ĆWICZENIE 5

Brama dostępowa – komunikacja (po protokole DNP3) ze zdalnym Centrum Nadzoru

Politechnika Wrocławska – Laboratorium systemowe

Nazwa dokumentu : **REF-PW-LAB_CW5**

Numer referencyjny : REF/PW/LAB/2017/07/18

Wersja : B1

Data : 2017-09-07

ZATWIERDZONY PRZEZ	DATA	WERSJA	KOMENTAŻ
Leszek Suchodolski	*2017-07-18*	*A*	*Pierwsza wersja ćwiczenia*
Kamil Sokołowski	*2017-09-07*	*B1*	*Korekta edytorska*
Dariusz Radomski			

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 Mikolow, Poland
Share capital: 43,031,400.00 PLN
Registry Court: Sad Rejonowy Katowice-Wschod,
VIII Wydzial Gospodarczy KRS; KRS No.: 0000202164
Tax ID No.: PL 8840007793, REGON: 890006542

SPIS TREŚCI

1. ZAKRES ĆWICZENIA

W ćwiczeniu studenci mają okazję zapoznać się z komunikacją cyfrową między zabezpieczeniem elektro-energetycznym P127 (komunikacja za pośrednictwem sterownika C264), komputerem klasy PC pełniącym funkcję Gateway (Bramy Dostępowej) oraz komputerem klasy PC pełniącym funkcję zdalnego centrum nadzoru. Student będzie mógł prześledzić przesyłanie i wymianę informacji począwszy od urządzeń nadzorujących pracę obwodów pierwotnych (zabezpieczenia) po centra dyspozytorskie (człowiek nadzorujący pracę stacji elektroenergetycznej).

Studenci zapoznają się z protokołem komunikacyjnym DNP3 oraz ze sposobem parametryzacji ustawień komunikacyjnych urządzeń, biorących udział w wymianie danych.

Zakres ćwiczenia obejmuje obserwację wymiany danych między symulatorem systemu SCADA (oprogramowanie Axon TEST) i aplikacją Gateway - symulacja łącza stacji elektroenergetycznej i centrum nadzoru (komunikacja po protokole DNP3). Oraz obserwację wymiany danych między aplikacją Gateway i urządzeniem IED (ang. Intelligent Electronic Device) – symulacja komunikacji wewnątrz stacji elektroenergetycznej.

Zakres prac:

- weryfikacja połączeń elektrycznych i parametrów komunikacyjnych urządzeń na stanowisku do ćwiczeń,
- wymuszanie zmian stanów wejść i sygnałów logicznych rejestrowanych przez urządzenie IED,
- obserwacja zdarzeń/sygnalizacji wysyłanych przez IED poprzez aplikację Gateway do zdalnego centrum nadzoru (SCADA)
- obserwacja komend sterowania wysyłanych przez zdalne centrum nadzoru (SCADA) poprzez aplikację Gateway do IED
- analiza ramek protokołu DNP3 dla stanów statycznych, pomiarów i sterowań
- sporządzenie sprawozdania z przebiegu ćwiczenia,

Celem ćwiczenia jest:

- zapoznanie studentów z protokołem komunikacyjnym DNP3.0
- zapoznanie z analizą ramek wymienianych między urządzeniami podczas komunikacji,
- zapoznanie z ogólnym zastosowaniem konwerterów protokołów i zastosowaniem bramy dostępowej Gateway

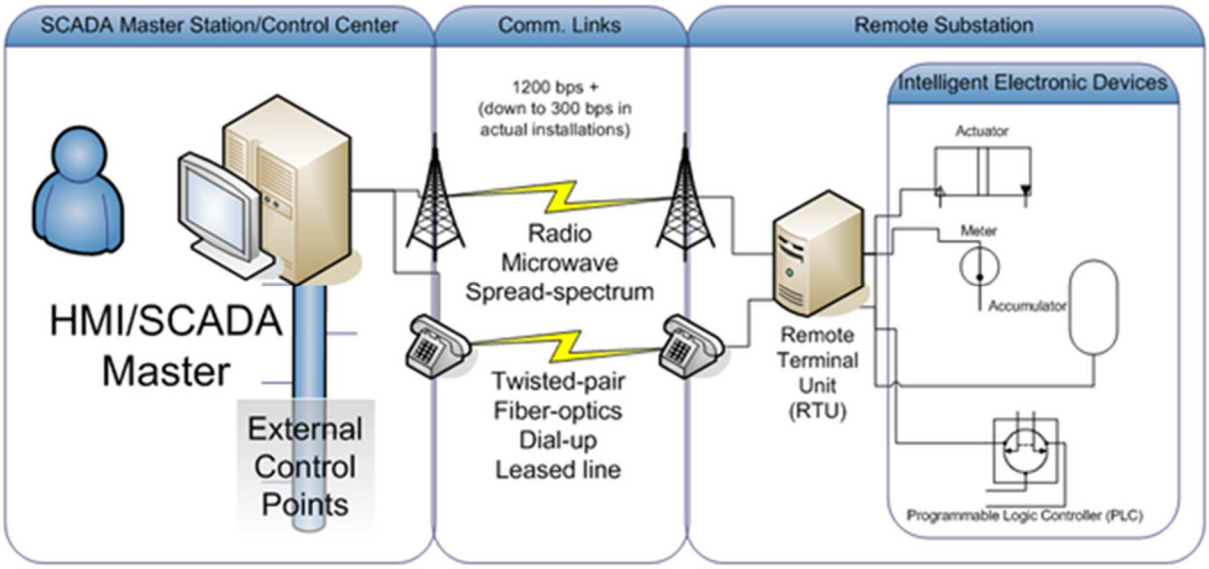
2. WPROWADZENIE TEORETYCZNE

Transmisja szeregowa to jeden z najstarszych i najtańszych sposobów na przesyłanie danych między urządzeniami. Zaletą transmisji szeregowej jest to, że większość urządzeń nie wymaga dodatkowych specjalistycznych modułów lub oprogramowania (standardowa dostępność interfejsu RS232 oraz aplikacji typu terminal w każdym komputerze klasy PC). Ponadto powszechna dostępność konwerterów RS232/RS485 pozwala na elastyczne budowanie złożonych układów połączeń szeregowych wielu urządzeń – tzw. magistrale komunikacyjne.

Protokół komunikacyjny to zbiór zasad dotyczących sposobu transmisji oraz interpretacji danych wymienianych między urządzeniami. Aby zapewnić poprawność wymiany danych oraz ich zrozumienie urządzenia biorące udział w wymianie danych muszą mieć zbiór tych zasad (czyli protokół) zaimplementowany w jednakowy sposób – mówimy wtedy o zgodności protokołów. Na rynku istnieje wiele standardów/protokołów, których powstawanie, na przestrzeni ostatnich 40 lat, spowodowane było ciągłym rozwojem technologii komputerowych, chęcią doskonalenia procesów przesyłania danych oraz zwiększanie niezawodności i bezpieczeństwa przesyłu danych.

DNP3 (ang. Distributed Network Protocol version 3) to obecnie jeden z najczęściej stosowanych protokołów szeregowych w krajowych (polskich) systemach elektroenergetycznych. Ideą przyświecającą twórcom protokołu było stworzenie otwartego standardu zapewniającego współpracę/zgodność standardów komunikacyjnych komputerów stacyjnych (lokalnych i zdalnych stanowisk dyspozytorskich HMI, SCADA), RTU (koncentratorów danych) oraz IED (zabezpieczeń elektroenergetyczne). Protokół DNP3 powstał na bazie protokołu/standardu IEC60870-5 i opracowała go w 1993 roku Kanadyjska firm GE-Harris. DNP3 wciąż pozostaje standardem otwartym.

Poniższy Rys. 1 przedstawia ogólną koncepcję komunikacji pomiędzy stacją elektroenergetyczną, a zdalnym stanowiskiem dyspozytorskim za pośrednictwem koncentratora danych, którym w tym przypadku jest RTU. Łączami komunikacyjnymi mogą być linie telefoniczne (komutowane/dzierżawione) lub fale radiowe/komunikacja bezprzewodowa.



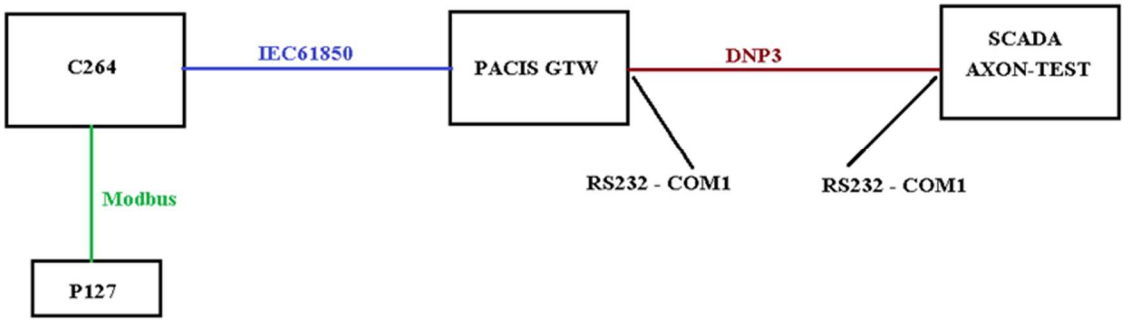
Rys. 1 Przykładowy[1] schemet komunikacji między stacją a dyspozytornią

2.1. Stanowisko pracy – układ połączeń

Stanowisko laboratoryjne składa się z zabezpieczenia elektroenergetycznego wyposażonego w moduł komunikacji szeregowej (model P127) oraz dwóch komputerów klasy PC pełniących funkcje:

- Gateway – odpowiedzialnego za transmisje danych ze stacji do zdalnego centrum nadzoru, system SCADA),
- Zdalnego centrum nadzoru – stanowisko dyspozytorskie SCADA (zdalne sterowania oraz odczyt danych ze stacji za pośrednictwem Gateway)

Na rysunku Rys. 1 przedstawiono schemat prawidłowego połączenia pomiędzy urządzeniami. Komputery PC połączone są ze sobą przewodem krosowanym RS232 poprzez porty szeregowe COM1 w obu urządzeniach.



Rys. 2 Układ laboratoryjny - schemat połączeń

[1] Rysunek zaczerpnięty ze stron wikipedia.org

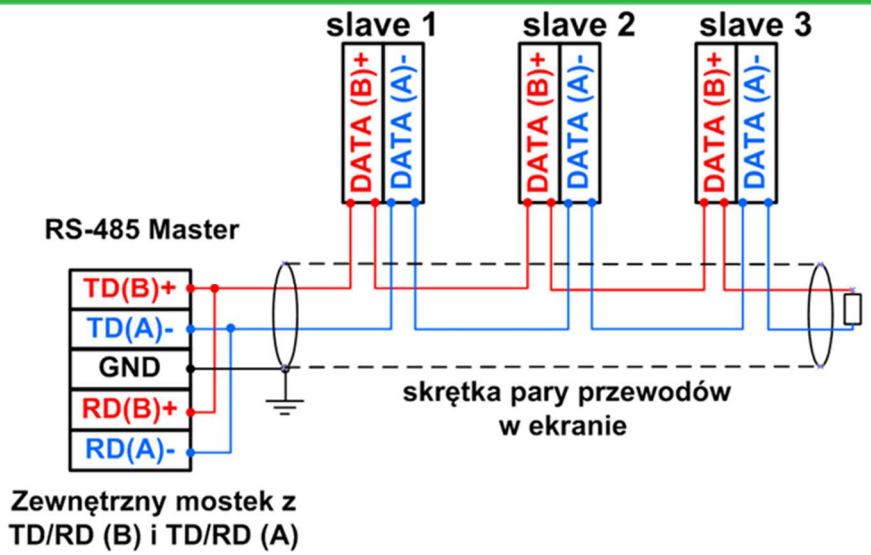
Za pomocą Rys. 2 można zweryfikować połączenia elektryczne między elementami ćwiczenia. Na rysunku Rys. 3 znajduje się fragment DTR (Dokumentacji Techniczno-Ruchowej) dla urządzeń P127. IED P127 jest połączone z C264 łączem RS485 w protokole Modbus, w układzie tym C264 pełni tu rolę konwertera protokołów. C264 jest również serwerem danych dla klienta PACIS Gateway w standardzie IEC61850.

Input 7 + terminal	57	58	Input 6 + terminal	Output 5	1	2	Common output 1	Case earth connection	29	30	Terminal RS485
Input 7 – terminal	59	60	Input 6 – terminal	Common output 5	3	4	Output 1 (NC)	RS485 - terminal	31	32	RS485 +
Input 8 + terminal (1)	61	62	Input COM – terminal (1)	Output 6	5	6	Output1 (NO)	Vaux + terminal	33	34	Vaux – terminal
Input A + terminal (1)	63	64	Input 9 + terminal (1)	Common output 6	7	8	Common output 2	Relay failed (WD)	35	36	Common "Watchdog"
Input C + terminal (1)	65	66	Input B + terminal (1)	Common output 7	9	10	Output 2 (NC)	Relay healthy (WD)	37	38	
Current I1 (3) meas. 1A/5A	67	68	Current I1 (3) meas. 1A/5A	Output 7	11	12	Output 2 (NO)		39	40	
Voltage input VA	69	70	Voltage input VA	Common output 8	13	14	Output 3	Current input IA (5A)	41	42	Current input IA (5A)
Voltage input VB	71	72	Voltage input VB	Output 8	15	16	Common output 3	Current input IB (5A)	43	44	Current input IB (5A)
Voltage input VC/Vr	73	74	Voltage input VC/Vr	Input 3 + terminal	17	18	Output 4	Current input IC(5A)	45	46	Current input IC(5A)
Current I2 (3) meas. 1A/5A	75	76	Current I2 (3) meas. 1A/5A	Input 3 – terminal	19	20	Common output 4	Current input Ie (5A)	47	48	Current input Ie(5A)
Case earth connection(2)	77	78	RS485-2 term. Z (2)	Input 4 + terminal	21	22	Input 1 + terminal	Current input IA (1A)	49	50	Current input IA (1A)
RS485-2 – terminal (2)	79	80	RS485-2 + terminal (2)	Input 4 – terminal	23	24	Input 1 – terminal	Current input IB (1A)	51	52	Current input IB (1A)
IRIG-B mod – terminal (2)	81	82	IRIG-B mod + terminal (2)	Input 5 + terminal	25	26	Input 2 + terminal	Current input IC (1A)	53	54	Current input IC (1A)
IRIG-B dem – terminal (2)	83	84	IRIG-B dem + terminal (2)	Input 5 – terminal	27	28	Input 2 – terminal	Current input Ie (1A)	55	56	Current input Ie (1A)

Rys. 3 Wycinek DTR dla P127

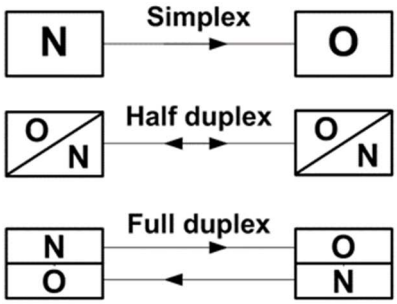
2.2.Transmisja szeregowa

W rzeczywistych rozwiązaniach stacyjnych połączenia szeregowe między urządzeniami realizowane jest zazwyczaj zgodnie ze standardem RS-485 (ang. Recommended Standard). Prawidłowe połączenie elektryczne zaprezentowano na Rys. 4. Urządzenie pracujące w charakterze Gateway i/lub RTU określane jest jako Master, a pozostałe urządzenia to Slave.



