przechwycić i zapisać ramki komunikacji. Wykonać po kilka prób zmiany położenia łączników oraz prób sterowań.

Sterowanie wyłącznikiem w polu:

Komenda na wyłącznik „Otwórz” – Adres: 0x4007,
Komenda na wyłącznik „Zamknij” – Adres: 0x400F,

Stany statyczne:

Stany wejść cyfrowych – Adres: 0x10,
Wejście L1 reprezentuje bit 0 i odpowiednio Wejście L6 bit 5;
format danych: *unsigned short int(16)*, który można sprawdzić w dokumentacji urządzenia.

Odczyt wartości prądu:

Prąd fazy L1 - Adres: 0x0040,
mnożnik według karty urządzenia wynosi: 0,01;
format danych: *unsigned short int (16b)*,

Dokonać analizy zgromadzonych ramek komunikacyjnych i porównać je ze stanem fizycznym wartości elektrycznych, porównać ze wartościami dostępnymi na wyświetlaczu C264. Wyciągnąć wnioski i zaproponować rozwiązania jeżeli są konieczne.

3.3.Komunikacja w protokole Modbus cz.2

Kolejna część ćwiczenia polega na symulacji urządzenia *Master* z wykorzystaniem dostępnego oprogramowania. Należy wymusić odpowiednie zapytanie podane przez prowadzącego ćwiczenie i przeanalizować komunikację cyfrową między *Master* i *Slave*.

Przygotowanie stanowiska:

Na komputerze *PC* uruchomić oprogramowanie symulujące urządzenie *Master* (Załącznik 6). Przygotować układ sieci *Modbus* tak, aby *P116* połączyć z komputerem *PC* za pomocą konwertera *RS-232/RS-485*.

Pierwszy błąd odpowiedzi:

Wprowadzić w parametrach oprogramowania *Master* adres rejestru *Slave* (podany przez prowadzącego) i zwrócić uwagę na ramkę odpowiedzi w oknie monitoringu



oprogramowania. Dokonać analizy ramki zapytania i odpowiedzi z uwzględnieniem kodu błędu.

Drugi błąd odpowiedzi:

Wysłać zapytanie funkcją podaną przez prowadzącego. Dokonać analizy ramki zapytania i odpowiedzi z uwzględnieniem kodu błędu odpowiedzi. Dla ułatwienia analizy ramek należy pytać o jeden adres.

W sprawozdaniu wyjaśnić jakie są przyczyny powstających błędów. Zaproponować rozwiązania dla obydwu prób, tak aby uzyskać prawidłowe komunikaty.

3.4. Obserwacja ramki komunikacyjnej za pomocą oscyloskopu

Ostatnia część ćwiczenia polega na porównaniu „analogowej” postaci ramki komunikacyjnej z jej cyfrowym odpowiednikiem oraz na obserwacji wpływu zakłóceń na kanał komunikacyjny.

Obserwacja komunikacji:

Wykorzystać układ sieci *Modbus* z symulatorem *Master* bez podłączonego urządzenia *Slave*. Za pomocą oscyloskopu wykonać pomiar sygnału analogowego na łączu *RS-485* (dwa kanały), porównać wyniki z przesyłaną z symulatora ramką cyfrową otrzymaną z monitora portu szeregowego (Załącznik 6). Ustawić symulator *Master* na zapytanie o stany statyczne.

Wykonać pomiar sygnału analogowego dla trzech różnych ramek bez odpowiedzi (bez podłączonego urządzenia *Slave*) oraz jeden pomiar zawierający odpowiedź (*P1 16* podłączone do sieci *Modbus*).

Badanie wpływu zakłóceń:

W układzie sieci *Modbus* z symulatorem *Master* oraz *P1 16* jako urządzeniem *Slave*. Zbadać wpływ zakłócenia na kształt ramki analogowej w przewodzie *RS-485*:

- zarejestruj ramkę analogową bez zakłócenia;
- zarejestruj ramkę analogową zakłóconą;
- zmień przewód komunikacji na ekranowany i ponownie zarejestruj ramkę analogową z obecnym zakłóceniem

Zanotuj obserwacje i umieść je w sprawozdaniu.



4. SPIS RYSUNKÓW, TABEL I ZAŁĄCZNIKÓW DO ĆWICZENIA

Rys. 1 Układ laboratoryjny - schemat połączeń.....	4
Rys. 2 Wycinek DTR dla wybranych urządzeń.....	5
Rys. 3 RS-485 układ dwuprzewodowy z wieloma odbiornikami.....	6
Rys. 4 Typ transmisji	6
Rys. 5 Budowa ramki Modbus.....	8
Rys. 6 Ramki Modbus w postaci analogowej.....	11
Tab. 1 Kontrola parzystości	7
Tab. 2 Typy i rodzaje zmiennych w Modbus RTU	8
Tab. 3 Podstawowe funkcje dostępne w Modbus RTU	9
Tab. 4 Standardowe kody błędów w Modbus RTU.....	9



