

WAGO I/O System 750 XTR



750-8213/040-010

PFC200 G2 2ETH M12 CAN XTR

**sterownik PFC200 G2; 2 x ETHERNET M12,
CAN, CANopen; do zastosowań w ekstremalnych
warunkach**

Wersja 1.2.0, ważna od wersji FW 03.06.09(18)

Niniejszy podręcznik nie obejmuje sterowników z FW od 19
oraz środowiska programowania CODESYS V3.5.

© 2025 WAGO GmbH & Co. KG
Wszystkie prawa zastrzeżone.

WAGO GmbH & Co. KG

Hansastraße 27
D-32423 Minden

tel.: +49 (0) 571/8 87 – 0

faks: +49 (0) 571/8 87 – 1 69

e-mail: info@wago.com

www: www.wago.com

Wsparcie techniczne PL:

tel.: +48 71 360 29 33

e-mail: wsparcie.techniczne@wago.com

Przy tworzeniu niniejszej dokumentacji podjęto wszelkie możliwe działania w celu zapewnienie jej prawidłowości i kompletności. Pomimo zachowania najwyższej staranności wykluczenie błędów nie jest możliwe. Będziemy więc wdzięczni za wszelkie wskazówki i sugestie, które prosimy kierować na poniższy adres e-mail: documentation@wago.com

Należy zwrócić uwagę na fakt, że zastosowane w niniejszym podręczniku nazwy sprzętu i oprogramowania oraz nazwy marek poszczególnych firm podlegają ochronie znaków towarowych, marek lub ochronie patentowej.

Znak WAGO jest zastrzeżonym znakiem towarowym spółki WAGO Verwaltungsgesellschaft mbH.

Spis treści

1	Wskazówki dotyczące dokumentacji	15
1.1	Zakres obowiązywania	15
1.2	Prawa autorskie	15
1.3	Prawa własności	16
1.4	Symbole	17
1.5	Zastosowane systemy liczbowe	18
1.6	Sposoby zapisu	18
2	Ważne objaśnienia	19
2.1	Podstawy prawne	19
2.1.1	Zastrzeżenie prawa do zmian technicznych	19
2.1.2	Kwalifikacje personelu	19
2.1.3	Stosowanie serii 750 zgodne z przeznaczeniem	19
2.1.4	Stan techniczny urządzeń	20
2.2	Wskazówki dotyczące bezpieczeństwa	21
2.3	Warunki licencji dla zastosowanych pakietów oprogramowania	24
2.4	Specjalne warunki zastosowania urządzeń ETHERNET	25
3	Przegląd	26
4	Dane	29
4.1	Budowa sprzętu	29
4.1.1	Widok	29
4.1.2	Nadruk	31
4.1.2.1	Numer produkcyjny	31
4.1.3	Złącza	32
4.1.3.1	Oprzewodowanie	32
4.1.3.2	Złącze serwisowe	33
4.1.3.3	Złącza sieciowe	34
4.1.3.4	CANopen	35
4.1.4	Połączenia systemowe	37
4.1.4.1	Styki magistrali systemowej	37
4.1.4.2	Styki magistrali obiektowej	38
4.1.5	Elementy sygnalizacyjne	39
4.1.6	Elementy sygnalizacyjne dla zasilania	39
4.1.7	Elementy sygnalizacyjne dla sieci/systemu	40
4.1.8	Elementy sygnalizacyjne dla gniazda na kartę pamięci	41
4.1.9	Elementy sygnalizacyjne dla sieci	42
4.1.10	Elementy obsługi	43
4.1.10.1	Przełącznik trybu pracy	43
4.1.10.2	Przycisk RESET	44
4.1.11	Gniazdo karty pamięci	45
4.2	Schemat połączeń wewnętrznych	46
4.3	Dane techniczne	47
4.3.1	Dane urządzenia	47
4.3.2	Dane systemowe	47
4.3.3	Zasilanie	48
4.3.4	Zegar	49