Rys. 4 RS-485 układ dwuprzewodowy z wieloma odbiornikami

W połączeniach szeregowych rozróżniamy następujące typy transmisji pomiędzy nadajnikiem i odbiornikiem:
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. 5 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 parzystość – 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	
		odd	*even*
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.Model ISO-OSI

Protokół DNP3 wykorzystuje (w ograniczonym zakresie) model OSI, który:

- organizacja ISO rozpoczęła opracowywać w 1977 roku
- jest akceptowany i powszechnie stosowany w celu przedstawienia i zrozumienia komunikacji między urządzeniami w sieci
- definiuje siedem warstw i opisuje jakie zadania każda z warstw powinna pełnić w procesie wymiany danych między urządzeniami

Modeli OSI definiuje następujące warstwy:

OSI Model		
Layer		Protocol Data unit (PDU)
Host Layers	7. Application	Data
	6. Presentation	
	5. Session	
	4. Transport	Segment datagram (TCP), Datagram (UDP)
Media Layers	3. Network	Packet
	2. Data link	Frame
	1. Physical	Bit

Tab. 2 Model OSI

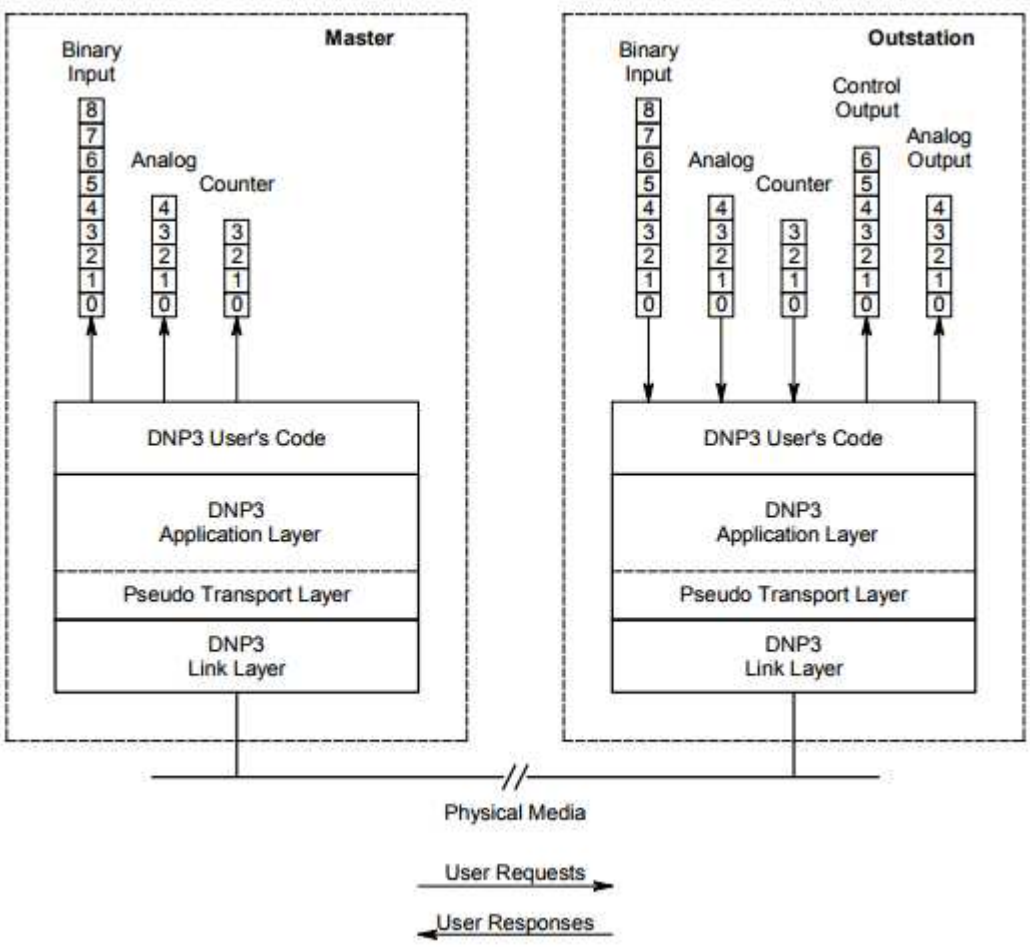
Funkcje warstw są następujące (każda z warstw działa dwukierunkowo tzn. współpracuje z sąsiednimi warstwami w sposób zależny od kierunku przepływy danych):

- Warstwa Fizyczna (ang. Physical Layer) - przejmuje dane (w postaci ramek) z warstwy łącza danych i przesyła je bit po bicie przez medium transmisyjne (przewody, światłowody, fale radiowe) do odbiorcy, oraz z drugiej strony, przyjmuje strumienie bitów i przekazuje je do Warstwy Łącza Danych w postaci ramek. Medium transmisji bitów jest często nazywane Warstwą Zerowa.
- Warstwa Łącza Danych (ang. Data Link Layer) - odpowiada za kontrolę spójność i zgodność danych nadawanych i odbieranych poprzez m.in. dodawanie (przy wysyłaniu) i kontrolę (przy odbieraniu) bajtów CRC – bajty CRC (ang. Cyclic Redundancy Check – cykliczny kod nadmiarowy) służą kontroli/weryfikacji poprawności transmitowanych danych. Warstwa Łącza Danych odpowiada za składanie strumienia bitów danych (odbieranych przez Warstwę Fizyczną) i przesłanie ramek do warstwy wyższej oraz z drugiej strony za odbiór pakietów danych z warstw wyższych i przekazanie ich do Warstwy Fizycznej w celu ich wysłania. Warstwa Łącza Danych w protokole DNP3 posiada własny 10 bajtowy nagłówek (dokładany do danych otrzymanych z warstw wyższych).
- Warstwa Sieciowa (ang. Network Layer) – odpowiedzialna jest za ze kierowanie przepływem pakietów w sieci. Zapewnia ona, że pakiety przesyłane między komputerami nie łączącymi się bezpośrednio, będą przekazywane z urządzenia na urządzenie, aż osiągną adresata. Proces znajdowania drogi w sieci nazywa się rutowaniem (routing). Warstwa ta nie posiada żadnych mechanizmów wykrywania oraz korygowania błędów transmisji pakietów.
- Warstwa Transportowa (ang. Transport Layer) – odpowiedzialna jest m.in. za zapewnienie niezawodnej komunikacji pomiędzy urządzeniami dbając o to, aby odbiorca dostawał pakiety w tej samej kolejności w jakiej nadawca je wysyła. Warstwa Transportowa w protokole DNP3 posiada własny 1 bajtowy nagłówek (dokładany do danych otrzymanych z warstw wyższych) – jest to tzw. Warstwa „pseudo" Transportowa z uwagi na to, że jej głównym zadaniem jest segmentacja i desegmentacja długich ramek warstwy aplikacji dostosowując długość poszczególnych segmentów do wymagań standardu (szczegóły poniżej).

- Warstwa Sesji (Session Layer) – odpowiedzialna jest za kontrolę nawiązywanie i zrywanie połączenia przez aplikacje.
- Warstwa Prezentacji (Presentation Layer) - odpowiedzialna jest za zarządzanie sposobami kodowania nadawanych/odbieranych danych zapewniając w ten sposób wzajemne dopasowanie sposobów ich reprezentacji, a w konsekwencji wzajemne zrozumienie komunikujących się aplikacji. Warstwa prezentacji rozwiązuje takie problemy jak: niezgodność reprezentacji liczb, znaków końca wiersza, liter narodowych, itp. Przykładową funkcją realizowaną przez tą warstwę jest kompresja przesyłanych danych, pozwalająca na zwiększenie szybkości transmisji informacji.
- Warstwa Aplikacji (Application Layer) – ma różnorodne zastosowania a jej głównym celem jest dostarczenie danych końcowemu użytkownikowi lub też pobranie do niego danych do przetworzenia i wysłania. Warstwa Aplikacji w protokole DNP3 posiada własny x bajtowy nagłówek (jego długość zależy od kierunku transmisji danych) informujący o formacie nadawanych/odbieranych danych.

Organizacja IEC (ang. International Electrotechnical Commission) specyfikuje uproszczony model, zawierający jedynie Warstwę Fizyczną, Warstwę łącza Danych oraz Warstwę Aplikacji. Taki uproszczony model nosi nazwę EPA (ang. Enhanced Performance Architecture) i został on wykorzystany przy tworzeniu specyfikacji protokołu DNP3. Specyfikacja Protokołu DNP3 przewiduje jeszcze jedną warstwę - Warstwę Pseudo-transportową. Przedrostek „pseudo" wynika z faktu, że w protokole DNP3 warstwa ta realizuje jedynie niewielki zakres funkcji przewidziany dla Warstwy Transportowej w modelu ISO-OSI.

W uproszczony sposób komunikację w protokole DNP przedstawia Rys. 6 (jak widać bazy danych w urządzeniu Master i Outstation nie są i nie muszą być jednakowe, ważne jest natomiast aby obiekty o które pyta lub którymi steruje Master występowały w Outstation):



Rys. 6 Uproszczony schemat komunikacji DNP3.0[2]

2.4.Warto wiedzieć i zapamiętać

Warto wiedzieć/pamiętać, że:

- Protokół komunikacyjny umożliwia wymianę danych między wieloma urządzeniami z wykorzystaniem jednego łącza fizycznego (tzw. magistrala komunikacyjna przewód, światłowód) lub bezprzewodowego (fale radiowe)
- Master, to urządzenie kontrolujące i inicjujące wymianę informacji; w transmisji szeregowej na jednym łączu danych występuje tylko jeden Master,
- Slave to urządzenie posiadające dane, potrafi ono reagować na pytania/ramki przesłane przez urządzenie Master; na jednym łączu może być wiele urządzeń typu Slave
- odległość urządzeń Slave od Master'a oraz ich ilość (podłączona jednocześnie do magistrali komunikacyjnej) zależy m.in. od prędkości transmisji i od warunków w jakich urządzenia pracują, ale przyjmuje się, że odległość nie jest większa niż 1,2 km a maksymalna ilość urządzeń to 32.

[2] Rysunek pochodzi z dokumentacji standardu DNP3.0

- Protokół DNP3 wykorzystuje trzy z siedmiu warstw Modelu ISO-OSI – Warstwa Łącza Danych, Warstwa Transportowa oraz Warstwa Aplikacji. Każda z tych trzech warstw uzupełnia dane wymieniane między aplikacjami o własne dane, które służą do sterowania i kontroli przepływu danych.
- Protokół DNP3 występuje również w wersji sieciowej tzn. ramki tego protokołu przesyłane są nie po łączu szeregowym (RS232/485) ale po łączu Ethernet'owym; mówimy wówczas o protokole „DNP3 over TCP/IP" (TCP i IP to protokoły sieciowe)
- ISO to organizacja – ang. International Standard Organization
- OSI to model – ang. Open Systems Interconnection
- "Ramka" protokołu komunikacyjnego to pojęcie określające uporządkowany ciąg bajtów zawierających zarówno dane użytkownika, informacje sterujące przepływem danych oraz bajty kontrolne służące weryfikacji poprawności przesyłanych danych.
- Ramka protokołu DNP3 jest ramką typu FT3 (opisaną w normie IEC 870-5-1 Transmission Frame Format), która posiada nagłówek o stałej długości oraz opcjonalne bloki danych użytkownika; każdy blok danych jest uzupełniany o 2 bajtowe CRC; nagłówek posiada dwa bajty startowe, jeden baj zawierający informację o długości danych, jeden bajt kontrolny oraz adres nadawcy (user data) i odbiorcy.

2.5.Protokół komunikacji DNP3 – informacje praktyczne

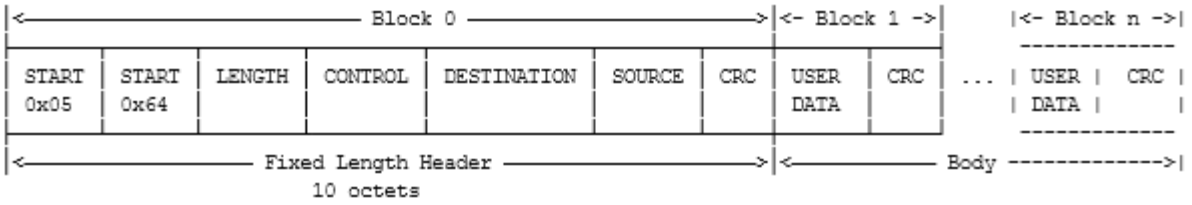
Pełna specyfikacja protokołu dostępna jest w Internecie. Istnieją liczne organizacje zajmujące się propagowaniem w Internecie wiedzy o tym protokole jak np.: *www.dnp.org*. Rozdział ten przybliża jedynie bardzo podstawowe dane na temat protokołu i jego praktycznego zastosowania w ćwiczeniu. Niektóre istotne z punktu widzenia specyfikacji protokołu DNP3 zagadnienia zostaną pominięte z uwagi na fakt, że specyfikacja ta jest bardzo obszerna, a celem ćwiczenia jest jedynie zapoznanie się koncepcją protokołów wielowarstwowych.

Protokół DNP3 opisany jest w czterech dokumentach:
- Data Link Layer Protocol Description – opis warstwy „łącza danych"
- Transport Functions - opis warstwy „transportowej"
- Application Layer Protocol Description - opis warstwy „aplikacji"
- Data Object Library - biblioteka obiektów

Warstwa Łącza Danych:

Warstwa Łącza Danych uzupełnia dane (USER DATA) otrzymywane z warstw wyższych (Warstwy Transportowej, Warstwy Aplikacji) o tzw. nagłówek, który ma zawsze długość 10 bajtów.

Nagłówek (Block 0) zaprezentowano na Rys. 7:



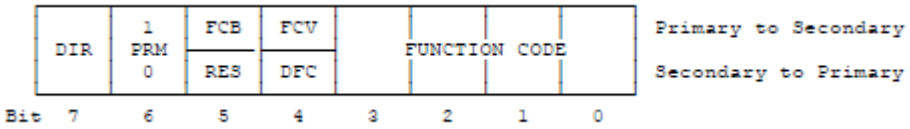
Rys. 7 Nagłówek warstwy Łącza danych dla DNP3.0[3]

gdzie:

- START - dwa bajty (two octets) startowe nagłówka zawsze 0x0564 (zapis heksadecymalny, w praktyce „0x" jest pomijane i w zapisach pojawia się jedynie 05 64) – znak rozpoznawczy protokołu DNP3.
- LENGTH – jeden bajt (one octet) określający łączną ilość bajtów danych (USER DATA) zarówno w nagłówku (Block 0) jak i we wszystkich kolejnych blokach danych (Block od 1 do n). Z nagłówka liczone są tylko bajty CONTROL, DESTINATION oraz SOURCE co daje łącznie 5 bajtów – jest to zarazem minimalna wartość jaką przyjmuje pole LENGTH nagłówka ramki i pole to ma taką wartość tylko wówczas, gdy ramka posiada sam nagłówek (tylko Block 0). Bajty CRC nie są wliczane do długości danych. Jako że pole LENGTH ma długość jednego bajta, maksymalna długość danych przesyłana w jednej ramce to 255 bajtów (2^8) w tym 5 bajtów nagłówka Warstwy Łącza Danych. W przypadku, gdy długość danych użytkownika przekracza 250 bajtów, wówczas realizowany jest proces segmentacji ramek zarówno w Warstwie Aplikacji jak i w warstwie Transportowej.
- CONTROL – jeden bajt (octet) – szczegółowy opis poniżej
- DESTINATION – dwa bajty (octets adres w postaci 0xabcd) – pole to zawiera adres odbiorcy ramki. Pierwszy bajt pola DESTINATION to mniej znaczący bajt (LSB, 0xcd) a drugi bajt to bardziej znaczący bajt (MSB, 0xab)
- SOURCE – dwa bajty (octets adres w postaci 0xabcd) – pole to zawiera adres nadawcy ramki. Pierwszy bajt pola SOURCE to mniej znaczący bajt (LSB, 0xcd) a drugi bajt to bardziej znaczący bajt (MSB, 0xab)
- CRC – dwa bajty (octets), na które składa się bardziej i mniej znaczący bajt CRC. Bajty CRC dodawane są na końcu każdego bloku danych (od 0 do n).
- USER DATA – blok danych użytkownika (Block 1 do Block n), każdy blok danych występujący po nagłówku ma długość 16 bajtów; wyjątek stanowi ostatni blok (lub pierwszy, jeżeli jest jedyny), który może mieć różną długość od 1 do 16 bajtów zależnie od potrzeb.