ZAŁĄCZNIK 1 – Oprogramowanie CAT



ZAŁĄCZNIK 2 – Poruszanie się po panelu P116



ZAŁĄCZNIK 3 – Poruszanie się po panelu C264



ZAŁĄCZNIK 4 – Odczyt zdarzeń



ZAŁĄCZNIK 5 – Monitorowanie portu szeregowego PC



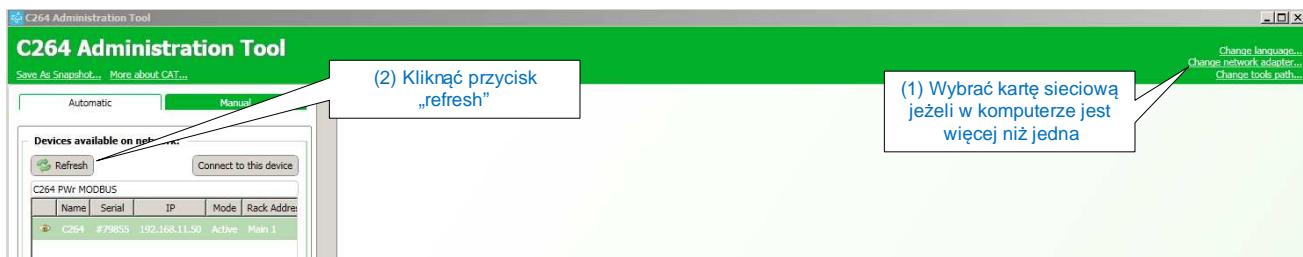
ZAŁĄCZNIK 6 – Symulacja Modbus Master

KONIEC DOKUMENTU

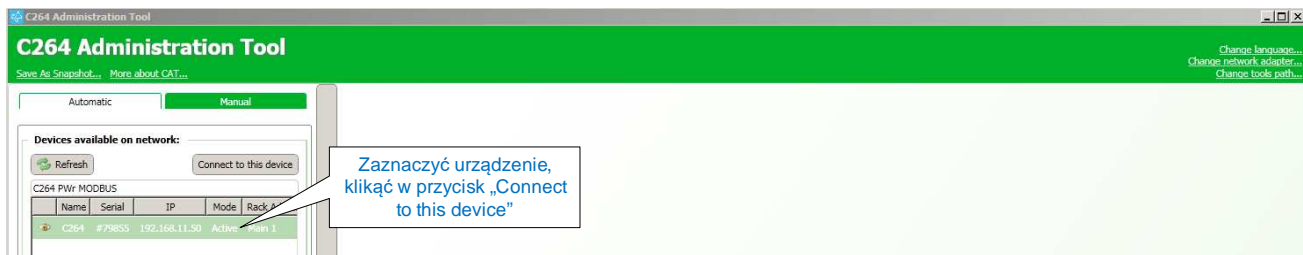


ZAŁĄCZNIK 1 – Oprogramowanie CAT

Uruchomienie oprogramowania CAT (ang. Computer Administration Tool) następuje poprzez skrót umieszczony na pulpicie stanowiska komputerowego PC.



Należy wybierać połączenie sieciowe (1), a następnie w zakładce „Automatic” wykonać skanowanie (2) w poszukiwaniu urządzenia C264.



Wybrać dostępne urządzenie i połączyć się z nim poprzez (przycisk „Connect to this device”).

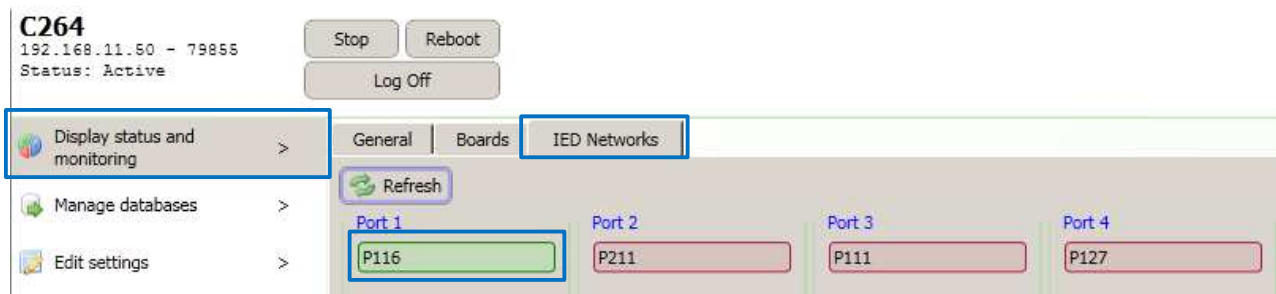
Należy zalogować się wybierając użytkownika, oraz wpisując odpowiednie hasło.



UWAGA: Jeden użytkownik może zalogować się do urządzenia C264 tylko jeden raz. Należy o tym pamiętać, jeżeli korzysta się z przedniego panelu operatorskiego. Aby wylogować użytkownika z panelu C264 należy zapoznać się z odpowiednią instrukcją

dołączoną do ćwiczenia (Załącznik 3). Wylogować użytkownika z oprogramowania CAT można po naciśnięciu przycisku „Log Off”

Po poprawnym zalogowaniu się w urządzeniu C264, status połączenia z IED można podejrzeć jak na załączonym rysunku poniżej. Urządzenia z którymi sterownik oczekuje na połączenie widnieją na liście „IED Networks”.



Poprawnie połączone urządzenia IED, będą podświetlone kolorem zielonym.

Dostępne - skonfigurowane w urządzeniu C264 – wartości statyczne, pomiary oraz zarejestrowane zdarzenia można wczytać w zakładce „Manage events and states”.