4.3.5	Programowanie	49
4.3.6	Magistrala systemowa	49
4.3.7	ETHERNET	50
4.3.8	CANopen	50
4.3.9	Technika podłączania przewodu	51
4.3.10	Warunki mechaniczne	51
4.3.11	Warunki klimatyczne	51
4.4	Aprobaty	53
4.5	Normy i dyrektywy	55
5	Opis funkcjonowania	62
5.1	Sieć	62
5.1.1	Konfiguracja interfejsów	62
5.1.1.1	Praca w trybie przełącznym	62
5.1.1.2	Praca przy rozłączonych interfejsach sieciowych	63
5.1.1.3	Przykłady przyporządkowania MAC-ID i adresów IP	64
5.1.2	Bezpieczeństwo sieci	65
5.1.2.1	Użytkownicy i hasła	65
5.1.2.1.1	Usługi i użytkownicy	65
5.1.2.1.2	Grupa użytkowników WBM	66
5.1.2.1.3	Grupa użytkowników Linux®	66
5.1.2.1.4	Grupa użytkowników SNMP	66
5.1.2.2	Uwierzytelnianie serwera WWW	67
5.1.2.2.1	Szyfrowanie TLS	67
5.1.2.3	Certyfikaty Root	69
5.1.3	Konfiguracja sieci	70
5.1.3.1	Nazwa hosta/nazwa domeny	70
5.1.3.2	Routing	70
5.1.4	Usługi sieciowe	73
5.1.4.1	DHCP Client	73
5.1.4.2	DHCP Server	73
5.1.4.3	DNS Server	75
5.1.5	Funkcjonalność Cloud Connectivity	76
5.1.5.1	Komponenty pakietu oprogramowania Cloud Connectivity	77
5.2	Funkcja karty pamięci	78
5.2.1	Formatowanie	78
5.2.2	Bezpieczeństwo danych	79
5.2.2.1	Funkcja „Backup“	79
5.2.2.2	Funkcja Restore	80
5.2.3	Wkładanie karty pamięci podczas pracy	82
5.2.4	Wyjmowanie karty pamięci podczas pracy	82
5.2.5	Ustawienia katalogu Home dla systemu runtime	83
5.2.6	Ładowanie projektu bootowalnego	83
5.3	Elementy oprogramowania wymagające licencji	85
6	Montaż	86
6.1	Pozycja montażu	86
6.1.1	Układ współrzędnych	86
6.1.2	Przegląd pozycji montażu	86
6.2	Konstrukcja	88
6.3	Montaż na szynie	88

6.3.1	Właściwości szyny montażowej	88
6.3.2	Szyny montażowe WAGO	90
6.4	Odstępy	91
6.5	Kolejność montażu	92
6.6	Montaż urządzeń	93
6.6.1	Montaż sterownika	93
6.6.2	Dodawanie modułów I/O	94
7	Podłączanie urządzeń	95
7.1	Styki magistrali obiektowej / zasilanie sieci obiektowej	95
7.2	Podłączanie przewodów do CAGE CLAMP®	96
7.3	Koncepcja zasilania	97
7.3.1	Dodatkowe przepisy dotyczące zasilania	98
7.3.2	Przykład zasilania	100
7.3.3	Zasilacze	101
7.4	Uziemienie	102
7.4.1	Uziemienie szyny montażowej	102
7.4.1.1	Zabudowa na ramie	102
7.4.1.2	Budowa izolowana	102
7.4.2	Uziemienie funkcjonalne	103
7.5	Ekranowanie	104
7.5.1	Informacje ogólne	104
7.5.2	Przewody sieci obiektowej	104
7.5.3	Ekranowane przewody sygnałowe	105
7.5.4	System łączenia ekranów	105
8	Uruchamianie	106
8.1	Włączanie sterownika	106
8.2	Ustalanie adresu IP hosta	107
8.3	Ustawianie adresu IP	108
8.3.1	Przydzielanie adresu IP za pomocą DHCP	109
8.3.2	Zmiana adresu IP za pomocą narzędzia konfiguracyjnego „CBM” i programu terminalowego	110
8.3.3	Zmiana adresu IP przy użyciu „WAGO Ethernet Settings”	113
8.3.4	Czasowe ustawienie stałego adresu IP	115
8.4	Testowanie połączenia sieciowego	116
8.5	Zmiana haseł	117
8.6	Wyłączanie / restart	118
8.7	Wyzwalanie funkcji RESET	119
8.7.1	Gorący reset	119
8.7.1.1	System runtime CODESYS V2	119
8.7.1.2	System runtime e!RUNTIME	119
8.7.2	Zimny reset	119
8.7.2.1	System runtime CODESYS V2	119
8.7.2.2	System runtime e!RUNTIME	120
8.7.3	Reset programowy (restart)	120
8.7.4	Reset fabryczny	120
8.8	Konfiguracja	122
8.8.1	Konfiguracja za pomocą systemu zarządzania przez WWW (WBM)	123
8.8.1.1	Zarządzanie użytkownikami WBM	125