Pole CONTROL nagłówka Warstwy Łącza Danych ma długość jednego bajta, a jego format obrazuje Rys. 8.:

[3] Rysunek pochodzi z dokumentacji standardu DNP3.0



Rys. 8 Pole CONTROL nagłówka Warstwy Łącza Danych dla DNP3.0[4]

Bity od 4 do 7 służą do kontroli/sterowania transmisji danych. Bity od 0 do 3 zawierają kod funkcji (FUNCTION CODE). Pole CONTROL może przybierać wartości jak w Tab. 3:

Outstation to Master	Master to Outstation	Function Code Name	Type	Comment
00	80	ACK	Sec-to-Pri	
01	81	NACK		Link reset required
0B	8B	LINK_STATUS		
0F	8F	NOT_SUPPORTED		
10	90	ACK		Receive buffers full
11	91	NACK		Receive buffers full
1B	9B	LINK_STATUS		Receive buffers full
1F	9F	NOT_SUPPORTED		Receive buffers full
40	C0	RESET_LINK_STATES	Pri-to-Sec	FCB = 0 (secondary ignores FCB)
44	C4	UNCONFIRMED_USER_DATA		FCB = 0 (secondary ignores FCB)
49	C9	REQUEST_LINK_STATUS		FCB = 0 (secondary ignores FCB)
52	D2	TEST_LINK_STATES		FCB = 0
53	D3	CONFIRMED_USER_DATA		FCB = 0
60	E0	RESET_LINK_STATES		FCB = 1 (secondary ignores FCB)
64	E4	UNCONFIRMED_USER_DATA		FCB = 1 (secondary ignores FCB)
69	E9	REQUEST_LINK_STATUS		FCB = 1 (secondary ignores FCB)
72	F2	TEST_LINK_STATES		FCB = 1
73	F3	CONFIRMED_USER_DATA		FCB = 1

Tab. 3 Wartości pola CONTROL

Natomiast bity odpowiadające za kod funkcji mogą przybierać wartości jak w poniższej Tab. 4:

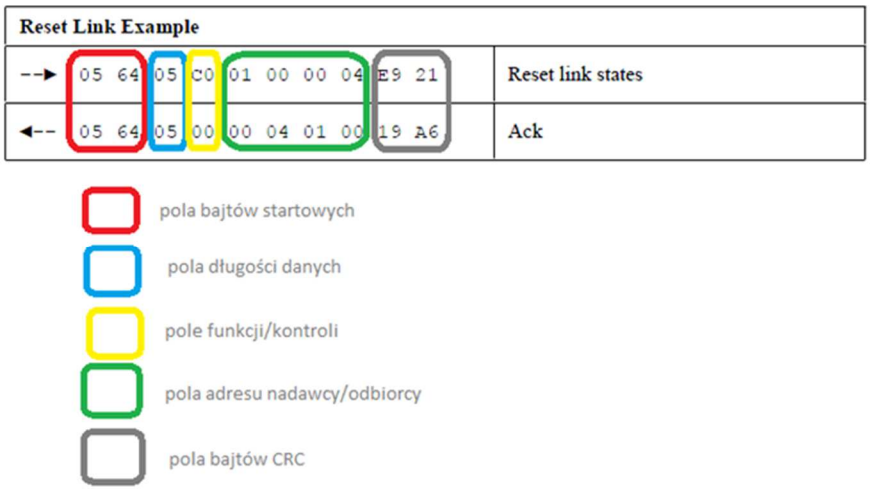
[4] Rysunek pochodzi z dokumentacji standardu DNP3.0

Primary Function Code	Function Code Name	FCV
0	RESET_LINK_STATES	0
1	-	-
2	TEST_LINK_STATES	1
3	CONFIRMED_USER_DATA	1
4	-	0
5		-
6		-
7		-
8		-
9	REQUEST_LINK_STATUS	0
A	-	-
B	-	-
C	-	-
D	-	-
E	-	-
F	-	-

Secondary Function Code	Function Code Name
0	ACK
1	NACK
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
A	-
B	LINK_STATUS
C	-
D	-
E	-
F	NOT_SUPPORTED

Tab. 4 Wartości bitów FUNCTION CODE pola CONTROL

Przykład wymiany ramek protokołu DNP3 składających się tylko z nagłówka Warstwy Łącza Danych, której celem jest reset statusu połączenia (Reset na poziomie Warstwy Łącza Danych) pokazano na Rys. 9:



Rys. 9 Ramka Reset na poziomie Warstwy Łącza Danych

Krótkie objaśnienie:
05 64 to w przypadku obu ramek bajty startowe zgodnie ze specyfikacją
05 to w przypadku obu ramek pole długości danych (5 bo jest tylko nagłówek)

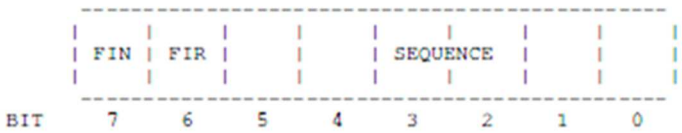
C0/00 to pola funkcji/kontroli – wykorzystano funkcje „RESET_LINK_STATES" w pierwszej ramce oraz „ACK" w drugiej ramce
01 00 00 04 to pola adresów – DESTINATION = 01 00; SOURCE = 00 04
00 40 01 00 to pola adresów – DESTINATION = 00 04; SOURCE = 01 00
E9 21 to pola CRC
19 A6 to pola CRC

Warstwa Transportowa (Pseudo-transportowa):

Warstwa Transportowa ma istotne znaczenie dla tych bloków danych (USER DATA), których długość przekracza rozmiar 249 bajtów. W takim przypadku uruchamiany jest proces fragmentacji danych, w którego prawidłowej obsłudze kluczową role odgrywa właśnie Warstwa Transportowa. Jej rolą jest podzielenie całego bloku danych na fragmenty o długości 249 bajtów każdy, przy czym ostatni fragment może mieć dowolną długość od min. 1 bajta do max. 249 bajtów. Poszczególne fragmenty są uzupełniane o 1 bajt nagłówka i przekazywane kolejno do Warstwy Łącza Danych w celu dalszego przetwarzania. W przypadku, gdy Warstwa Transportowa otrzyma wiele fragmentów z Warstwy Łącza Danych, jej rolą jest złożenie fragmentów w całość i przekazanie do Warstwy Aplikacji – procesy te to fragmentacja i defragmentacja danych użytkownika realizowane zależnie od kierunku przepływu danych.

Pojedyncza ramka w Warstwie Transportowej składa się z pól TH i USER DATA, gdzie:
TH – to jeden bajt (octet) nagłówka Warstwy Transportowej (Transport Header - opisany poniżej)
USER DATA – to ciąg max 249 bajtów danych użytkownika otrzymanych z Warstwy Aplikacji lub gotowych do przekazania do Warstwy Aplikacji

Pole TH (Transport Header) o długości jednego bajta ma następujący format:



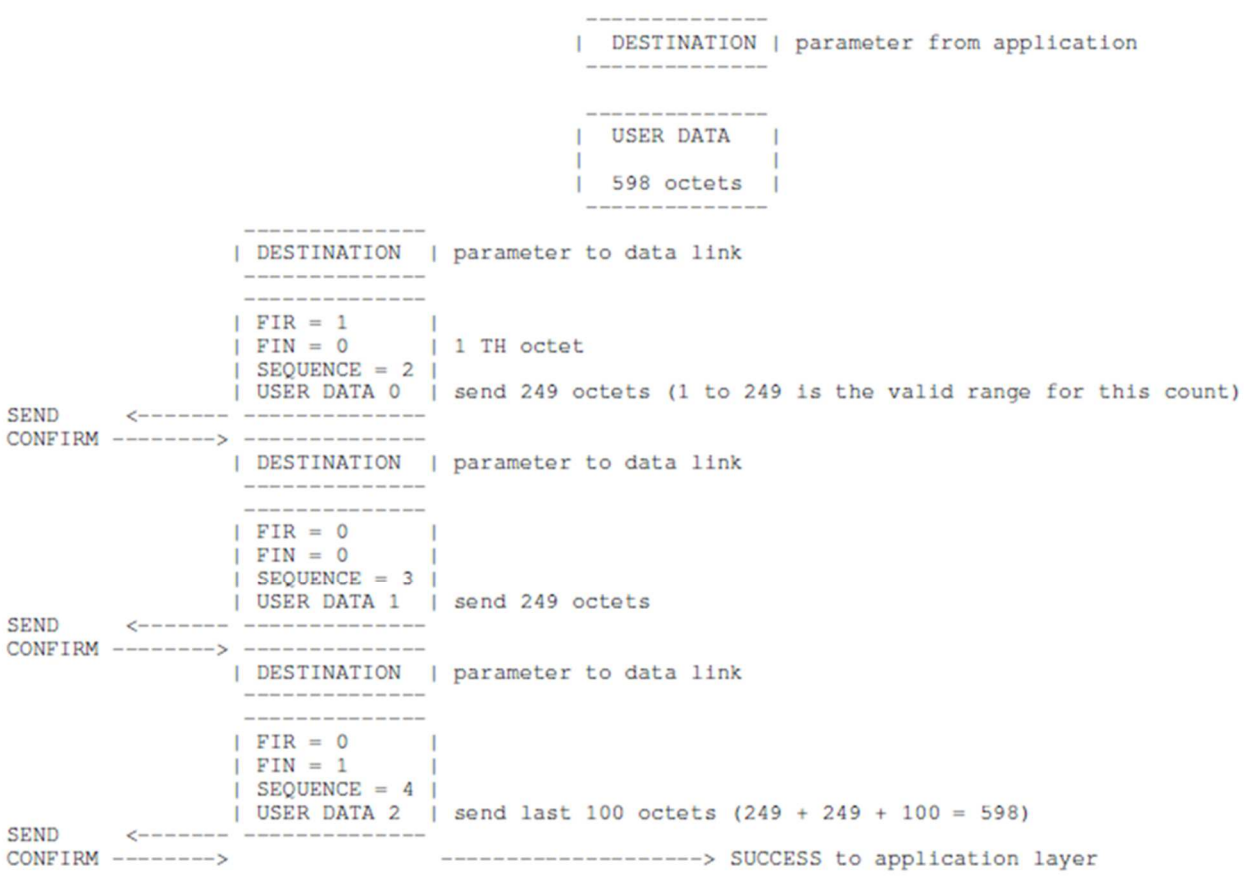
Rys. 10 Pole TH Warstwy Transportowej dla DNP3.0[5]

Bit 7 – Ustawiony, wskazuje na ostatni fragment z sekwencji ramek (lub pierwszy, jeżeli jest tylko jeden fragment). Wyzerowany bit 7 informuje o kolejnych ramkach czekających na transmisję.
Bit 6 – Ustawiony wskazuje na pierwszy fragment z sekwencji ramek. Wyzerowany bit 6 informuje, że ramka nie jest pierwszą w sekwencji ramek.
Bity od 0 do 5 – SEQUENCE – licznik ramek, inkrementowany dla każdej kolejnej ramki przetwarzanej przez Warstwę Transportową – ma wartość od 0 do 63 (po ramce nr 63 kolejna ma numer 0)
W przypadku, gdy rozmiar bloku danych (USER DATA) zawiera się w przedziale > od 1 i <

[5] Rysunek pochodzi z dokumentacji standardu DNP3.0

od 249 wówczas pola FIN i FIR mają wartość 1.

Przykład zachowania pól FIR, FIN i SEQUENCE nagłówka Warstwy Transportowej w przypadku konieczności wysłania 598 bajtów (USER DATA) zaprezentowany na Rys. 11.



Rys. 11 Pola FIR, FIN oraz SEQUENCE nagłówka Warstwy Transportowej dla DNP3.0[6]

Warstwa Aplikacji

Warstwa Aplikacji podobnie jak – poprzednio omówione warstwy – uzupełnia dane użytkownika (USER DATA) o własny nagłówek, którego długość zależy od kierunku transmisji danych (Master Station -> Outstation lub Outstation -> Master Station). Rolą nagłówka jest kontrola przepływu danych oraz fragmentacja i defragmentacja danych użytkownika. Rozróżniamy nagłówek Pytania (Request Header) oraz nagłówek Odpowiedzi (Response Header). Mają one następująca postać:

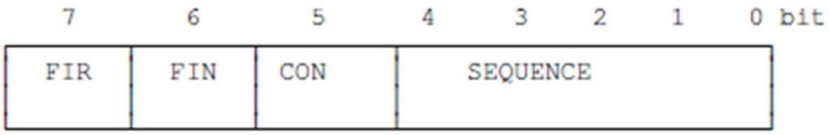
Pytanie: Application Control (AC); Function Code (FC),
Odpoweidź: Application Control (AC); Function Code (FC); Internal Indications (IIN),

Ramka odpowiedzi zawiera dodatkowe pole IIN (2 bajty, Internal Indication), które zawiera

[6] Rysunek pochodzi z dokumentacji standardu DNP3.0

informacje o statusie urządzenia wysyłającego odpowiedź.

Pole AC (Application Control) ma długość 1 bajta i strukturę podobną do nagłówka Warstwy Transportowej; format pola AC zaprezentowano na Rys. 12.

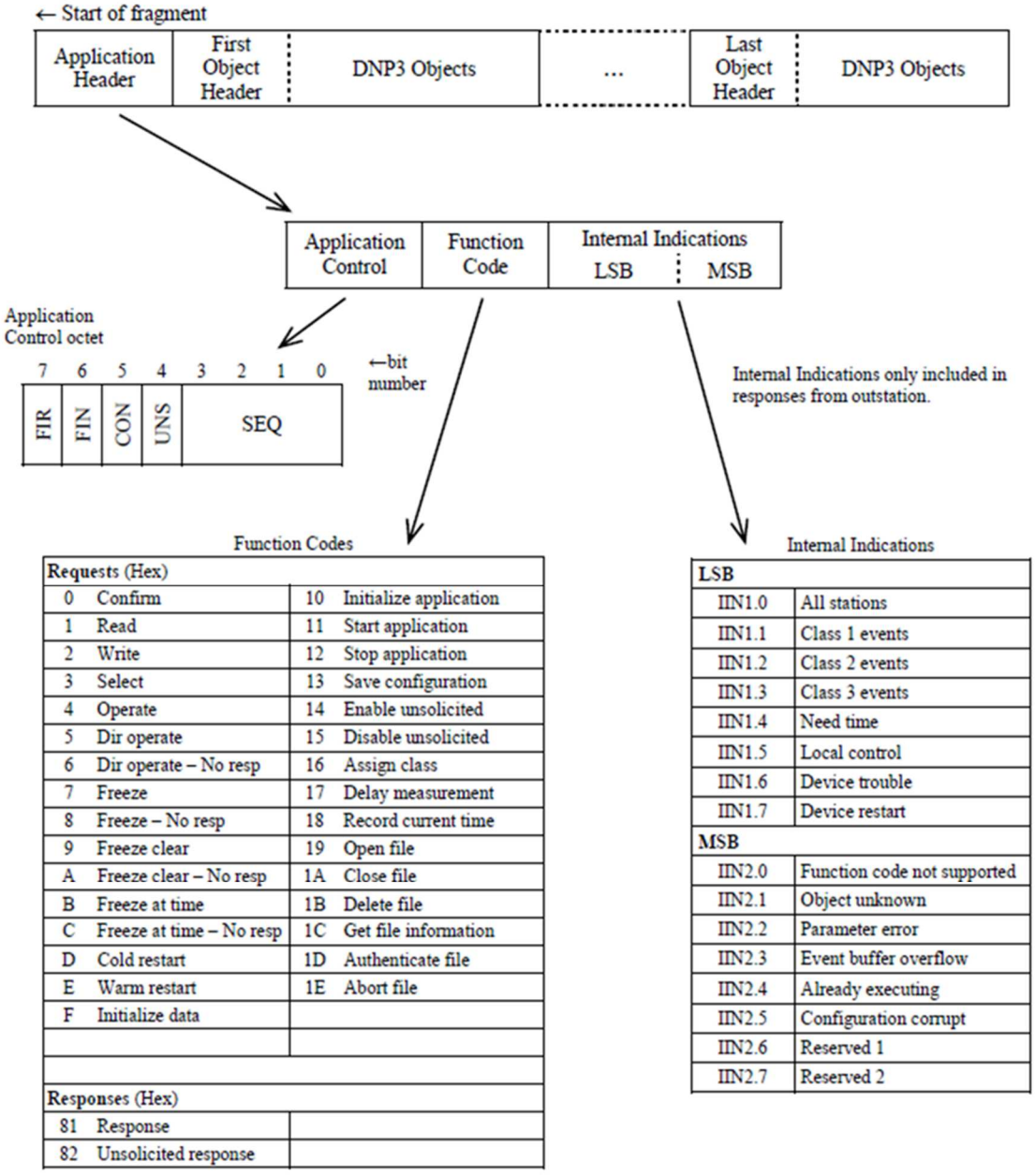


Rys. 12 Format pola Application Control (AC) dla DNP3.0[7]

Pole SEQUENCE w Warstwie Aplikacji ma 5, a nie 6 bitów jak w przypadku Warstwy Transportowej.
Pole CON – gdy bit ma wartość 1 wówczas aplikacja wysyłają dana ramkę oczekuje na potwierdzenie jej odbioru
Pole SEQUENCE przyjmuje wartości od 0 do 15 (numeracja fragmentów), jest to numeracja zarezerwowana dla wszystkich pytań wysyłanych przez Master Station oraz do wszystkich odpowiedzi wysyłanych przez Outstation. Fragmenty o numeracji od 16 do 31 zarezerwowane są dla spontanicznych ramek wysyłanych przez Outstation. Ramka spontaniczna to taka ramka, której wysyłanie nie jest skutkiem uprzedniego pytania z Master Station (są to najczęściej zdarzenia lub inne informacje, które musza być niezwłocznie dostarczone, a stosuje się ją aby ograniczyć transfer danych do niezbędnego minimum – brak ramek z pytaniami, transfer danych gdy nastąpiła zmiana).