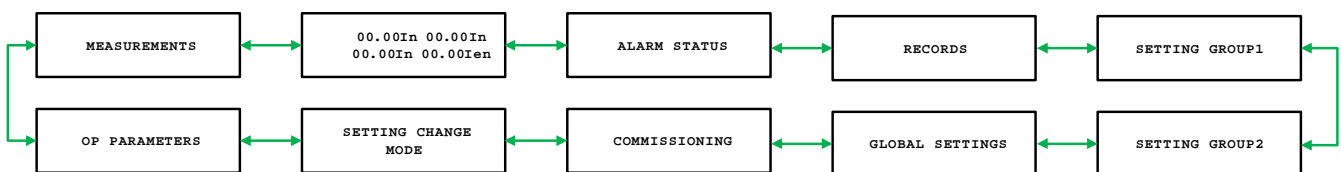
Po sprawdzeniu interesujących parametrów warto wylogować użytkownika z C264.



ZAŁĄCZNIK 2 – Poruszanie się po panelu P116

Parametry transmisji szeregowej w P116 można sprawdzić oraz dokonać ich zmiany z dostępnego menu na panelu przednim urządzenia, wybierając za pomocą przycisków, strzałek odpowiednią grupę ustawień.

Dostępne kategorie menu jak na rysunku:

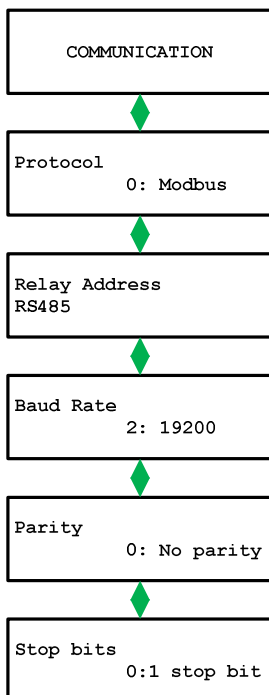


Nawigując po menu w poziomie należy odszukać kategorię „Global Settings”.

Wciśnięcie strzałki w dół , pozwoli otworzyć wybraną pozycję menu.

Dalej wybrać za pomocą strzałek w poziomie pozycję „Communication”, zagłębienie się w menu zawsze po wyborze strzałki skierowanej w dół.

Dostępne parametry komunikacyjne jak na załączonym rysunku:



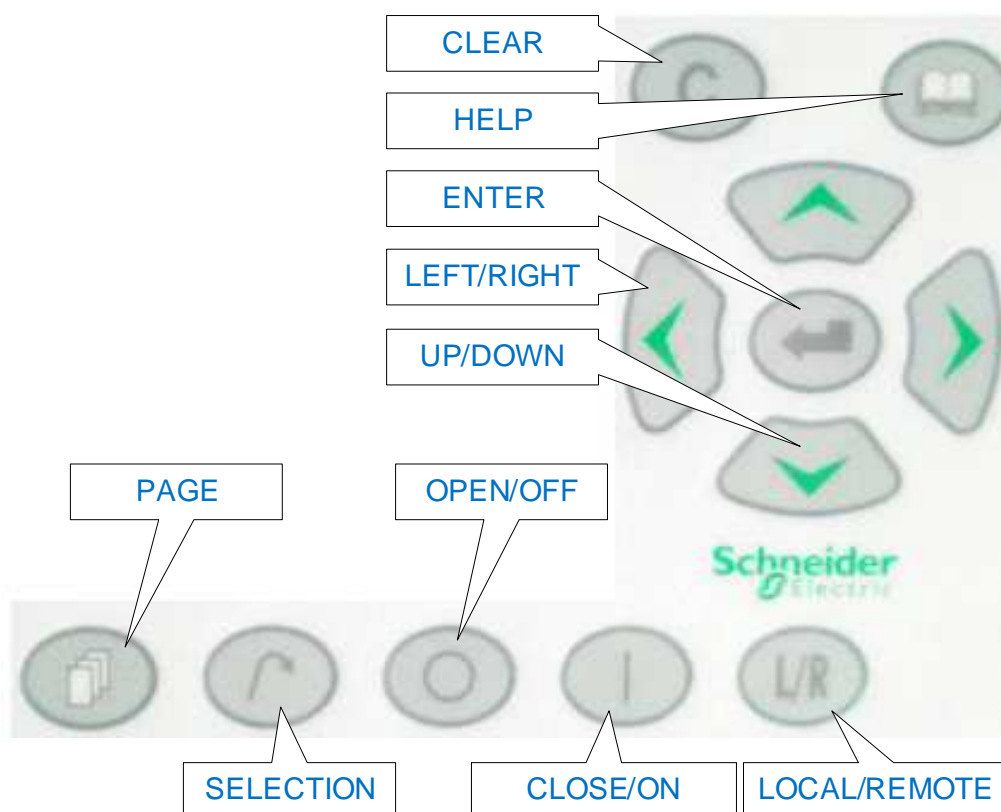
Wybór i zatwierdzenie parametru za pomocą przycisku OK. Zmiana za pomocą strzałek w pionie . Przycisk „C” pozwala opuścić menu. Aby opuścić tryb edycji należy równocześnie nacisnąć strzałki lewo + góra i zatwierdzić przyciskiem OK.