8.8.1.2	Ogólne informacje o stronie	128
8.8.2	Konfiguracja za pomocą Console-Based-Management-Tool (CBM) przez program terminalowy	130
8.8.2.1	Struktura menu CBM	131
8.8.3	Konfiguracja za pomocą „WAGO Ethernet Settings“	134
8.8.3.1	Zakładka Identification	136
8.8.3.2	Zakładka Network	137
8.8.3.3	Zakładka PLC	139
8.8.3.4	Zakładka Status	140
9	Środowisko systemowe CODESYS 2.3	141
9.1	Instalacja środowiska programistycznego CODESYS 2.3	141
9.2	Pierwszy program z CODESYS 2.3	141
9.2.1	Otwieranie środowiska programistycznego CODESYS	141
9.2.2	Zakładanie projektu i wybór systemu docelowego	141
9.2.3	Konfiguracja sterownika	143
9.2.4	Edycja bloku funkcyjnego	149
9.2.5	Ładowanie programu PLC do sterownika	151
9.2.6	Tworzenie projektu bootowalnego	153
9.3	Sposób zapisywania adresów logicznych	153
9.4	Tworzenie zadań	154
9.4.1	Zadania cykliczne	157
9.4.2	Zadania dowolne	158
9.4.3	Debugowanie programu IEC	158
9.5	Zdarzenia systemowe	162
9.5.1	Tworzenia obsługi zdarzeń	165
9.6	Obrazy procesu	167
9.6.1	Obraz procesu dla modułów I/O podłączonych do sterownika	169
9.6.2	Obraz procesu dla urządzeń slave podłączonych do sieci obiektowej	170
9.7	Dostęp do obrazów procesu danych wejściowych i wyjściowych przez CODESYS 2.3	170
9.8	Przykład adresowania	172
9.9	Synchronizacja magistrali systemowej	173
9.9.1	Przypadek 1: Interwał zadania CODESYS mniejszy od cyklu magistrali systemowej	173
9.9.2	Przypadek 2: Interwał zadania CODESYS mniejszy od podwójnego cyklu magistrali systemowej	175
9.9.3	Przypadek 3: Interwał zadania CODESYS większy od podwójnego cyklu magistrali systemowej	176
9.9.4	Przypadek 4: Interwał zadania CODESYS większy niż 10 ms	177
9.9.5	Konfiguracja magistrali systemowej	178
9.9.5.1	Oddziaływanie trybu Update na zadania CODESYS	179
9.9.5.1.1	Asynchroniczny tryb Update	179
9.9.5.1.2	Synchroniczny tryb Update	180
9.10	Ustawienia pamięci w CODESYS	180
9.10.1	Pamięć programu	180
9.10.2	Pamięć danych i ograniczenie modułu	182
9.10.3	Pamięć RAM nieulotna	183