Poniższy Rys. 13 opisuje nagłówek Warstwy Aplikacji (Application Header) oraz podaje możliwą wartość pola FC (kod funkcji) oraz pola IIN:

[7] Rysunek pochodzi z dokumentacji standardu DNP3.0



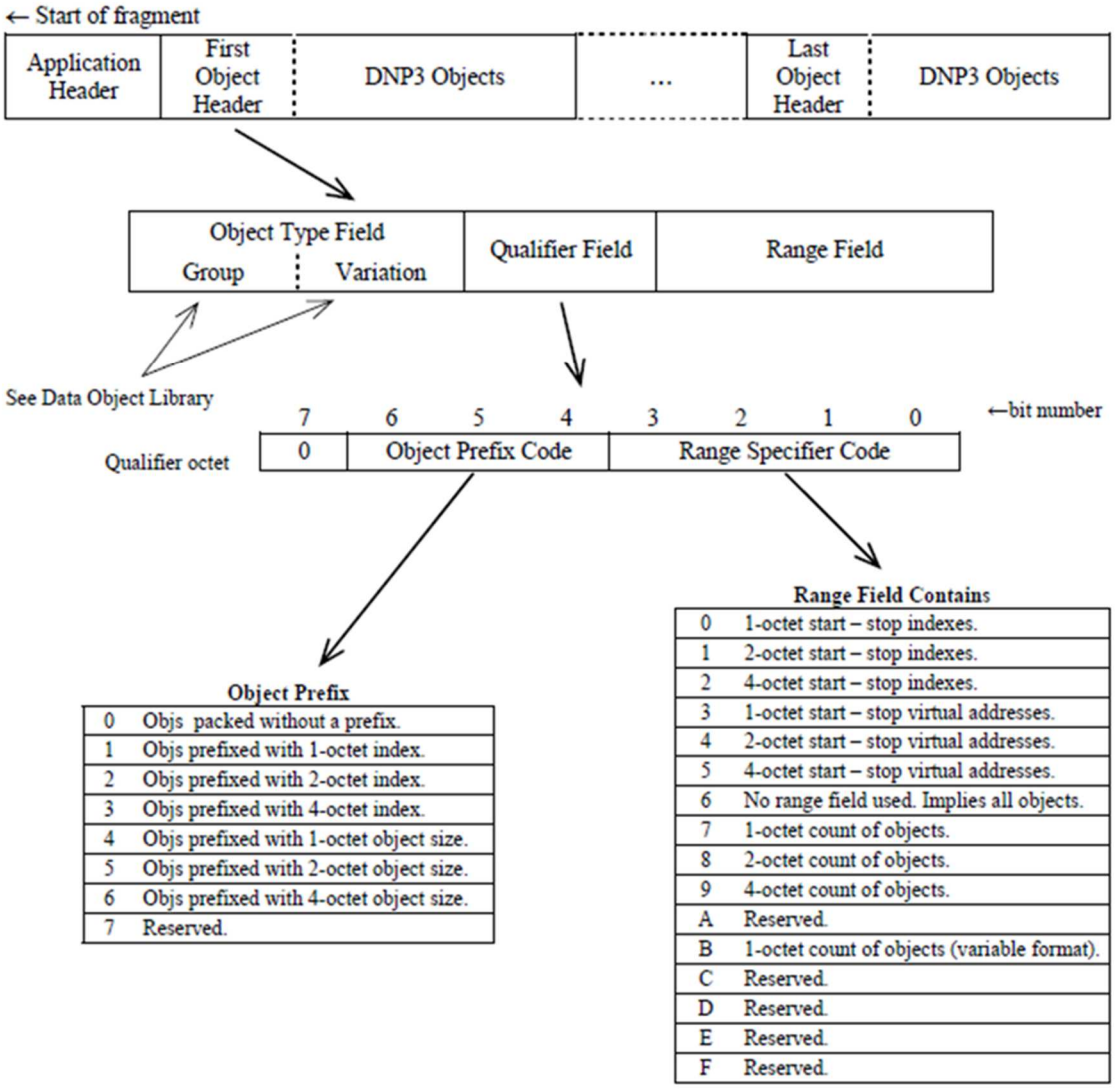
Requests (Hex)	
0 Confirm	10 Initialize application
1 Read	11 Start application
2 Write	12 Stop application
3 Select	13 Save configuration
4 Operate	14 Enable unsolicited
5 Dir operate	15 Disable unsolicited
6 Dir operate – No resp	16 Assign class
7 Freeze	17 Delay measurement
8 Freeze – No resp	18 Record current time
9 Freeze clear	19 Open file
A Freeze clear – No resp	1A Close file
B Freeze at time	1B Delete file
C Freeze at time – No resp	1C Get file information
D Cold restart	1D Authenticate file
E Warm restart	1E Abort file
F Initialize data	
Responses (Hex)	
81 Response	
82 Unsolicited response	

LSB	
IIN1.0	All stations
IIN1.1	Class 1 events
IIN1.2	Class 2 events
IIN1.3	Class 3 events
IIN1.4	Need time
IIN1.5	Local control
IIN1.6	Device trouble
IIN1.7	Device restart
MSB	
IIN2.0	Function code not supported
IIN2.1	Object unknown
IIN2.2	Parameter error
IIN2.3	Event buffer overflow
IIN2.4	Already executing
IIN2.5	Configuration corrupt
IIN2.6	Reserved 1
IIN2.7	Reserved 2

Rys. 13 Nagłówek Warstwy Aplikacji dla DNP3.0[8]

Powyższy rysunek wprowadza pole o nazwie Object Header – czyli Nagłówek Danych. W ramce Warstwy Aplikacji (USER DATA) takich Nagłówków Danych może być wiele, a ich liczba zależy od tego jakie informacje są wymieniane pomiędzy Master Station, a Outstation. Format Nagłówka Danych zaprezentowano na Rys. 14.

[8] Rysunek pochodzi z dokumentacji standardu DNP3.0



Rys. 14 Object Header w Warstwie Aplikacji dla DNP3.0[9]

Przedmiotem ćwiczenia nie jest szczegółowe zapoznanie się ze wszystkimi formatami Nagłówka Danych oraz Typami Danych określonymi przez specyfikację protokołu DNP3 i wymienianymi pomiędzy Master Station i Outstation (informacje te są dostępne w specyfikacji protokołu) – wynika to z faktu, że zarówno typów nagłówka jak i typów obiektów jest bardzo dużo. Dlatego tematyka ta będzie omówiona w dalszej części wprowadzenia jedynie na kilku przykładach.

W protokole DNP3 istnieje możliwość przesyłania danych w różnych formatach (typach obiektów). Na potrzeby ćwiczenia zamieszono poniżej jedynie kilka podstawowych/przykładowych formatów danych, a pozostałe (jest ich w sumie około 80) znajdują się w dokumencie Data Object Library będącym elementem specyfikacji protokołu. Na potrzeby ćwiczenia formaty danych dostępne w protokole DNP3 będziemy nazywali po prostu Obiekty Danych. Obiekt Danych to struktura opisująca dany obiekt

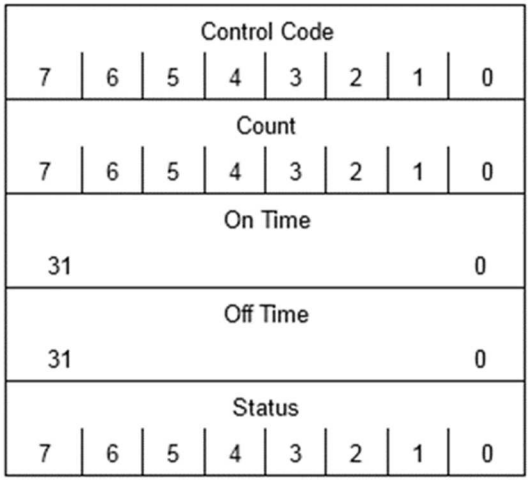
[9] Rysunek pochodzi z dokumentacji standardu DNP3.0

wraz z zestawem jego parametrów (jeżeli to konieczne). Jak pokażą poniższe przykłady istnieją zarówno bardzo proste i jak i złożone struktury w zależności od tego jaki obiekt opisują.

Obiekty w protokole DNP3 opisywane są przy pomocy dwóch atrybutów – Object Group OG (grupa) oraz Object Variations OV (wariacja). OG i OV stworzono po to aby odpowiednio pogrupować obiekty (np. pomiary, wejścia binarne, sterowania, zdarzenia, liczniki itd. Itp.) i zdefiniować ich możliwe podtypy (wariacje, np. z flagami/bez flag, z czasem/bez czasu itd. Itp.). Dokumentacja protokołu podaje te atrybuty „dziesiętnie" ale należy pamiętać, że w ramce protokołu wszystkie wartości są konwertowane na postać „heksadecymalną" stąd np. obiekt typu OG/OV=32/02 (zmiana wejścia analogowego) w ramce jest widoczny jako OG/OV=20/02.

OBIEKT DANYCH – „STEROWANIE"

W ćwiczeniu do wykonania sterowania wykorzystywany jest Obiekt Danych typu 12/01 opisany w specyfikacji DNP3 jako CONTROL RELAY OUTPUT BLOCK - CROB, dla którego ObjectGroup =12, a ObejctVariation = 01. Sposób kodowania obiektu 12/01 zaprezentowano na Rys. 15,



SQ4 {Control code = *BS8* [0..7]
Count = *UI8* [0..7] <0..255>
On-time = *UI32* [0..31] <0..2^{32}-1, ms>
Off-time = *UI32* [0..31] <0..2^{32}-1, ms>
Status = *UI7* [0..6] <0..127>
Reserved = [0..0] <0..1>
}

Control code ={
Code = *BS4* [0..3] <0..15>
Queue = *BS1* [4] <0, normal; 1, requeued>
Clear = *BS1* [5] <0, normal; 1, clear>
Trip/Close = *BS2* [6..7] <00, NUL; 01, Close; 10, Trip>
}

Rys. 15 Data Object 12/01 dla DNP3.0[10]

gdzie:
ControlCode [1 bajt] – zawiera kod funkcji sterowania
Count [1 bajt] – zawiera liczbę sterowań
On-time [4 bajty] – czas trwania stanu wysokiego impulsu sterowania wyrażony w [ms]
Off-time [4 bajty] - czas trwania stanu niskiego impulsu sterowania wyrażony w [ms]

Count: atrybut ten określa, ile razy sterowanie ma być wykonane. Jeżeli atrybut ma wartość „0" sterowanie nie będzie wykonane. Po każdym sterowaniu wartość atrybutu jest dekrementowana o „1" a gdy przyjmie wartość „0" serowanie jest traktowane jako zakończone/wykonane.

Trip/Close: Znaczenie poszczególnych bitów Control Code przedstawia Rys. 15. Istotne dla wykonania sterowań są bity 6 oraz 7. Bity te określają, który przekaźnik

[10] Rysunek pochodzi z dokumentacji standardu DNP3.0

(załączający/wyłączający) ma być aktywowany w przypadku, gdy występują dwa przekaźniki dla danego punktu sterowanego. Wartość NUL tego atrybutu pozwala na wykonanie operacji "select" bez aktywacji przekaźników funkcyjnych (załącz/wyłącz). W przypadku, gdy nie ma przekaźnika funkcyjnego „select" ustawienie pola na NUL nie spowoduje żadnej akcji. W systemach, gdzie nie ma przekaźników funkcyjnych (załącz/wyłącz) atrybut ten powinien mieć zawsze wartość NUL wskazując, że dla danego punktu sterowniczego przekaźnik sterujący jest jednoznacznie określony/znany. Atrybut ten nie pozwala na jednoczesne ustawienie wartości TRIP I CLOSE.

Code: atrybut ten określa jakie sterowanie ma być wykonane i przyjmuje wartości od 0 do 15 (4 bity):

0: brak specyfikacji funkcji sterowania
1: „Pulse On" – przekaźnik sterujący ustawiany jest w stan wysoki na czas „on-time", a następnie w stan niski na czas „off-time" i pozostawiane w tym stanie.
2: „Pulse Off" – przekaźnik sterujący ustawiany jest w stan niski na czas „off-time", a następnie w stan wysoki na czas „on-time" i pozostawiane w tym stanie.
3: "Latch On" - przekaźnik sterujący ustawiany jest w stan wysoki
4: "Latch Off" - przekaźnik sterujący ustawiany jest w stan niski
5 - 15: niezdefiniowane

Queue: atrybut ten mówi czy dane sterowanie ma być kolejkowane czy nie; jeżeli wartość atrybutu Control Code jest zerowa (NULL) wówczas żadne sterowanie nie jest kolejkowane; jeżeli istnieje to czyszczona jest kolejka sterowań łącznie ze sterowaniem realizowanym w danym momencie (jeżeli atrybut Clear jest ustawiony). Sterowania z ustawionym atrybutem Queue są kolejkowane, a po zakończeniu sterowania są usuwane z kolejki.

Clear: jeżeli ten atrybut jest ustawiony wówczas z kolejki (jeżeli istnieje) usuwane są wszystkie sterowania łącznie z tym, które jest realizowane w danym momencie; rozpoczęte sterowanie nie jest przerywane i jest realizowane do końca.

Status: Informacja odnośnie statusu wykonywania sterowania przez urządzenie SLAVE jest przesyłana w ramach atrybutu *Status*, który może mieć następujące wartości:

0: żądanie sterowania zaakceptowane, zainicjowane lub kolejkowane.
1: żądanie sterowania niezaakceptowane, ponieważ upłynął time-out (arm timer) związany z poprzednią komendą Select. Timer "arm timer" rozpoczął odmierzanie czasu w momencie, gdy dla danego punktu została odebrana komenda Select.
2: dla danego punktu sterowniczego odebrano komendę Operate bez uprzedniej komendy Select.
3: żądanie sterowania niezaakceptowane, ponieważ zawiera ono błędne informacje/parametry atrybutów
4: żądanie sterowania niezaakceptowane, ponieważ dla danego punktu nie przewidziano sterowania
5: żądanie sterowania niezaakceptowane, ponieważ kolejka jest już zapełniona lub dla danego punktu sterowanie jest w trakcie realizacji.
6: żądanie sterowania niezaakceptowane, ponieważ występują problemy sprzętowe
7 - 127: niezdefiniowane

OBIEKT DANYCH – „ZDARZENIE - ZMIANA STANU WEJŚCIA BINARNEGO Z CZASEM"

Aby urządzenie Master odczytało informację o zdarzeniu zarejestrowanym przez urządzenie Slave najczęściej stosuje ono pytanie o tzw. „klasy", a odpowiedzią urządzenia Slave może być np. zbiór Obiektów Danych typu 02/02 opisany w specyfikacji DNP3 jako „BINARY INPUT CHNGE WITH TIME", dla którego ObjectGroup =02 i ObejctVariation = 02. W specyfikacji protokołu DNP3 przewidziano cztery rodzaje klas: „CLASS 0 DATA", „CLASS 1 DATA", „CLASS 2 DATA" oraz „CLASS 3 DATA" i są odpowiednio typu 60/01, 60/02, 60/03 i 60/04

Kodowanie obiektu 02/02 przedstawiono na Rys. 16,

FLAG							
7	6	5	4	3	2	1	0
TIME OF OCCURRENCE							
7	6	5	4	3	2	1	0
15	14	13	12	11	10	9	8
23	22	21	20	19	18	17	16
31	30	29	28	27	26	25	24
39	38	37	36	35	34	33	32
47	46	45	44	43	42	41	40

SQ2 {FLAG = *BS8* [0..7]
Time of Occurrence = *UI48* [0..47] <2^{48} -1 ms>
}

FLAG ={ *BS8* [0..7]
On-line = *BS1* [0] <0, off-line; 1, on-line>
Restart = *BS1* [1] <0, normal; 1, restart>
Communication lost = *BS1* [2] <0, normal; 1, lost>
Remote forced data = *BS1* [3] <0, normal; 1, forced>
Local forced data = *BS1* [4] <0, normal; 1, forced>
Chatter filter = *BS1* [5] <0, normal; 1, filter on>
Reserved = *BS1* [6] <0>
State = *BS1* [7] <0,1 BIN>
}

Rys. 16 Rysunek pochodzi z dokumentacji standardu DNP3.0[11]

gdzie:
FLAG [1 bajt]: zawiera informacje jak na powyższym rysunku
TIME OF OCCURENCE [6 bajtów]: zawiera liczbę [ms] jak upłynęła od 1 stycznia 1970 roku do momentu, w którym wystąpiło zdarzenie

Obiekt typu 02/02 wykorzystywany jest do przesyłania informacji o zmianie stanu wejścia binarnego wraz z informacją o tym kiedy zmiana nastąpiła czyli z tzw. znacznikiem czasu.