ZAŁĄCZNIK 3 – Poruszanie się po panelu C264

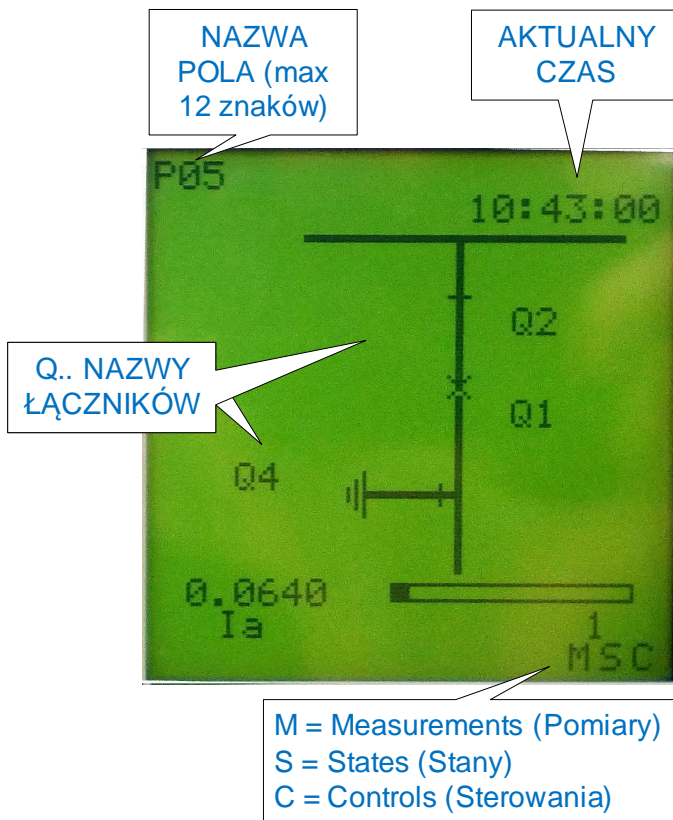
Panel przedni C264 nazywany LHMI (ang. Local Human Machine Interface) umożliwia podgląd skonfigurowanych pól rozdzielni. Podgląd dyskretnych stanów wejść na sprzętowych kartach DIU (ang. Digital Input Unit). Podgląd zarejestrowanych w sterowniku zdarzeń, alarmów, błędów sprzętowych, programowych i konfiguracyjnych. Możliwe jest również wykonanie sterowań łącznikami w polu jak i podgląd dostępnych w nim pomiarów.

Przechodzenie pomiędzy dostępnymi widokami umożliwiają dostępne na panelu przyciski, których opis znajduje się na załączonym rysunku:



- PAGE** – w połączeniu ze strzałkami pozwala na przewijanie stron
- SELECTION** – wybrany na widoku pola, pozwala zaznaczyć obiekt którym chcemy sterować. Obiekty, litery MSC oznaczają kolejno pomiary, stany i sterowania.
- ENTER** – pozwala na zatwierdzenie wyboru obiektu
- CLEAR** – pozwala na zrezygnowanie z wyboru obiektu, wycofanie się.

Widok przykładowego pola z opisem:



Sterowanie wyłącznikiem Q1

Aby wysłać komendę sterowniczą dla wyłącznika Q1 należy na widoku pola dla ćwiczenia, przyciskiem „SELECT” wybrać Q1 (Q1 w polu będzie migać) a następnie w zależności od pozycji wybrać przycisk „OPEN/OFF” lub „CLOSE/ON”.

Przy pierwszej próbie wysłania komendy C264 zapyta o hasło (logowania) – naciskamy wówczas „ENTER” (jeżeli jesteśmy już zalogowani w C264 ponowne podanie hasła nie będzie wymagane).



UWAGA: Jeden użytkownik może zalogować się do urządzenia C264 tylko jeden raz. Należy o tym pamiętać, jeżeli korzysta się z oprogramowania CAT. Aby wylogować użytkownika z panelu C264 należy wybrać przycisk „HELP” – pojawi się widok serwisowy. Następnie przycisnąć „ENTER”, a dalej strzałką „góra” lub „dół” wybrać opcję „LOGOFF” i zatwierdzić „ENTER”.

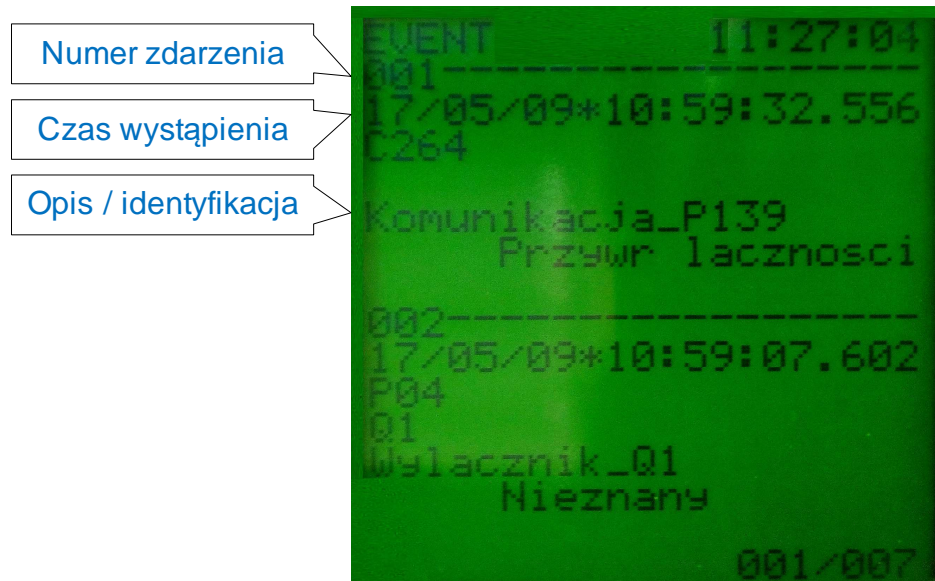


ZAŁĄCZNIK 4 – Odczyt zdarzeń

Elementy SSiN pozwalają na podgląd zdarzeń na stacji elektro-energetycznej. Rejestrują również operacje dokonywane przez użytkowników.