9.11	Ogólne ustawienia systemu docelowego	184
9.12	Wizualizacja CODESYS	184
9.12.1	Ograniczenia wizualizacji CODESYS	187
9.12.2	Usuwanie zakłóceń wizualizacji internetowej CODESYS	189
9.12.3	Często zadawane pytania na temat wizualizacji internetowej CODESYS	190
10	Środowisko systemowe e!RUNTIME	192
10.1	Wskazówki ogólne	192
10.2	Priorytety CODESYS V3	193
10.3	Zakresy pamięci w e!RUNTIME	194
10.3.1	Pamięć programu i danych	194
10.3.2	Ograniczenie modułu	194
10.3.3	Pamięć RAM nieulotna	194
11	Modbus – CODESYS V2	195
11.1	Informacje ogólne	195
11.2	Właściwości	195
11.3	Konfiguracja	196
11.3.1	Modbus settings	197
11.3.2	Modbus TCP settings	198
11.3.3	Modbus UDP settings	198
11.3.4	Modbus RTU settings	198
11.4	Wymiana danych	200
11.4.1	Obraz procesu	201
11.4.2	Zakres znaczników	202
11.4.3	Rejestry Modbus	203
11.4.4	Mapowanie Modbus	203
11.4.4.1	Mapowanie Modbus dla usług dostępu bitowego typu odczyt FC1, FC2	203
11.4.4.2	Mapowanie Modbus dla usług dostępu bitowego typu zapis FC5, FC15	204
11.4.4.3	Mapowanie Modbus dla usług dostępu do rejestru typu odczyt FC3, FC4, FC23	205
11.4.4.4	Mapowanie Modbus dla usług dostępu do rejestru typu zapis FC6, FC16, FC22, FC23	207
11.5	Rejestry Modbus WAGO	209
11.5.1	Właściwości obrazu procesu	210
11.5.1.1	Rejestr 0x1022 – Liczba rejestrów w obrazie procesu wejść Modbus	210
11.5.1.2	Rejestr 0x1023 – Liczba rejestrów w obrazie procesu wyjść Modbus	210
11.5.1.3	Rejestr 0x1024 – Liczba bitów w obrazie procesu wejść Modbus	210
11.5.1.4	Rejestr 0x1025 – Liczba bitów w obrazie procesu wyjść Modbus	210
11.5.2	Konfiguracja sieci	211
11.5.2.1	Rejestr 0x1028 – Konfiguracja IP	211
11.5.2.2	Rejestr 0x102A – liczba zastosowanych połączeń TCP	211
11.5.2.3	Rejestr 0x1030 – Modbus TCP Socket Timeout	211
11.5.2.4	Rejestr 0x1031 – Adres MAC interfejsu ETHERNET 1 (eth0)	211

11.5.2.5	Rejestr 0x1037 – zwłoka odpowiedzi Modbus TCP	211
11.5.3	Rejestr statusu PLC	212
11.5.4	Modbus watchdog	212
11.5.4.1	Rejestr 0x1100 – Watchdog Command	214
11.5.4.2	Rejestr 0x1101 – Watchdog Status	216
11.5.4.3	Rejestr 0x1102 – Watchdog Timeout	216
11.5.4.4	Rejestr 0x1103 – Watchdog Config	217
11.5.4.5	Rejestr 0x1104 – Watchdog Operation Mode	217
11.5.5	Rejestr stałych Modbus	218
11.5.6	Elektroniczna tabliczka znamionowa	218
11.5.6.1	Rejestr 0x2010 – wersja (firmware index)	218
11.5.6.2	Rejestr 0x2011 – kod serii	218
11.5.6.3	Rejestr 0x2012 – kod urządzenia	218
11.5.6.4	Rejestr 0x2013 – wersja major firmware	219
11.5.6.5	Rejestr 0x2014 – wersja minor firmware	219
11.5.6.6	Rejestr 0x2015 – wersja MBS	219
11.6	Diagnostyka	220
11.6.1	Diagnostyka dla Modbus master	220
11.6.2	Diagnostyka dla systemu runtime	220
11.6.3	Diagnostyka przez serwer błędów	220
12	Modbus – e!RUNTIME	223
12.1	Przegląd adresów Modbus	223
12.2	Rejestry Modbus	224
12.2.1	Modbus watchdog	226
12.2.1.1	Rejestr 0xFA00 – Watchdog Command	228
12.2.1.2	Rejestr 0xFA01 – Watchdog Timeout	229
12.2.1.3	Rejestr 0xFA02 – Watchdog Status	229
12.2.1.4	Rejestr 0xFA03 – Watchdog Config	230
12.2.1.5	Rejestr Modbus TCP Connection Watchdog	231
12.2.2	Rejestr statusu	232
12.2.2.1	Rejestr statusu PLC	232
12.2.3	Elektroniczna tabliczka znamionowa	232
12.2.3.1	Nr katalogowy	232
12.2.3.2	Wersja firmware	232
12.2.3.3	Wersja sprzętu	232
12.2.3.4	Firmware loader / Boot loader	232
12.2.4	Wersja obrazu procesu Modbus	232
12.2.5	Rejestr obrazu procesu Modbus	232
12.2.6	Rejestr stałych	233
12.2.7	Rejestr Live	233
12.3	Obliczanie mocy CPU Modbus master	234
13	CANopen master i slave	235
13.1	Katalog obiektów	235
13.2	Profil komunikacji	236
13.2.1	Konfiguracja mastera	240
13.3	Wymiana danych	242
13.3.1	Obiekty komunikacyjne sterownika	242
13.3.2	Adresowanie specyficzne dla sieci obiektowej	242
13.3.3	Przykłady definicji zmiennych sieciowych PFC	246