[11] Rysunek pochodzi z dokumentacji standardu DNP3.0

Ponadto w ramach atrybutu *FLAG* dostępne są następujące informacje (odpowiednio na poszczególnych bitach):

Bit on-line: wysoki stan wskazuje, że dane wejście binarne jest odczytane prawidłowo (jego stan odpowiada rzeczywistości); jeżeli ten bit ma wartość „0" czyli „off-line" wówczas przesyłany stan danego wejścia binarnego może nie być prawidłowy.
Bit restart: wskazuje, że urządzenie "pobudzające" dane wejście binarne było restartowane.
Bit communication lost: wskazuje, że urządzenie przesyłające informację o danym wejściu binarnym utraciło łączność z urządzeniem, które stanowi źródło danych o stanie danego wejścia binarnego.
Bit remote forced data: wskazuje, że stan w jakim znajduje się dane wejście binarne został wymuszony w urządzeniu, które stanowi źródło danych o stanie danego wejścia binarnego.
Bit local forced data: wskazuje , że stan w jakim znajduje się dane wejście binarne został wymuszony w urządzeniu przesyłającym stan danego wejścia binarnego.
Bit chatter filter: wskazuje, że stan danego wejścia binarnego był filtrowany w celu usuniecie zbędnych stanów przejściowych.
Bit state: wskazuje, aktualny stan danego wejścia binarnego.

Obiekt 60/01 CLASS 0 DATA – obiekty klasy „0": Obiekt tego typu nie ma żadnego kodowania tzn. nie służy on do przesyłania żadnych informacji. Domyślnie do klasy „0" przypisane są wszystkie obiekty danych w urządzeniu/stacji Slave, które nie zostały przypisane do klas „1", "2" i „3". Obiekty danych przypisane do tej klasy mogą być dowolnego typu, czyli dowolnej kombinacji ObjectGroup i ObjectVariation. Klasa ta zawiera obiekty danych, które nie są traktowane jako priorytetowe.

Obiekt 60/02 CLASS 1 DATA – obiekty klasy „1": Obiekt tego typu nie ma żadnego kodowania tzn. nie służy on do przesyłania żadnych informacji. Do klasy „1" przypisane są wszystkie obiekty danych w urządzeniu/stacji Slave o najwyższym priorytecie. Obiekty danych przypisane do tej klasy mogą być dowolnego typu czyli dowolnej kombinacji ObjectGroup i ObjectVariation i są to na ogół grupy obiektów oraz zmiany ich statusu.

Obiekt 60/03 CLASS 2 DATA – obiekty klasy „2": Obiekt tego typu nie ma żadnego kodowania tzn. nie służy on do przesyłania żadnych informacji. Do klasy „2" przypisane dowolne obiekty danych w urządzeniu/stacji Slave o priorytecie niższym niż obiekty z klasy „1". Obiekty danych przypisane do tej klasy mogą być dowolnego typu czyli dowolnej kombinacji ObjectGroup i ObjectVariation i są to na ogół grupy obiektów oraz zmiany ich statusu.

Obiekt 60/04 CLASS 3 DATA – obiekty klasy „3": Obiekt tego typu nie ma żadnego kodowania tzn. nie służy on do przesyłania żadnych informacji. Do klasy „3" przypisane dowolne obiekty danych w urządzeniu/stacji Slave o priorytecie niższym niż obiekty z klasy „1" i „2". Obiekty danych przypisane do tej klasy mogą być dowolnego typu czyli dowolnej kombinacji ObjectGroup i ObjectVariation i są to na ogół grupy obiektów oraz zdarzenia.

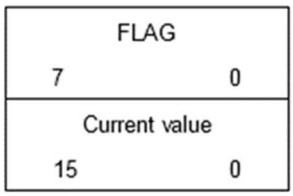
OBIEKT DANYCH – „ZDARZENIE - ZMIANA STANU WEJŚCIA ANALOGOWEGO"

Pytanie „klasy" jest wykorzystywane przez Master'a do pozyskiwania ze Slave'a informacji

o zmianach związanych z wejściami analogowymi. W takim przypadku odpowiedzią urządzenia Slave może być np. zbiór Obiektów Danych typu 20/02 opisany w specyfikacji DNP3 jako „16 BIT CHANGE EVENT WITHOUT TIME", dla którego ObjectGroup = 20 i ObejctVariation = 02.

UWAGA zapis OG/OV = 20/02 jest zapisem heksadecymalnym (takie wartości widać w ramce protokołu DNP3); w zapisie dziesiętnym obiekt posiada OG/OV = 32/02

Kodowanie Obiektu 20/02 przedstawiono na Rys. 17,



SQ2 {FLAG = *BS8* [0..7]
Current value = *I16* [0..15] <2^{15}-1..-2^{15}>
}

FLAG ={
On-line = *BS1* [0] <0, off-line; 1, on-line>
Restart = *BS1* [1] <0, normal; 1, restart>
Communication lost = *BS1* [2] <0, normal; 1, lost>
Remote forced data = *BS1* [3] <0, normal; 1, forced>
Local forced data = *BS1* [4] <0, normal; 1, forced>
Over-range = *BS1* [5] <0, normal; 1, over-range>
Reference check = *BS1* [6] <0, normal; 1, error>
Reserved = *BS1* [7] <0>
}

Rys. 17 Kodowanie Obiektu 32/02 dla DNP3.0[12]

gdzie:
FLAG [1 bajt]: zawiera informacje jak na powyższym rysunku
CURRENT VALUE [2 bajty]: zawiera aktualną (na moment generowania/raportowania danej informacji) wartość wejścia analogowego lub ostatnią wartość wygenerowaną przez urządzenie, które zmianę zarejestrowało.

Obiekt typu 20/02 jest obiektem służącym do przesłania informacji o zmianie stanu 16 bitowego wejścia analogowego (sprzętowego/ fizycznego lub software'owego) bez wskazania, kiedy zmiana nastąpiła czyli bez tzw. znacznika czasu. 16 bitowa wartość może reprezentować zarówno „spróbkowaną" wartość wejścia analogowego jak i wartość

[12] Rysunek pochodzi z dokumentacji standardu DNP3.0

wyliczoną.

Zmiana stanu wejścia analogowego będzie raportowana tylko wówczas, gdy aktualna wartość różni się od poprzedniej zarejestrowanej wartości o więcej niż tzw. deadband. Parametr ten jest konfigurowany w urządzeniu raportującym dane wejście analogowe i służy do filtracji stanów przejściowych/nieustalonych danego wejścia oraz ograniczeniu ruchu w sieci informacyjnej do niezbędnego minimum.

FLAG: W ramach tego atrybutu dostępne są następujące informacje (odpowiednio na poszczególnych bitach):

Bit on-line: wysoki stan wskazuje, że dane wejście binarne jest odczytane prawidłowo (jego stan odpowiada rzeczywistości); jeżeli ten bit ma wartość „0" czyli „off-line" wówczas przesyłany stan danego wejścia binarnego może nie być prawidłowy.
Bit restart: wskazuje, że urządzenie "pobudzające" dane wejście binarne było restartowane.
Bit communication lost: wskazuje, że urządzenie przesyłające informację o danym wejściu binarnym utraciło łączność z urządzeniem, które stanowi źródło danych o stanie danego wejścia binarnego.
Bit remote forced data: wskazuje, że stan w jakim znajduje się dane wejście binarne został wymuszony w urządzeniu, które stanowi źródło danych o stanie danego wejścia binarnego.
Bit local forced data: wskazuje , że stan w jakim znajduje się dane wejście binarne został wymuszony w urządzeniu przesyłającym stan danego wejścia binarnego.
Bit over range: wskazuje, że stan danego wejścia analogowego przekracza $+2^{15}$ -1 lub jest mniejszy niż -2^{15}
Bit reference check: wskazuje, że sygnał odniesienia wykorzystywany do próbkowania dennego wejścia analogowego nie jest „stabilny" co może wskazywać na to, że spróbkowany sygnał nie jest poprawny.

2.6.Przykładowa analiza ramek wymienianych w protokole DNP3

Przykład 1: Komendy, Sterowania:

Przebieg transmisji pomiędzy stacją Master i Slave w przypadku sterowania może wyglądać w następujący sposób:

Master->Salve:
05 64 1A C4 02 00 01 00 A5 E9 E7 C7 05 0C 01 28 01 00 0F 00 01 01 F4 01 00 00 E8 4C F4 01 00 00 00 0E 52

Slave->Master:
05 64 1C 44 01 00 02 00 E2 59 C9 C7 81 00 00 0C 01 28 01 00 0F 00 01 01 F4 01 AF F4 00 00 F4 01 00 00 00 0E 52

Analiza ramki wysyłanej ze stacji Master do stacji Slave (podział na warstwy i odrzucenie bajtów CRC) może wyglądać następująco:

Krok 1, podział na warstwy:

Bajty	Opis
05 64 1A C4 02 00 01 00 A5 E9	10 bajtów zawierających nagłówek Warstwy Łącza Danych
E7	1 bajt nagłówkowy Warstwy Transportowej (pseudo-transportowej)
C7 05 0C 01 28 01 00 0F 00 01 01 F4 01 00 00 E8 4C F4 01 00 00 00 0E 52	2 bloki USER DATA, a po nich 2 bajty CRC, czyli 24 Bajty z danymi Warstwy Aplikacji (CRC pochodzi z warstwy Łącza Danych)

Krok 2, Wyodrębnienie danych Warstwy Aplikacji, przez odrzucenie CRC:

Bajty	Opis
05 64 1A C4 02 00 01 00 A5 E9	2 bajty CRC na końcu nagłówka Warstwy Łącza Danych
E7	1 bajt zaliczany do USER DATA
C7 05 0C 01 28 01 00 0F 00 01 01 F4 01 00 00 E8 4C F4 01 00 00 00 0E 52	2 bajty CRC po każdym 16 bajtowym bloku USER DATA, na końcu również 2 bajty CRC

Krok 3, Analiza danych poszczególnych warstw:

Bajty	Opis
05 64	dwa bajty (two octets) startowe, zawsze 0x0564
1A	ilość pozostałych bajtów danych 26
C4	bajt CONTROL, którego reprezentacja binatna 1100 0100, czyli: 7 DIR - kierunek przesłania danych z Master do Outstation 6 PRM - pierwsze zapytanie, 5 FCB - ang. frame count bit, ignorowany 4 FCV - ang. frame count valid, ignorowany 3-0 - ang. function code, wartość 4 oznacza UNCONFIRMED_USER_DATA
02 00	2 bajty DESTINATION, oznaczający adres 0x0002, czyli 2
01 00	2 bajty SOURCE, oznaczające adres 0x0001, czyli 1
E7	bajt który w postaci binarnej przyjmuje wartość 1110 0111, oznacza: 7 FIN - ostatni fragment w sekwencji transportowej, 6 FIR - pierwszy fragment w sekwencji transportowej, 5-0 SEQUENCE - 39 ramka w sekwencji transportowej,
C7	AC nagłówka Warstwy Aplikacji, wartość binarna 1100 0111, oznacza: 7 FIN - ostatni fragment w sekwencji aplikacji, 6 FIR - pierwszy fragment w sekwencji aplikacji, 5 CON - apliakcja nie oczekuje potwierdzenia, 4 UNS - nie jest to wiadomość spontaniczna, 3-0 SEQUENCE - 7 fragment w sekwencji aplikacji,
05	FC, wartość 5 ozancza Direct Operte

Bajty	Opis
0C 01	ObjectType – ObjectGroup=12/ObjectVariation=01, czyli Control Relay Output Block
28	QualifierField – liczba sterowań na dwóch bajtach + dwa bajty prefixu z indeksem sterowania
01 00	dwa bajty z ilością sterowania – tutaj jedno sterowanie
0F 00	dwa bajty na indeks (numer) sterowania – tutaj sterowanie numer 15
01	Control Code – "Pulse On"
01	Count – „1"
F4 01 00 00	On-Time - 500
F4 01 00 00	Off-Time - 500
00	Status - sukccess

Częściowa analiza ramki wysyłanej ze stacji Slave do Master, jako odpowiedź na sterowanie.

Krok 1 i 2, podział na warstwy oraz wyodrębnienie danych Warstwy Aplikacji:

Bajty	Opis
05 64 1C 44 01 00 02 00 E2 59	10 bajtów, w tym 2 bajty CRC na końcu nagłówka Warstwy Łącza Danych
C9	1 bajt warstwy transportowej, zaliczany do USER DATA
C7 81 00 00 0C 01 28 01 00 0F 00 01 01 F4 01 AF F4 00 00 F4 01 00 00 00 0E 52	2 bajty CRC po każdym 16 bajtowym bloku USER DATA, na końcu również 2 bajty CRC

Krok 3, Analiza danych zawężona do danych zawartych w Warstwie Aplikacji:

Bajty	Opis
C7	AC nagłówka Warstwy Aplikacji, wartość binarna 1100 0111, oznacza: 7 FIN - ostatni fragment w sekwencji aplikacji, 6 FIR - pierwszy fragment w sekwencji aplikacji, 5 CON - apliakcja nie oczekuje potwierdzenia, 4 UNS - nie jest to wiadomość spontaniczna, 3-0 SEQUENCE - 7 fragment w sekwencji aplikacji,
81	FC oznaczające odpowiedź
00 00	2 bajty zawierające flagi IIN, wartość binarna to 0000 0000, oznacza brak dodatkowych informacji w odpowiedzi.
0C 01	ObjectType – ObjectGroup=12/ObjectVariation=01, czyli Control Relay Output Block
28	QualifierField – liczba sterowań na dwóch bajtach + dwa bajty prefixu z indeksem sterowania

Bajty	Opis
01 00	dwa bajty z ilością sterowania – tutaj jedno sterowanie
0F 00	dwa bajty na indeks (numer) sterowania – tutaj sterowanie numer 15
01	Control Code – "Pulse On"
01	Count – „1"
F4 01 00 00	On-Time - 500
F4 01 00 00	Off-Time - 500
00	Status - sukccess

Widać wyraźnie, że odpowiedź od Slave zawiera dodatkowy bajt INN w tym konkretnym przypadku nie zawierający dodatkowych informacji.