Oprogramowanie CAT pozwala na pobranie i zapis listy zdarzeń w postaci pliku tekstowego.

Zdarzenia można podejrzeć na panelu sterownika C264 (200 ostatnich pozycji). Do nawigacji po panelu warto wykorzystać informacje zawarte w Załączniku 3. Należy przejść do widoku zdarzeń „EVENT”. Zarejestrowane informacje są ponumerowane, najnowsze zdarzenie posiada numer 001 i znajduje się na górze listy. Można przy nim odczytać czas wystąpienia, nazwę pola, nazwę modułu, nazwę sygnału i etykietę stanu np.: „Sygnał”, „Koniec sygnału”, „Zamknięty”.



Zapisy w dzienniku zdarzeń systemu PACiS – HMI dostępne po wybraniu zakładki „Zdarzenia”.

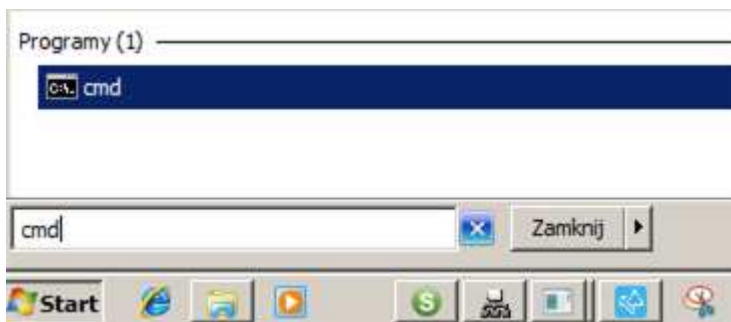
Data	Ścieżka	Opis	Komunikat	Jakość sygnału	Dyspozytor
09-05-2017 13:52:16.589	PWR_D20 / 110kV / ZS_LRW / 9_SYGN	Rezerwa5	Koniec sygnału	Prawidłowo	a (Eval License)
09-05-2017 13:52:16.589	PWR_D20 / 110kV / ZS_LRW / 9_SYGN	ZS P741/742-System 2	-	Prawidłowo	a (Eval License)
09-05-2017 13:52:16.589	PWR_D20 / 110kV / ZS_LRW / 9_SYGN	LRW P741/742- od TR1	-	Prawidłowo	a (Eval License)



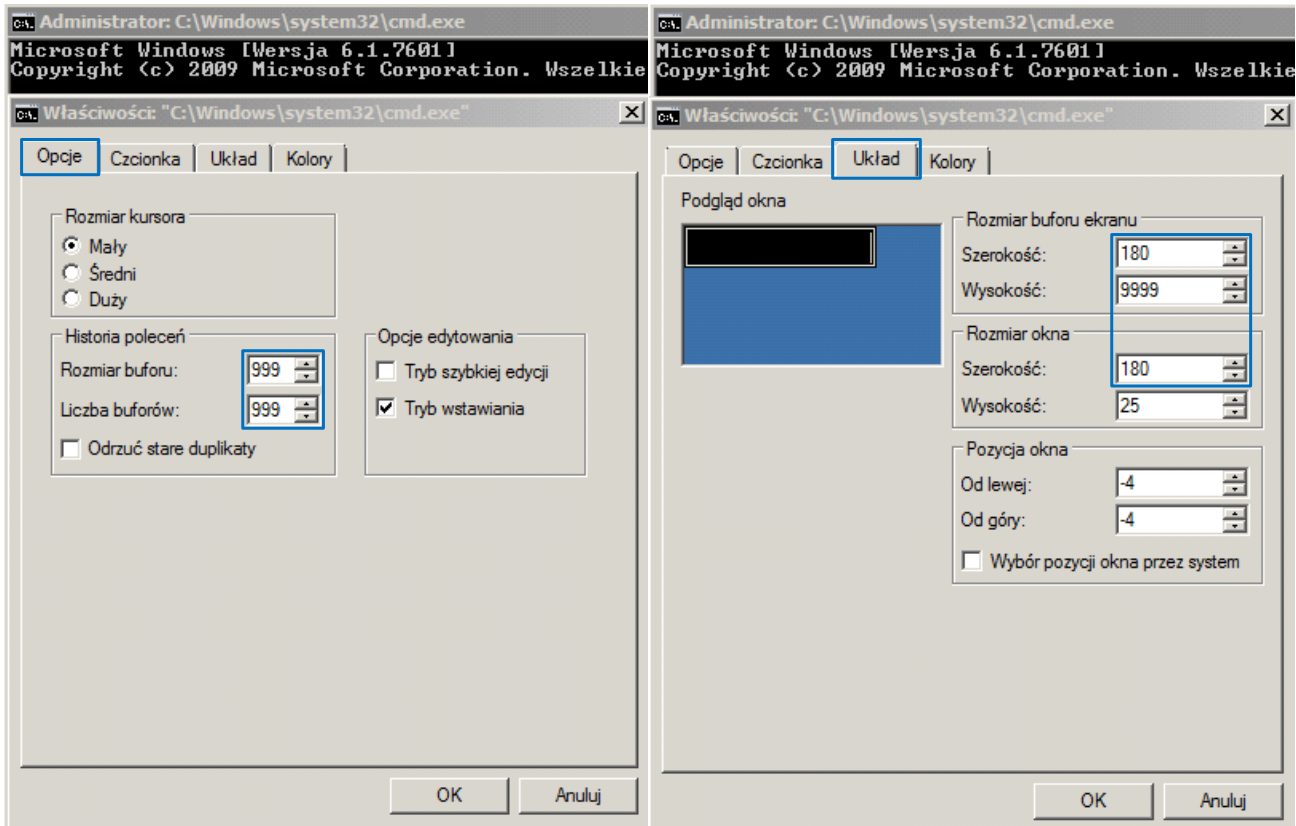
ZAŁĄCZNIK 5 – Monitorowanie portu szeregowego PC