13.3.3.1	Dostęp w CODESYS do zmiennych PFC	246
13.3.3.2	Indeksu maksymalne	247
13.3.4	Konfiguracja CANopen master	249
13.3.4.1	Wybór mastera	249
13.3.4.2	Ustawianie parametrów mastera	250
13.3.4.3	Dodawanie urządzeń slave	253
13.3.4.4	Konfiguracja PDO dla urządzeń slave	260
13.3.4.5	Konfiguracja obiektów Service Data	263
13.3.5	Konfiguracja CANopen slave	266
13.3.5.1	Konfiguracja zmiennych CANopen	267
13.3.5.2	Konfiguracja parametrów CANopen	268
13.4	Diagnostyka interfejsu sieciowego	269
13.4.1	BusDiag.lib	269
13.4.1.1	Tworzenie funkcji diagnostycznych w CODESYS 2.3	270
13.4.1.2	Wywołanie bloku diagnostycznego	272
13.4.1.3	Przeprowadzanie diagnostyki sieci za pomocą DiagGetBusState	273
13.4.1.4	Przeprowadzanie diagnostyki urządzenia za pomocą DiagGetState	275
13.4.1.5	Weryfikacja diagnostyki CANopen (komunikaty Emergency)	276
13.4.2	WagoCANopenDiag.lib	278
13.5	Wymiana danych pomiędzy Simple CAN Subscribers i sterownikiem w sieci CANopen	279
13.6	Wymiana danych między prostymi urządzeniami sieci CAN i PFC200 w sieci CAN Layer2	282
14	Diagnostyka	283
14.1	Komunikaty o pracy i statusie	283
14.1.1	LED dla zasilania	283
14.1.1.1	LED „A”	283
14.1.1.2	LED „C”	283
14.1.2	LED dla systemu / sieci obiektowej	284
14.1.2.1	LED „SYS”	284
14.1.2.2	LED „RUN”	287
14.1.2.3	LED „I/O”	290
14.1.2.4	LED „MS”	291
14.1.2.5	LED „CAN”	292
14.1.3	LED dla złącz sieciowych	293
14.1.4	LED gniazda karty pamięci	294
14.2	Komunikaty diagnostyczne przy użyciu sekwencji migania	295
14.2.1	Przebieg sekwencji migania	295
14.2.2	Przykład komunikatu diagnostycznego przy użyciu sekwencji migania	296
14.2.3	Kody migania LED „I/O” i sposoby usuwania błędu	297
14.2.4	Kody migania LED „MS” i sposoby usuwania błędu	303
15	Serwis	304
15.1	Wkładanie i wyjmowanie karty pamięci	304
15.1.1	Wkładanie karty pamięci	304
15.1.2	Wyjmowanie karty pamięci	304
15.2	Zmiany firmware	305