Przykład 2: Pytanie o zdarzenia/zmiany (pytanie o klasy – odpowiedź – zmiana wejścia binarnego):

Przebieg transmisji pomiędzy stacją Master i Slave w przypadku pytania o klasy (zdarzenia/zmiany) może wyglądać w następujący sposób:

Mster->Salve:
05 64 11 C4 02 00 01 00 29 E0 E5 C5 01 3C 02 06 3C 03 06 3C 04 06 EB 03

Slave->Master:
05 64 16 44 01 00 02 00 89 E5 C7 C5 81 00 00 02 02 17 01 03 81 20 DD 76 D3 5B C6 77 01 A1 C9

Częściowa analiza ramki wysyłanej ze stacji Master do stacji Slave (podział na warstwy i odrzucenie bajtów CRC) może wyglądać tak:

Krok 1 podział na warstwy:

05 64 11 C4 02 00 01 00 29 E0 – 10 bajtów warstwy łącza danych
E5 – 1 bajt warstwy pseudo-transportowej
C5 01 3C 02 06 3C 03 06 3C 04 06 EB 03 – 13 bajtów warstwy aplikacji

Krok 2 odrzucenie CRC:

05 64 11 C4 02 00 01 00 – warstwa łącza danych
E5 – warstwa pseudo-transportowa
C5 01 3C 02 06 3C 03 06 3C 04 06 – warstwa aplikacji

Krok 3 analiza danych warstwy aplikacji:

C5 - Application control (FIR, FIN, Seq etc)
01 - fuction code – 1 = Read

3C 02 - ObjectType – ObjectGroup=60/ObjectVariation=02 – Klasa 1
06 - QualifierField – wszystkie obiekty przypisane do tej klasy
3C 03 - ObjectType – ObjectGroup=60/ObjectVariation=03 – Klasa 2
06 - QualifierField – wszystkie obiekty przypisane do tej klasy
3C 04 - ObjectType – ObjectGroup=60/ObjectVariation=04 – Klasa 3
06 - QualifierField – wszystkie obiekty przypisane do tej klasy

Częściowa analiza ramki wysyłanej ze stacji Slave do stacji Master (podział na warstwy i odrzucenie bajtów CRC) może wyglądać tak:

Krok 1 podział na warstwy:

05 64 16 44 01 00 02 00 89 E5 – 10 bajtów warstwy łącza danych
C7 - 1 bajt warstwy pseudo-transportowej
C5 81 00 00 02 02 17 01 03 81 20 DD 76 D3 5B C6 77 01 A1 C9 - 20 bajtów warstwy aplikacji

Krok 2 odrzucenie CRC:

05 64 16 44 01 00 02 00 – warstwa łącza danych
C7 - warstwa pseudo-transportowa
C5 81 00 00 02 02 17 01 03 81 20 DD 76 D3 5B 01 - warstwa aplikacji

Krok 3 analiza danych warstwy aplikacji:

C5 - Application control (Fir, FIN, Seq etc)
81 - fuction code – 81 = Response
00 00 - INN – dwa bajty internal Indication – wszystkie flagi wyzerowane
02 02 - ObjectType – ObjectGroup=2/ObjectVariation=2 – obiekt typu zmiana stanu wejścia z czasem
17 - QualifierField – jeden bajt wskazujący liczbę obiektów
01 - Quantity- 1 = jeden obiekt
03 - Indeks – index wejścia binarnego = 3
81 - Flags – zgodnie z opisem obiektu 02/02
20 DD 76 D3 5B 01 - Time – zgodnie z opisem obiektu 02/02

Przykład 3: Pytanie o zdarzenia/zmiany (pytanie o klasy – odpowiedź – zmiana wejścia analogowego):

Przebieg transmisji pomiędzy stacją Master i Slave w przypadku pytania o klasy (zdarzenia/zmiany) może wyglądać w następujący sposób:

Mster->Salve:
05 64 11 C4 02 00 01 00 29 E0 E1 C1 01 3C 02 06 3C 03 06 3C 04 06 C4 3D
Slave->Master:
05 64 12 44 01 00 02 00 E7 A8 C3 C1 81 00 00 20 02 17 01 64 01 00 00 63 90

Częściowa analiza ramki wysyłanej ze stacji Master do stacji Slave (podział na warstwy i

odrzucenie bajtów CRC) może wyglądać tak:

Krok 1 podział na warstwy:

05 64 11 C4 02 00 01 00 29 E0 – 10 bajtów warstwy łącza danych
E1 – 1 bajt warstwy pseudo-transportowej
C1 01 3C 02 06 3C 03 06 3C 04 06 C4 3D – 13 bajtów warstwy aplikacji

Krok 2 odrzucenie CRC:

05 64 11 C4 02 00 01 00 – warstwa łącza danych
E5 - warstwa pseudo-transportowa
C1 01 3C 02 06 3C 03 06 3C 04 06 – warstwa aplikacji

Krok 3 analiza danych warstwy aplikacji:

C1 - Application control (Fir, FIN, Seq etc)
01 - fuction code – 1 = Read
3C 02 - ObjectType – ObjectGroup=60/ObjectVariation=02 – Klasa 1
06 - QualifierField – wszystkie obiekty przypisane do tej klasy
3C 03 - ObjectType – ObjectGroup=60/ObjectVariation=03 – Klasa 2
06 - QualifierField – wszystkie obiekty przypisane do tej klasy
3C 04 - ObjectType – ObjectGroup=60/ObjectVariation=04 – Klasa 3
06 - QualifierField – wszystkie obiekty przypisane do tej klasy

Częściowa analiza ramki wysyłanej ze stacji Slave do stacji Master (podział na warstwy i odrzucenie bajtów CRC) może wyglądać tak:

Krok 1 podział na warstwy:

05 64 12 44 01 00 02 00 E7 A8 – 10 bajtów warstwy łącza danych
C3 - 1 bajt warstwy pseudo-transportowej
C1 81 00 00 20 02 17 01 64 01 00 00 63 90 – 14 bajtów warstwy aplikacji

Krok 2 odrzucenie CRC:

05 64 12 44 01 00 02 00 – warstwa łącza danych
C3 - warstwa pseudo-transportowa
C1 81 00 00 20 02 17 01 64 01 00 00 – warstwa aplikacji

Krok 3 analiza danych warstwy aplikacji:

C1 - Application control (Fir, FIN, Seq etc)
81 - fuction code – 81 = Response
00 00 - INN – dwa bajty internal Indication – wszystkie flagi wyzerowane
20 02 - ObjectType – ObjectGroup=20/ObjectVariation=2 – obiekt typu zmiana stanu wej. Analog. (OG/OV-32/02)
17 - QualifierField – jeden bajt wskazujący liczbę obiektów

01 - Quantity- 1 = jeden obiekt
64 - Indeks – index wejścia analogowego = 64 heksadecymalnie (100 dziesiętnie)
01 - Flags – zgodnie z opisem obiektu 20/02
00 00 - Current Value – zgodnie z opisem obiektu 20/02

3. PRZEBIEG ĆWICZENIA

3.1. Obserwacja „akcji i reakcji" między SCADA , a IED (MiCOM P127).

Ćwiczenie należy rozpocząć od zestawienia komunikację między Bramą Dostępowoą GTW IEC/DNP3.0, a symulatorem systemu SCADA – AXON TEST. Aby osiągnąć układ jaki pokazano na Rys. 2. Należy ustawić odpowiednie parametry komunikacyjne łącza szeregowego RS232 w oprogramowaniu AXON TEST (według załącznika 1) oraz zweryfikować poprawność połączenia (załącznik 1 i 2).

Parametry transmisji szeregowej w IED:

- Adres GTW IEC/DNP3.0 (slave adres) - 2,
- Adres SCADA (master adres) - 1,
- Prędkość 9600b/sec,
- 8 bitów na znak, Brak parzystości, 1 bit stopu (w skrócie 8N1).

Pozostałe parametry komunikacji należy ustawić tak, jak podano w załączniku 1.

Zweryfikować poprawność komunikacji poprzez wymuszenie z zabezpieczenia P127 przykładowych sygnałów statycznych:

- Wyłącznik Q1(DPS), położenie: Wyłączony (0); Załączony (1). Indeks DNP: 4 i 5,
- Człon ruchomy wyłącznika Q1(SPS), położenie: Próba (0); Praca (1). Indeks DNP: 6,

Pomiarów (MV):

- Napięcie L1. Indeks DNP: 10
- Prąd fazy L1. Indeks DNP: 11

Komend (DPC):

- Wyłącznik Q0. Załącz („Pulse_ON"), P127-RL1. Indeks DNP: 1
- Wyłącznik Q0. Wyłącz (1), P127-RL2. Indeks DNP: 1

Wysyłając komendy należy zwrócić uwagę na stany wyjść przekaźnika P127. Sygnalizacja w postaci lampek, lub test ciągłości obwodu multimetru. Wartości pomiarowe, stany wejść i wyjść można sprawdzić w urządzeniu P127 (załącznik 4).

Poprawność wymuszanych stanów należy obserwować również w oprogramowaniu AXON-TEST oraz w oknie logów oprogramowania PACiS GTW (załącznik 1 i 2).

W sprawozdaniu należy umieścić informacje dotyczące prawidłowego (bądź nieprawidłowego) połączenia szeregowego. We wnioskach należy opisać potencjalne przyczyny nieprawidłowego połączenia posługując się zgromadzonymi logami.

Dodatkowym zadaniem jest obserwacja czasu zdarzeń statycznych (symbol * przy sygnaturze czasu oznacza zdarzenie/pomiar bez znacznika czasu bądź niesynchronizowane) w oknie „Digital Status" Pacis Gateway oraz w oknie „Viewer" SCADA symulatora oraz na dzienniku zdarzeń HMI. Przed zakończeniem ćwiczenia należy skontaktować się z grupą realizująca ćwiczenie nr 2, aby wydrukować

dziennik zdarzeń dotyczący pola P05 rozdzielni 15kV, z którego pochodzą wszystkie sygnały czytane w symulowanym systemie SCADA w ramach tego ćwiczenia.

3.2. Obserwacja ramek protokołu DNP3 dla stanów statycznych, pomiarów i komend z wykorzystaniem oprogramowania AXON-TEST oraz oprogramowania diagnostycznego DebugView.

Kolejna część ćwiczenia polega na obserwacji i diagnostyce komunikacji po protokole DNP3.0. Poprzez powtórzenie symulacji stanów statycznych opisanych w punkcie 3.1 oraz przechwycenie i późniejszą analizę komunikatów cyfrowych, należy zweryfikować poprawności przesyłanych stanów statycznych, pomiarów i sterowań. Należy zanotować obserwacje, wnioski i analizę sygnałów umieścić w sprawozdaniu.

W celu przechwycenia sygnałów cyfrowych należy w oprogramowaniu DebugView uruchomić monitor portu szeregowego (Załącznik 3) oraz zapisać ramki komunikacji do plików tekstowych. Wykonać po kilka prób zmiany położenia łączników oraz prób sterowań, a także przechwycić 2-3 różne wartości wymuszanych dla przekaźnika P127 pomiarów.

Sterowanie wyłącznikiem w polu (P04-15kV):
- Komenda „Pulse_ON" na wyłącznik „Załącz" – Indeks DNP: 1;
- Komenda „Pulse_OFF" na wyłącznik „Wyłącz" – Indeks DNP: 1;

Stany statyczne (P04-15kV):
- Wyłącznik Q1 – położenie (w P127 we.L1) – Indeks DNP: 4;
- Człon ruchomy wyłącznika Q1(w P127 we.L2) – Indeks DNP: 5;

Odczyt pomiarów (P05-15kV):
- Napięcie fazy L1 – Indeks DNP: 60;
- Prąd fazy L1 – Indeks DNP: 61;

format danych: Int16,

Dokonać analizy zgromadzonych ramek komunikacyjnych i porównać je ze stanem fizycznym wartości elektrycznych – w zabezpieczeniu oraz zapisie dziennika zdarzeń HMI. Wykorzystać wcześniejsze obserwacje. W sprawozdaniu opisać wnioski i zaproponować rozwiązania jeżeli są konieczne.

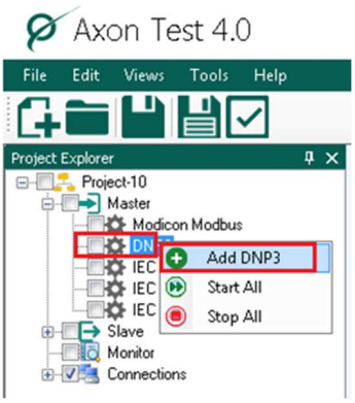
4. SPIS RYSUNKÓW, TABEL I ZAŁĄCZNIKÓW DO ĆWICZENIA

KONIEC DOKUMENTU

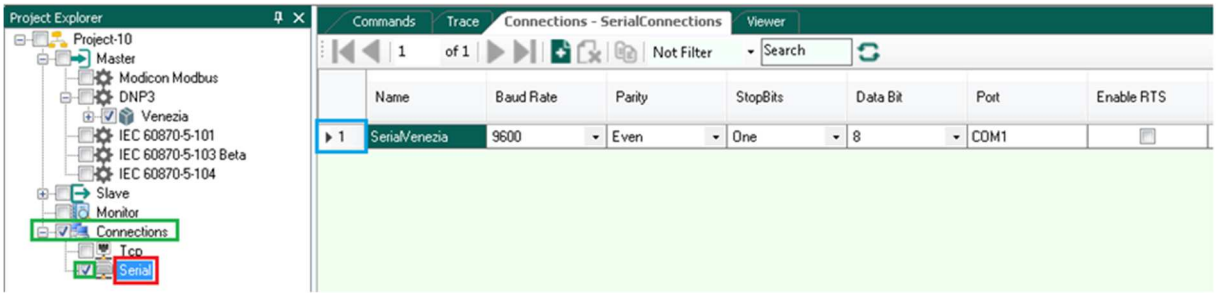
ZAŁĄCZNIK 1 – Obsługa Axon – Test, symulator master SCADA DNP3.

Parametryzacja:

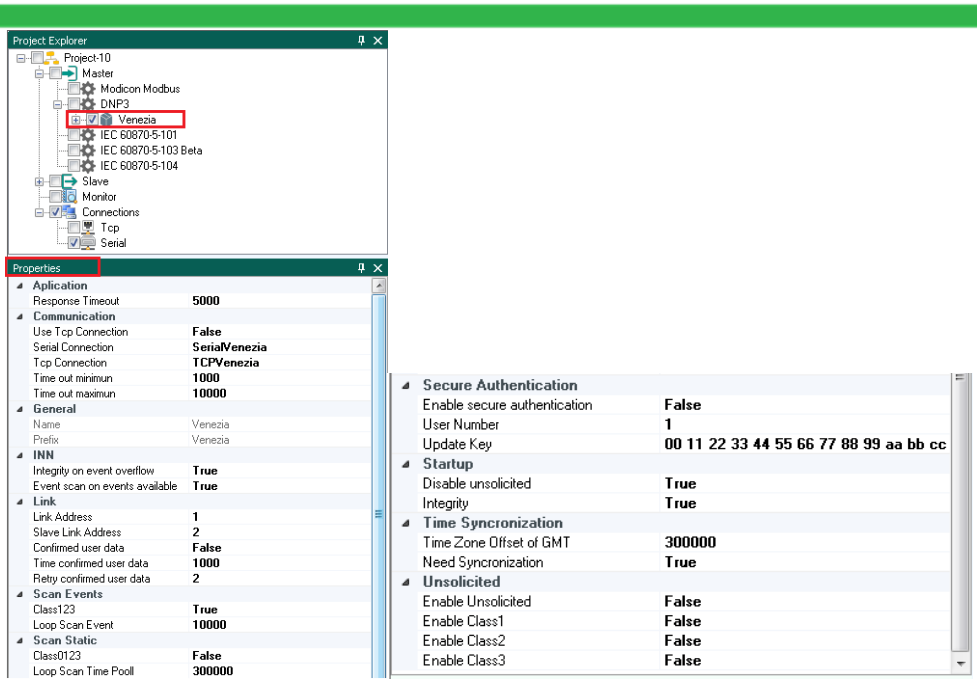
Należy uruchomić oprogramowanie Axon – Test. Następnie w części „Master" dodać urządzenie poprzez kliknięcie p.p.m „Add DNP3".



Nazwa dodanego urządzenia jest generowana automatycznie (w przykładzie nazwa to Venezia). Kolejnym etapem jest określenie parametrów portu komunikacyjnego – należy kliknąć dwa razy na ikonę „Serial", następnie w zakładce „Connections-SerialConnections" pojawi się wiersz (o nazwie powiązanej z urządzeniem DNP3) z parametrami transmisji szeregowej, gdzie należy ustawić odpowiednie parametry – wg. ćwiczenia 3.1. Klikając na zaznaczoną poniżej na niebiesko „1" możemy zweryfikować w oknie „Properties " poprawność wprowadzonych danych (te same ustawienia portu, powinny zostać nadane na rzeczywistym porcie komputera PC z zainstalowaną aplikacją Gateway).



Następnie definiujemy parametry komunikacji mastera DNP3 w oknie „Properties ", klikając na urządzenie – przykład, rysunek poniżej.



Informacje o dodatkowych parametrach:

- *Response Timeout* – określany w milisekundach.
- Use TCP Connection – komunikacja w protokole TCP powinna być wyłączona.
- Serial Connection – umożliwia wybór wszystkich zdefiniowanych połączeń szeregowych, należy wybrać zdefiniowaną wcześniej nazwę połączenia.