Monitorowanie portu szeregowego C264 będzie wywołane poprzez terminal *Telnet* dostępny z poziomu komputera PC na stanowisku do ćwiczenia. W tym celu należy połączyć się ze sterownikiem i wywołać odpowiednią komendę monitora portu szeregowego.

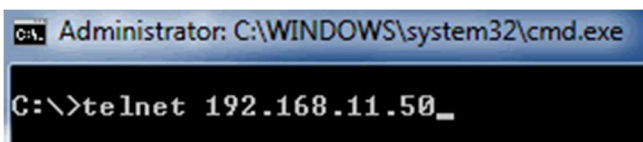
Uruchomić wiersza poleceń systemu operacyjnego Windows:



Warto zmienić „Właściwości” uruchomionego okna/programu *CMD.EXE* w celu zwiększenia bufora wyświetlanych danych:



Uruchomić usługę połączeń zdalnych – terminal *Telnet*. Otworzyć połączenie do sterownika C264. Wpisać polecenie „telnet 192.168.11.50” i potwierdzić klawiszem Enter.



UWAGA: Terminal *Telnet* przyjmuje znaki z klawiatury, nie pozwala on kopiować i wklejać ciągów znakowych, znaki przesyłane są jeden po drugim. Wszelkie komendy należy wpisać z klawiatury, a zatwierdzić klawiszem Enter.

Logowanie do sterownika :

Login: *target*

Hasło: *password*

Monitorowanie portu szeregowego:

Po połączeniu z C264, monitor portu szeregowego uruchomić za pomocą komendy:

```
traces_scc1=16
```

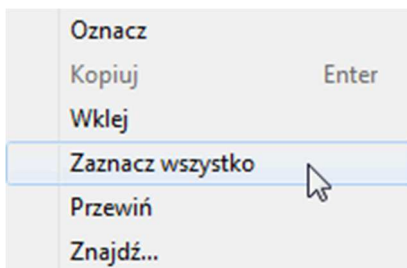
Po prawidłowym uruchomieniu komendy na ekranie terminala zaczną wyświetlać się informacje z monitora w formie tekstowej. Zwiększony bufor okna wynosi 9999 wierszy, należy zarejestrować interesujące ramki i zatrzymać monitor.

Aby zakończyć monitorowanie w oknie terminala przesyłamy komendę

```
traces_scc1=0
```

Jeżeli nie mamy pewności, że monitor się zatrzymał, komendę można powtórzyć. Warto pamiętać, że za każdym razem komendę zatwierdza się klawiszem Enter.

Po zatrzymaniu monitora, interesujące dane można skopiować poprzez edycję danych z poziomu okna aplikacji Windows. „Zaznacz wszystko” i kopiuj (klawiszem Enter), dane można wkleić w dowolnym edytorze tekstu.