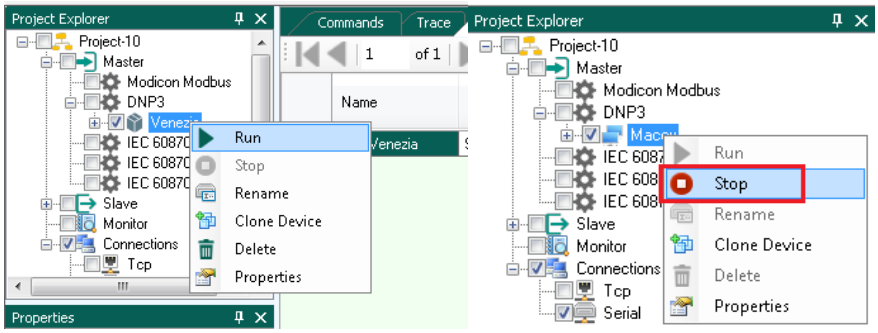
Najważniejsze parametry połączenia to:

- Link Address - adres urządzenia Master.
- Slave Link Address - adres urządzenia Slave.
- Scan Events:
    - Class 123 – Włącza lub wyłącza odpytanie o nowe zdarzenia
    - Loop Scan Event – cykl odpytania o nowe zdarzenia określany w milisekundach.
- Scan Static:
    - Class 0123 - Włącza lub wyłącza ogólne odpytanie (general interrogation).
    - Loop Scan Time Poll - cykl odpytania ogólnego określany w milisekundach.
- Time synchronization:
    - Time Zone Offset of GMT – parametr określany w minutach, przesunięcie czasowe względem UTC
    - Need synchronization – ustawienie mastera SCADA jako źródła synchronizacji czasowej, w ćwiczeniu należy ustawić na „False”.
- Disable Unsolicited: Opcja umożliwia włączenie lub wyłączenie „spontaniczności” obiektów klas 1, 2, 3 pochodzących z urządzenia Slave.

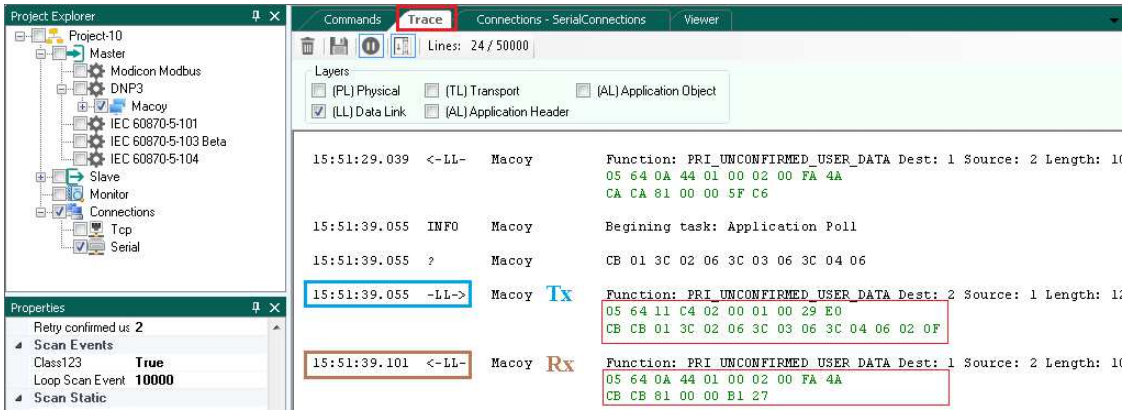
Pozostałe parametry należy ustawić według powyższego rysunku.

Symulacja, odczyt stanów:

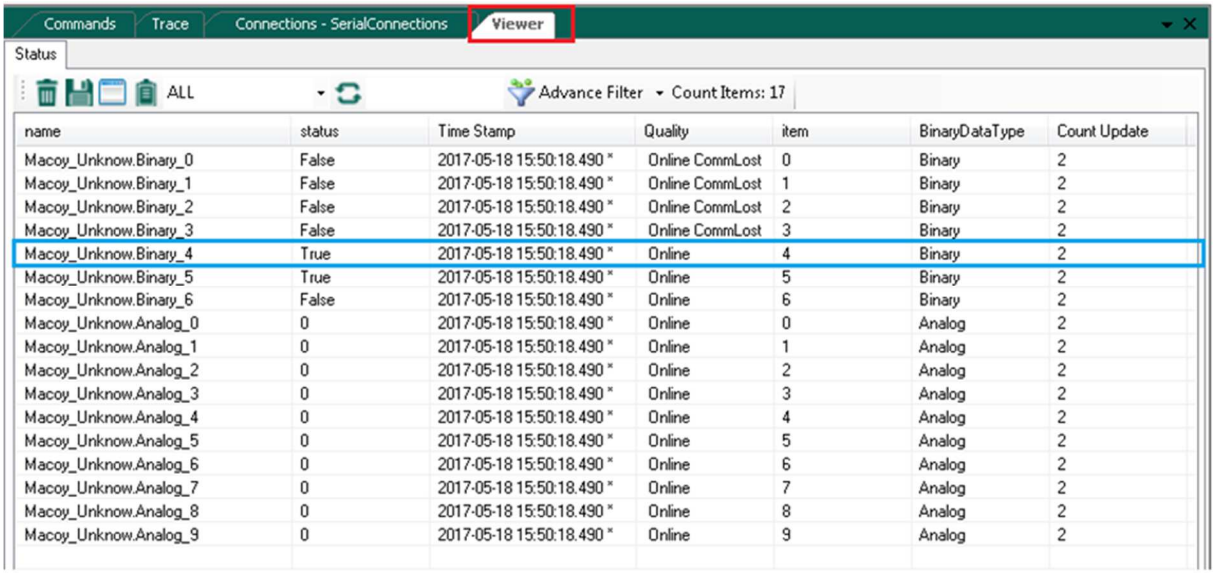
Symulację Master dla SCADA uruchamiamy przyciskiem Run klikając p.p.m. na urządzenie DNP3, aby zatrzymać symulację klikamy stop:



Po uruchomieniu prawidłowo skonfigurowanego Mastera urządzenie podświetli się na niebiesko, a w zakładce „Trace" powinniśmy zobaczyć ruch ramek z danymi w dwóch kierunkach.



Po nawiązaniu komunikacji, w zakładce Viewer można podglądać stany wszystkich punktów zaadresowanych w urządzeniu Slave. Zostaną wyświetlone punkty od adresu 0 do najwyższego adresu użytego w urządzeniu Slave – oddzielnie dla stanów cyfrowych (Binary) i analogowych (Analog).

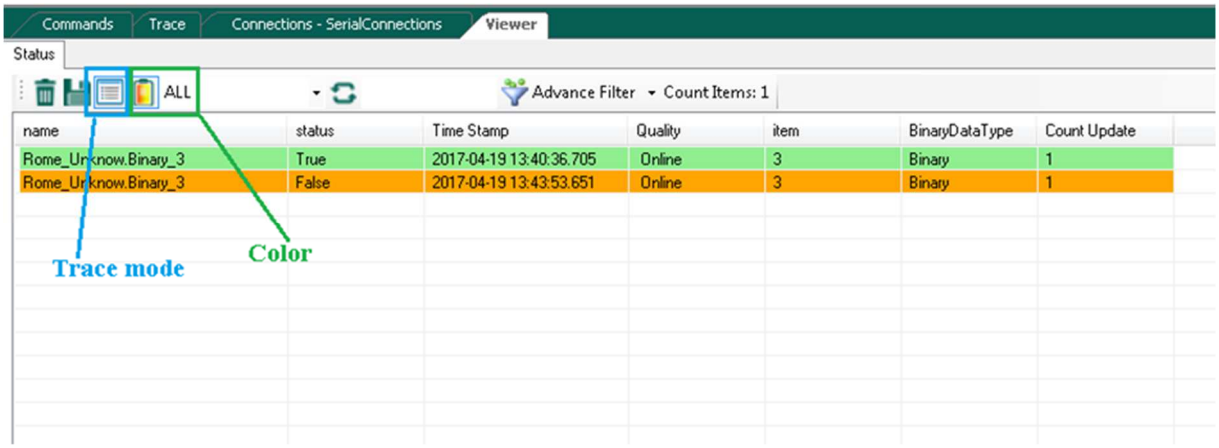


name	status	Time Stamp	Quality	item	BinaryDataType	Count Update
Macoy_Unknow.Binary_0	False	2017-05-18 15:50:18.490 *	Online CommLost	0	Binary	2
Macoy_Unknow.Binary_1	False	2017-05-18 15:50:18.490 *	Online CommLost	1	Binary	2
Macoy_Unknow.Binary_2	False	2017-05-18 15:50:18.490 *	Online CommLost	2	Binary	2
Macoy_Unknow.Binary_3	False	2017-05-18 15:50:18.490 *	Online CommLost	3	Binary	2
Macoy_Unknow.Binary_4	True	2017-05-18 15:50:18.490 *	Online	4	Binary	2
Macoy_Unknow.Binary_5	True	2017-05-18 15:50:18.490 *	Online	5	Binary	2
Macoy_Unknow.Binary_6	False	2017-05-18 15:50:18.490 *	Online	6	Binary	2
Macoy_Unknow.Analog_0	0	2017-05-18 15:50:18.490 *	Online	0	Analog	2
Macoy_Unknow.Analog_1	0	2017-05-18 15:50:18.490 *	Online	1	Analog	2
Macoy_Unknow.Analog_2	0	2017-05-18 15:50:18.490 *	Online	2	Analog	2
Macoy_Unknow.Analog_3	0	2017-05-18 15:50:18.490 *	Online	3	Analog	2
Macoy_Unknow.Analog_4	0	2017-05-18 15:50:18.490 *	Online	4	Analog	2
Macoy_Unknow.Analog_5	0	2017-05-18 15:50:18.490 *	Online	5	Analog	2
Macoy_Unknow.Analog_6	0	2017-05-18 15:50:18.490 *	Online	6	Analog	2
Macoy_Unknow.Analog_7	0	2017-05-18 15:50:18.490 *	Online	7	Analog	2
Macoy_Unknow.Analog_8	0	2017-05-18 15:50:18.490 *	Online	8	Analog	2
Macoy_Unknow.Analog_9	0	2017-05-18 15:50:18.490 *	Online	9	Analog	2

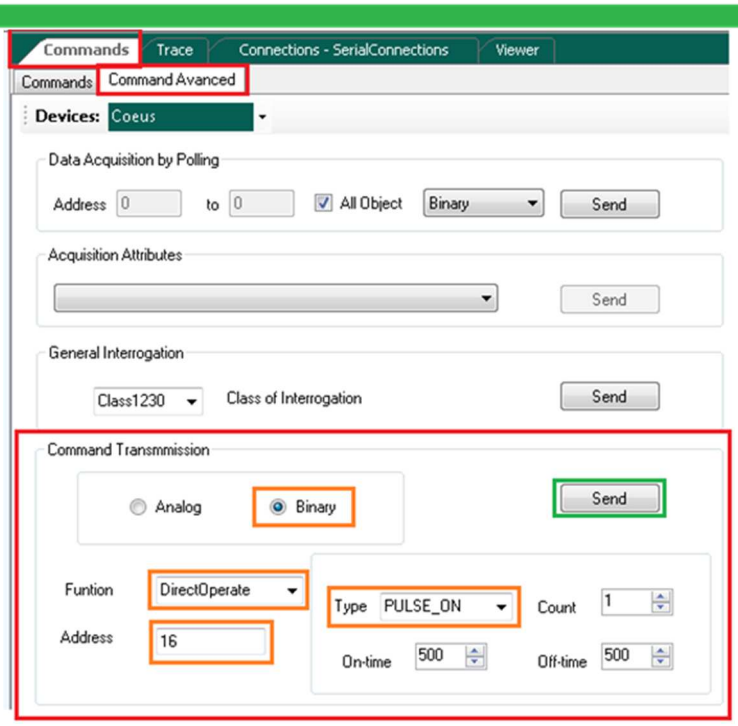
Znaczenie poszczególnych kolumn:

- Name - nazwy generowane przez oprogramowanie.
- Status - stan logiczny/wartość punktu.
- Time Stamp – czas wystąpienia zdarzenia w zabezpieczeniu. Jeżeli zostanie włączona opcja Scan Static - Class 0123 „True" wówczas czas zostanie zamieniony czasem periodycznego odczytu z urządzenia slave.
- Quality – jakość sygnału (flagi Quality wg opisu OBIEKTU DANYCH)
- Item – określa również adres kolejnego punktu.
- Binary Data Type – typ punktu – Binarny lub Analogowy.
- Count Update – liczniki określające numer zmiany stanu / wartości punktu.

Aby ułatwić podgląd zmieniających się stanów binarnych w danym momencie, w zakładce Viewer można wyczyścić wszystkie sygnały (ikona kosza) i włączyć funkcję „Trace mode" oraz „Color". W tej konfiguracji zmieniające się sygnały będą pojawiać się na liście „Viewer" jeden po drugim z różnymi kolorami, przykład poniżej:



Symulacja, wysyłanie komend:



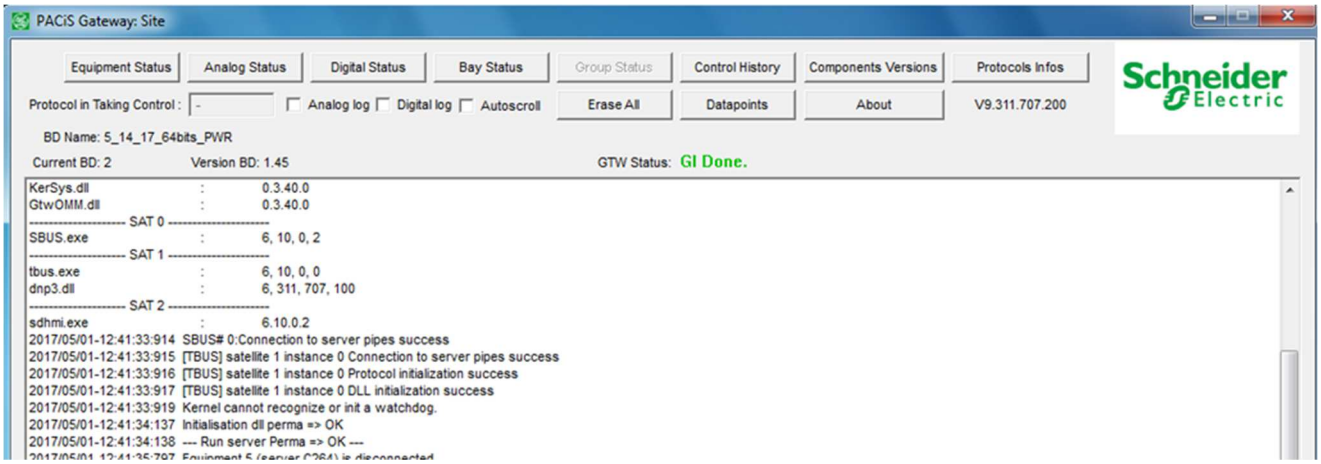
W zakładce „Commends" możemy wysłać komendę z wartością cyfrową – w rzeczywistości przesyłamy na określony adres urządzenia wartość „True" lub „Fales" – PULSE_ON lub PULSE_OFF.

Należy wykorzystać komendy tupu DirectOperate – czyli komendy bezpośrednie.

ZAŁĄCZNIK 2 – Interfejs diagnostyczny oprogramowania PACiS Gateway-obsługa.

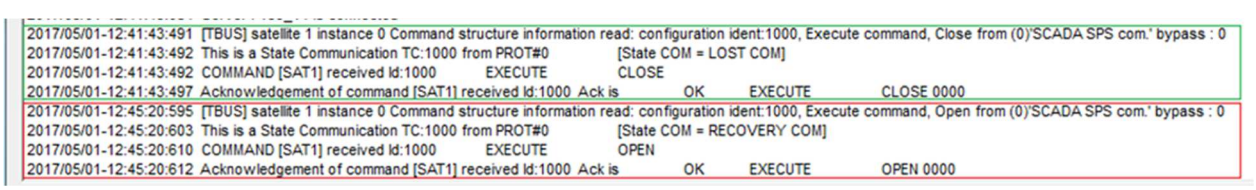
Należy uruchomić oprogramowanie PACiS Gateway z pulpitu komputera na stanowisku do ćwiczenia. Na komputerze tym zainstalowane jest oprogramowanie PACiS GTW IEC61850 / DNP3.

Widok interfejsu oprogramowania Gateway:



Powyżej pokazano komunikat (podświetlony na zielono) informujący o statusie oprogramowania Gateway „GTW Status: GI Done" informuje on o zakończeniu ogólnego odpytania wszystkich serwerów, o gotowości aplikacji do pracy.

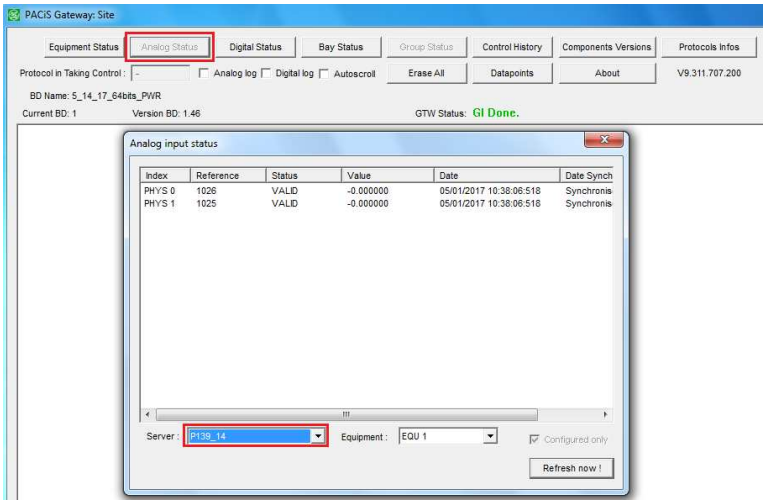
Poniżej znajduje się fragment logu, informujący o połączeniu z systemem nadrzędnym za pomocą portu 0. W ramce zielonej znajduje się status braku połączenia: „LOST COM" i Ack (Acknowledgement of command) – CLOSE. W ramce czerwonej znajduje się status nawiązania połączenia: „RECOVERY COM" i Ack (Acknowledgement of command) – OPEN.



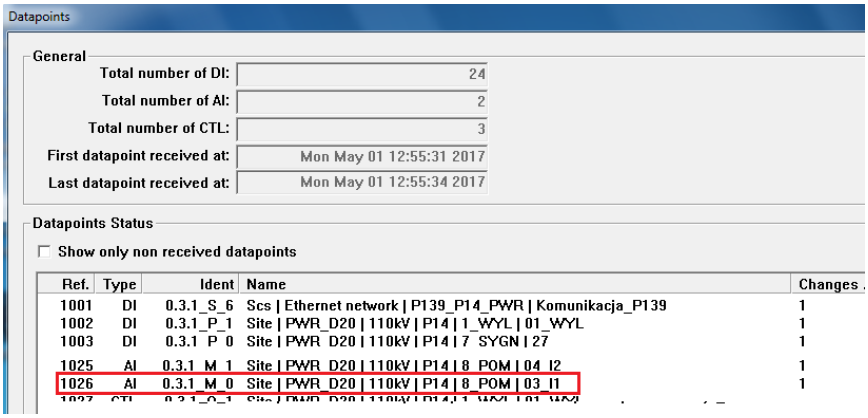
Aby na bieżąco w oknie logów podglądać wartości analogowe i/lub statyczne należy zaznaczyć opcję „Analog log", „Digital log". Dodatkowe zaznaczenie opcji Autoscroll umożliwia automatyczne przewijanie logów w oknie. Aby wyczyścić okno logów, co warto

wykonać przed testem weryfikującym komunikację z ćwiczenia 3.1, należy nacisnąć przycisk „Erase All". Nie ma możliwości zapisu danych z okna logów do pliku, można wykonać zrzut ekranu.

Podgląd wartości analogowych, jest możliwy po kliknięciu przycisku „Analog Status" i wybraniu serwera z którego dane pochodzą:



W zaprezentowanym przykładzie dane pochodzą z serwera P139. Numer „Reference" jest to numerem przypisanym do każdego punktu/danej. Aby sprawdzić jaka dana reprezentowana jest pod danym numerem referencyjnym, można uruchamiając przyciskiem „Datapoints" wejść w listę zawierającą spis wszystkich punktów przypisanych do bramy dostępowej oraz ich numerów referencyjnych.



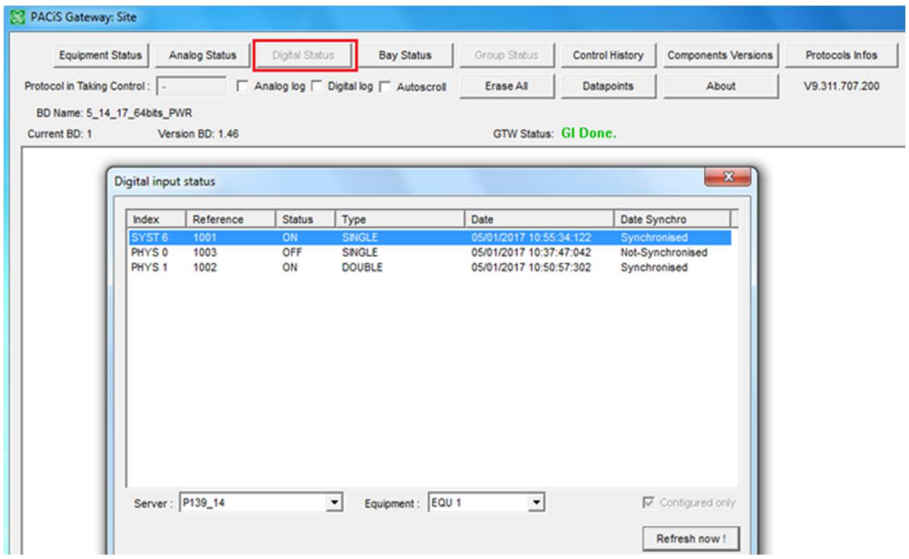
W powyższym prazykładzie, 1026 reprezentuje prąd fazy 1 – I1 w polu P14 stacji 110kV.

<u>Przykładowe wartości w ćwiczeniu:</u>

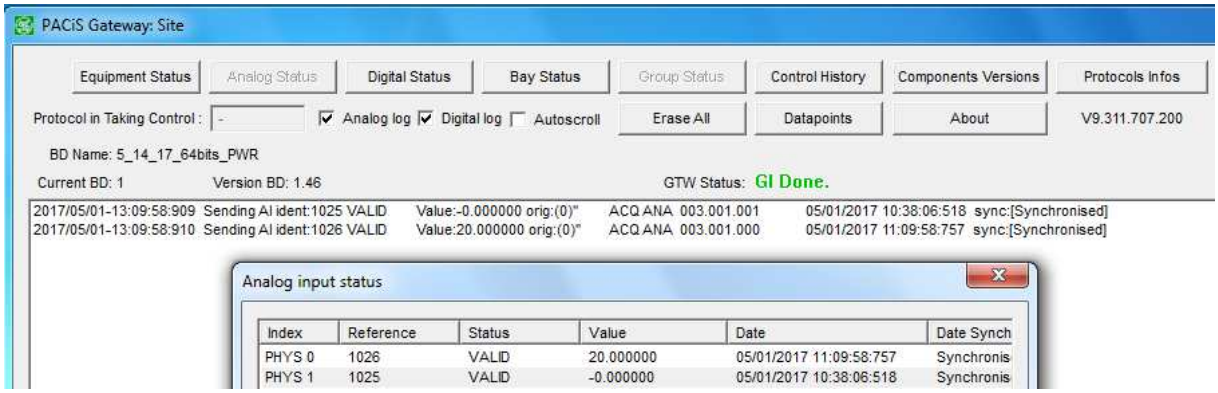
Ia P127	– Site | PWR_D20 | 15kV | P04 | POMIARY | Ia
Ua P127	– Site | PWR_D20 | 15kV | P04 | POMIARY | Ua
Wyłącznik Q1 P127	- Site | PWR_D20 | 15kV | P04 | Q1 | Wylacznik_Q1

Wózek wyłącznik Q1 P127 - Site | PWR_D20 | 15kV | P04 | Q1 | Wozek_L2

Podgląd wartości statycznych można osiągnąć za pomocą przycisku „Digital Status”:



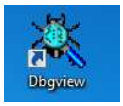
Przykład logu wartości analogowych w oknie logów oraz w oknie wartości analogowych zaprezentowano poniżej.



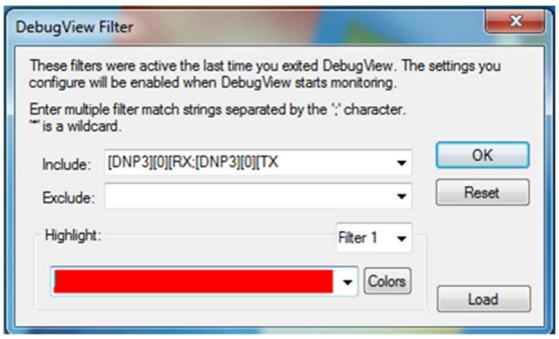
W oknie logów czas widoczny z lewej strony wpisu, jest czasem otrzymania wiadomości i jest on zgodny z czasem systemu operacyjnego komputera, na którym zainstalowano oprogramowanie PACIS Gateway. Czas widoczny z prawej strony okna logów, jest czasem nadanym przez urządzenie IED po zarejestrowaniu wartości pomiaru, ten sam czas jest widoczny w oknie „Analog Status” i „Digital Status”.

ZAŁĄCZNIK 3 – Obsługa oprogramowania DebugView.

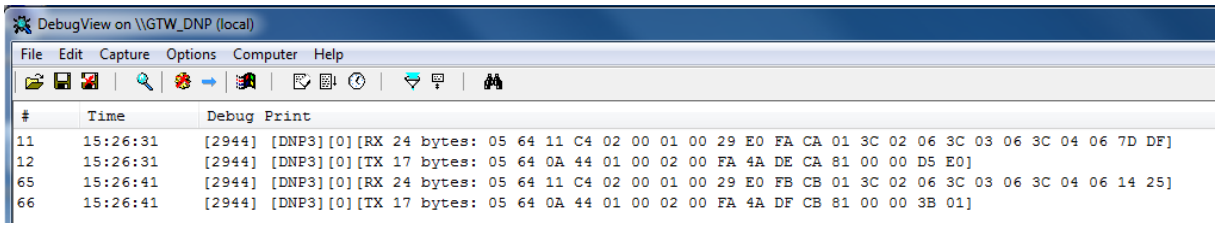
Należy uruchomić oprogramowanie DebugView z poziomu pulpitu komputera na którym jest zainstalowany PACiS GTW IEC61850 / DNP3.



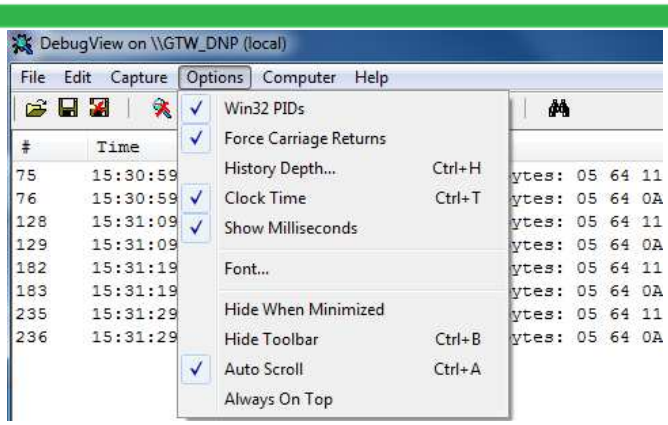
Wprowadzić następujący filtr w pierwszym oknie (składnia dostępna w pliku tekstowym „Filtr"):



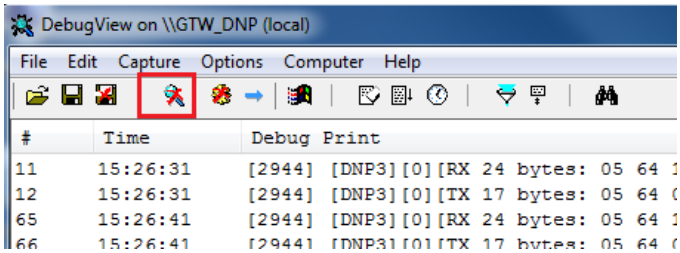
Potwierdzenie przyciskiem *OK* uruchamia okno logów, w tym przypadku wiadomość oznaczona jako RX to bajty danych wysłanych przez IED typu Master (Pytanie), TX to wiadomość z bajtami danych wysłanymi przez IED typu Slave (Odpowiedź):



W opcjach należy również włączyć sposób wyświetlania czasu „Clock Time", jak na rysunku poniżej:



Aby zatrzymać monitorowanie w oknie logów, należy kliknąć ikonę lupy zaznaczoną na czerwono poniżej:

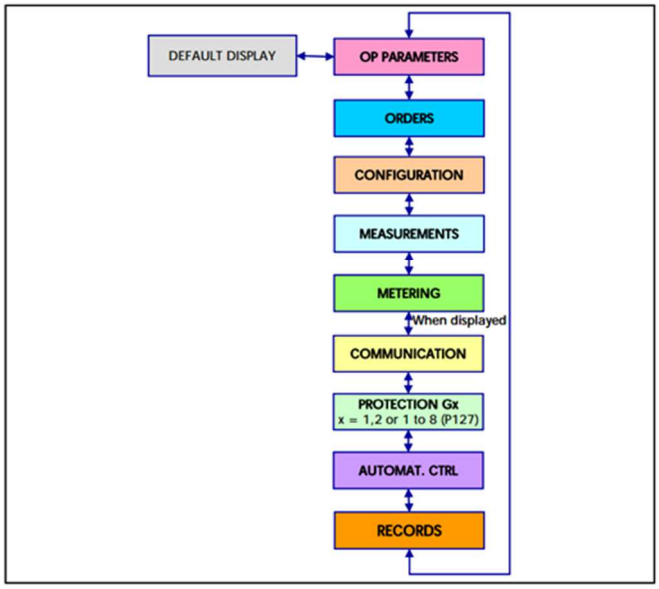


Aby zapisać otrzymane logi, z menu wybieramy File potem „Save as”.

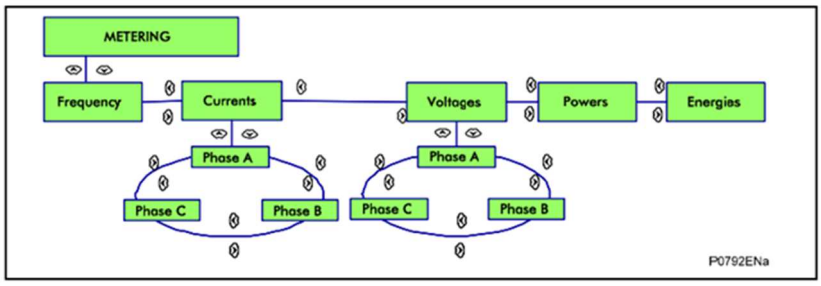
ZAŁĄCZNIK 4 – Nawigacja P127 do pomiarów i stanów wejść, wyjść cyfrowych.

To access these menus from the default display press ⊘.

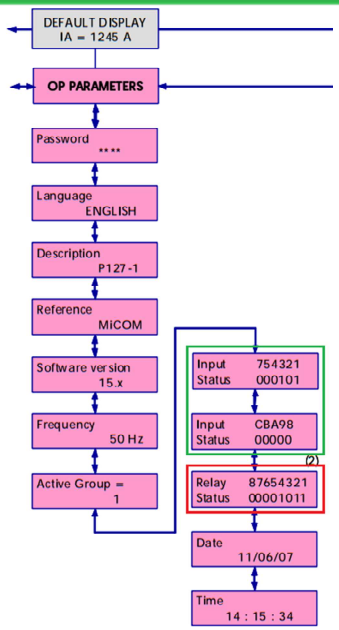
To return to the default display from these menus or submenus press ⊘.



To access METERING menu from the default display, press ⊘ then ⊘ until the header of menu is reached. The submenus of the Metering are:



Inputs and outputs (Relay) statuses:


DEFAULT DISPLAY
IA = 1245 A
OP PARAMETERS
Password
****
Language
ENGLISH
Description
P127-1
Reference
MiCOM
Software version
15.x
Frequency
50 Hz
Active Group =
1
Input 754321
Status 000101
Input CBA98
Status 00000
(2)
Relay 87654321
Status 00001011
Date
11/06/07
Time
14 : 15 : 34