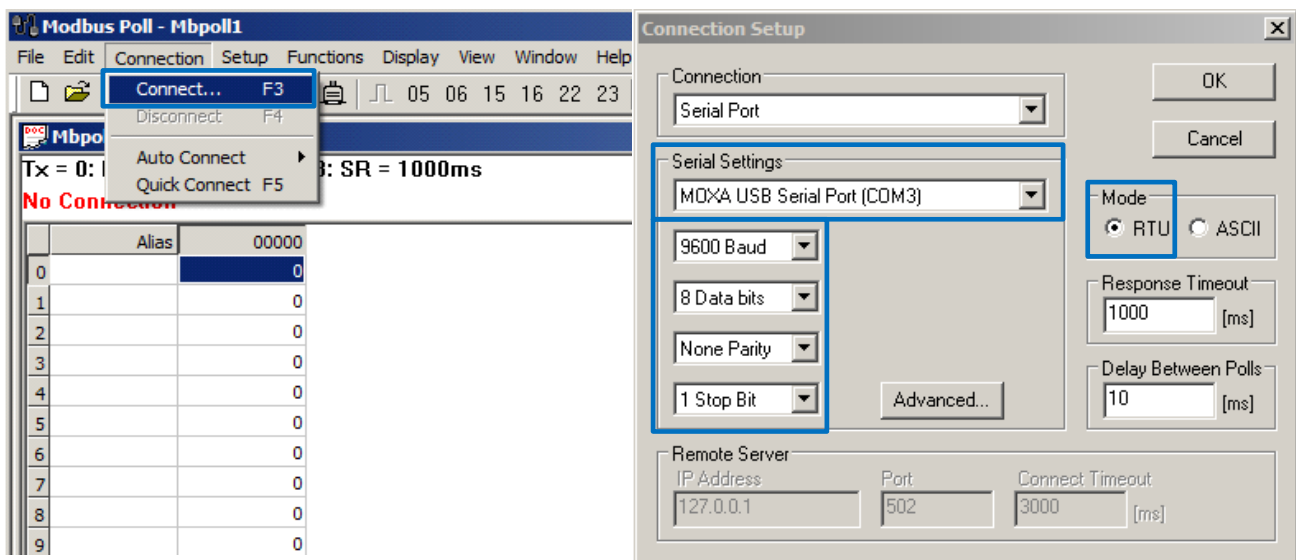




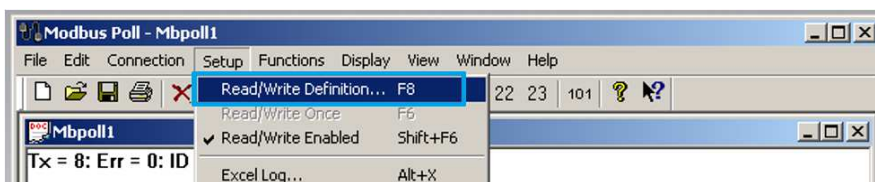
ZAŁĄCZNIK 6 – Symulacja Modbus Master

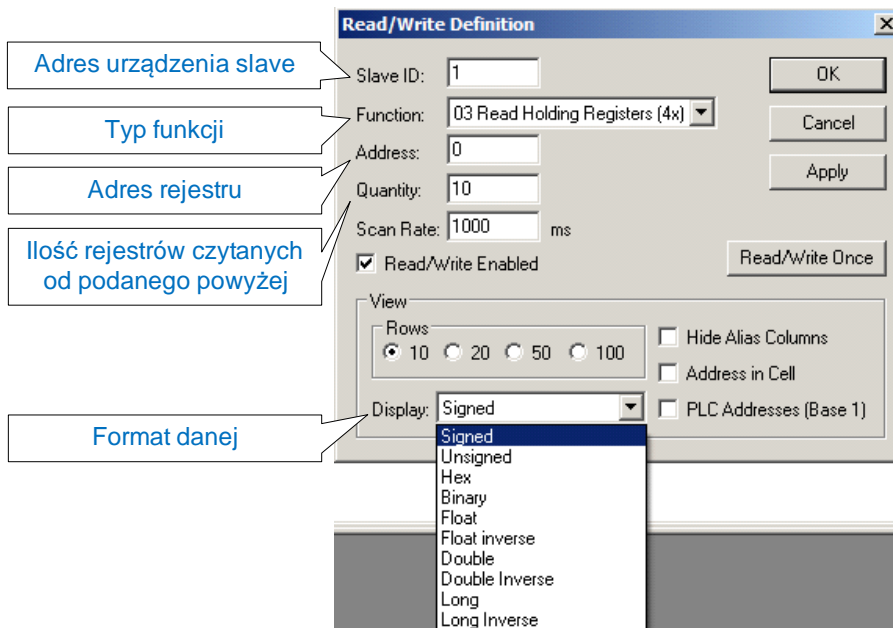
Symulacja urządzenia Master dla protokołu *Modbus* możliwa jest przez wiele dostępnych na rynku aplikacji. W ćwiczeniu wykorzystano oprogramowanie *Modbus Poll*. Aplikację można uruchomić przez dostępny skrót z poziomu pulpitu komputera PC na stanowisku do ćwiczenia.

Z menu aplikacji wybrać połączenie, wprowadzić parametry komunikacji jak na załączonym rysunku:



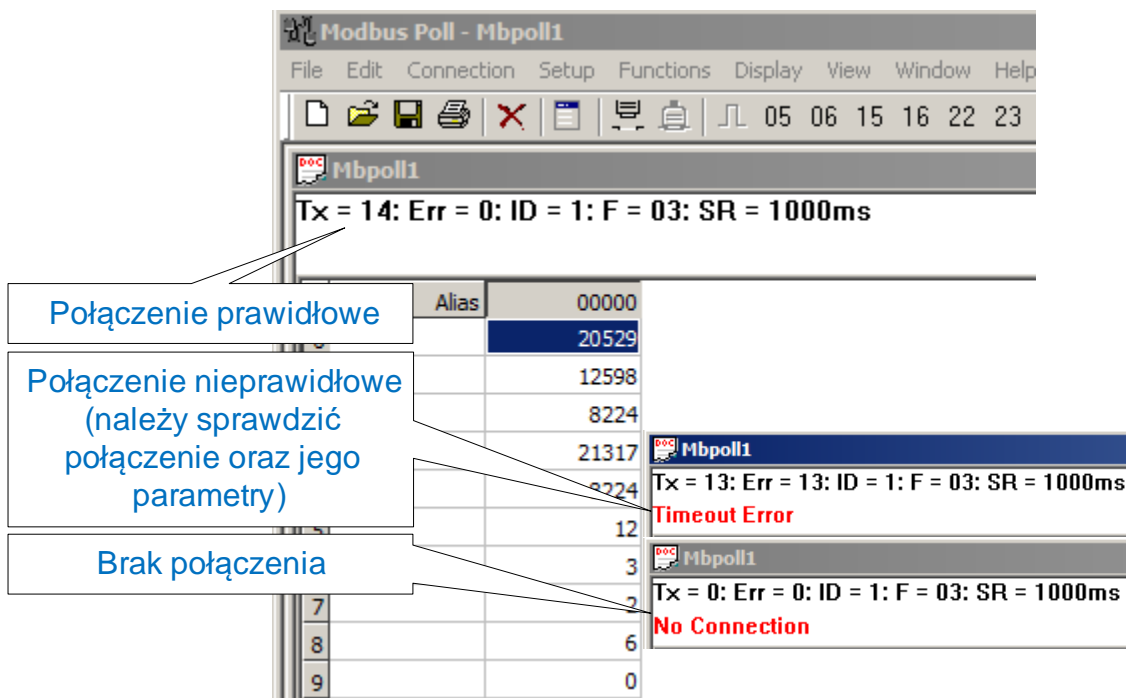
Następnie zdefiniować parametry ramki zapytania przesyłanej przez Master:



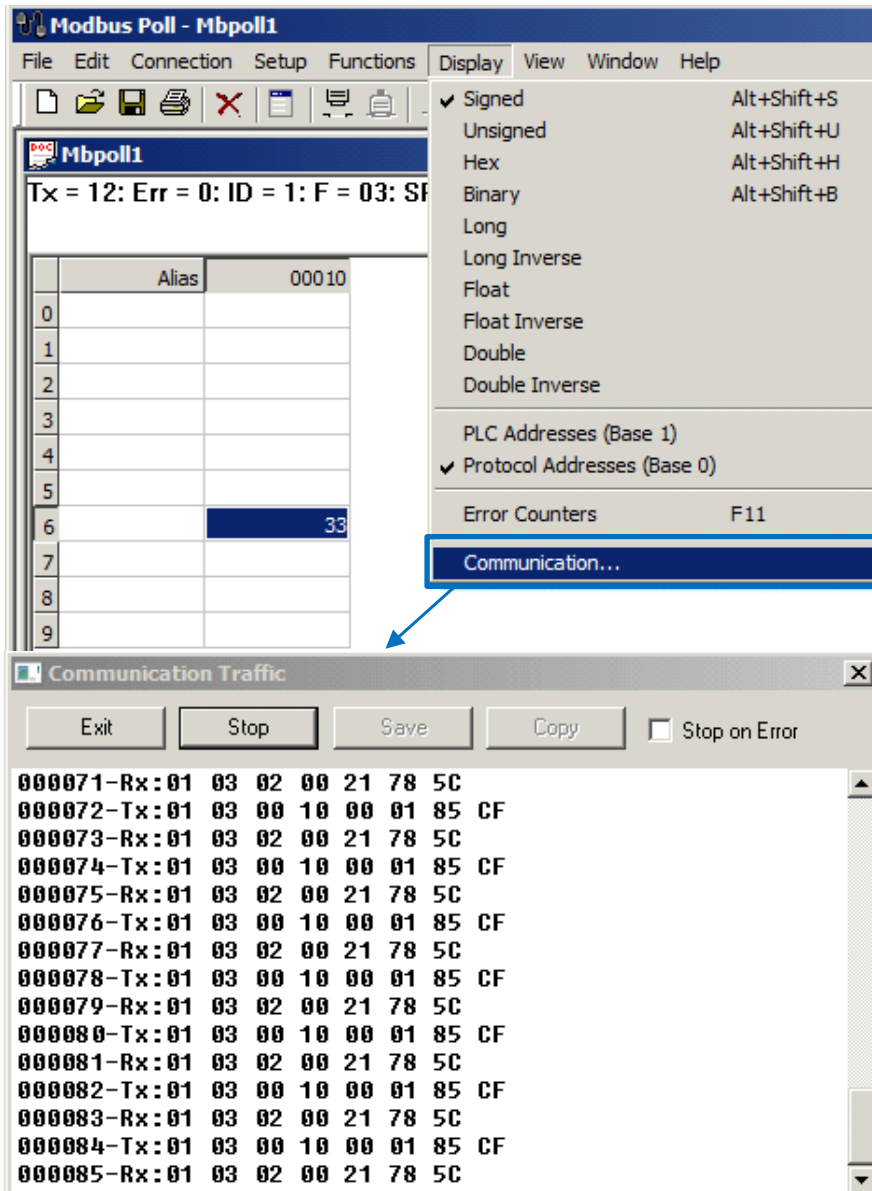


Jeśli odczyt dotyczy stanów statycznych to format danych można wyświetlić w postaci „Binary”.

Prawidłowe połączenie można zweryfikować jak na rysunku poniżej:



Podgląd przesłanych i odebranych komunikatów można uruchomić z poziomu menu „Display”:



Przyciskiem „STOP” można zatrzymać monitor, a interesujące dane skopiować (ctrl+c) i dalej wkleić w dowolnym edytorze tekstu.