15.2.1	Aktualizacja firmware standardowa / wsteczna przy użyciu e!COCKPIT.....	306
15.2.2	Aktualizacja firmware standardowa / wsteczna przy użyciu WAGOupload.....	307
15.2.3	Aktualizacja firmware standardowa / wsteczna przy użyciu karty pamięci i WBM.....	308
15.3	Aktualizacja certyfikatów Root	309
16	Demontaż.....	310
16.1	Usuwanie urządzeń	310
16.1.1	Demontaż sterownika.....	310
16.1.2	Demontaż modułu I/O	311
17	Utylizacja	312
17.1	Sprzęt elektryczny i elektroniczny	312
17.2	Opakowanie	312
18	Użytkowanie w przestrzeniach zagrożonych wybuchem	314
18.1	Przykładowa konstrukcja i oznaczanie.....	315
18.1.1	Oznaczanie dla Europy zgodne z ATEX i IECEx.....	315
18.1.2	Oznaczanie na USA (NEC) i Kanadę (CEC)	319
18.2	Warunki stosowania	322
18.2.1	Szczególne wskazówki i ochrona przeciwwybuchowa.....	322
18.2.2	Szczególne informacje dotyczące UL Hazardous Location	324
19	Załącznik.....	325
19.1	Dialogi konfiguracyjne	325
19.1.1	Web Based Management (WBM).....	325
19.1.1.1	Zakładka „Information“.....	325
19.1.1.1.1	Strona „Device Status“	325
19.1.1.1.2	Strona „Vendor Information“.....	327
19.1.1.1.3	Strona „PLC Runtime Information“	328
19.1.1.1.4	Strona „WAGO Software License Agreement“	330
19.1.1.1.5	Strona „Open Source Licenses“	331
19.1.1.1.6	Strona „WBM Third Party License Information“	332
19.1.1.1.7	Strona „WBM Version“	333
19.1.1.2	Zakładka „Configuration“	334
19.1.1.2.1	Strona „PLC Runtime Configuration“	334
19.1.1.2.2	Strona „TCP/IP Configuration“	337
19.1.1.2.3	Strona „Ethernet Configuration“	339
19.1.1.2.4	Strona „Configuration of Host and Domain Name“	342
19.1.1.2.5	Strona „Routing“	344
19.1.1.2.6	Strona „Clock Settings“	348
19.1.1.2.7	Strona „Configuration of Service Interface“	350
19.1.1.2.8	Strona „Create bootable Image“.....	351
19.1.1.2.9	Strona „Firmware Backup“	352
19.1.1.2.10	Strona „Firmware Restore“.....	354
19.1.1.2.11	Strona „Active System“	356
19.1.1.2.12	Strona „Mass Storage“	357
19.1.1.2.13	Strona „Software Uploads“	358
19.1.1.2.14	Strona „Configuration of Network Services“	359

19.1.1.2.15	Strona „Configuration of NTP Client“	361
19.1.1.2.16	Strona „PLC Runtime Services“	362
19.1.1.2.17	Strona „SSH Server Settings“	364
19.1.1.2.18	Strona „TFTP Server“	365
19.1.1.2.19	Strona „DHCP Server Configuration“	366
19.1.1.2.20	Strona „Configuration of DNS Server“	367
19.1.1.2.21	Strona „Status overview“	368
19.1.1.2.22	Strona „Configuration of Connection <n>“	369
19.1.1.2.23	Strona „Configuration of general SNMP parameters“	374
19.1.1.2.24	Strona „Configuration of SNMP v1/v2c parameters“	375
19.1.1.2.25	Strona „Configuration of SNMP v3 Users“	377
19.1.1.2.26	Strona „WBM User Configuration“	379
19.1.1.3	Zakładka „Fieldbus“	380
19.1.1.3.1	Strona „OPC UA Status“	380
19.1.1.3.2	Strona „OPC UA Configuration“	381
19.1.1.3.3	Strona „OPC UA Information Model“	384
19.1.1.3.4	Strona „Modbus Services Configuration“	385
19.1.1.3.5	Strony „BACnet ...“	386
19.1.1.4	Zakładka „Security“	387
19.1.1.4.1	Strona „OpenVPN / IPsec Configuration“	387
19.1.1.4.2	Strona „General Firewall Configuration“	389
19.1.1.4.3	Strona „Interface Configuration“	390
19.1.1.4.4	Strona „Configuration of MAC address filter“	391
19.1.1.4.5	Strona „Configuration of User Filter“	393
19.1.1.4.6	Strona „Certificates“	396
19.1.1.4.7	Grupa „Security Settings“	397
19.1.1.4.8	Strona „Advanced Intrusion Detection Environment (AIDE)“	398
19.1.1.5	Zakładka „Diagnostic“	400
19.1.1.5.1	Strona „Diagnostic Information“	400
19.1.2	Console-Based-Management (CBM)	401
19.1.2.1	Menu „Information“	401
19.1.2.1.1	Podmenu „Information“ > „Controller Details“	401
19.1.2.1.2	Podmenu „Information“ > „Network Details“	402
19.1.2.2	Menu „PLC Runtime“	403
19.1.2.2.1	Podmenu „PLC Runtime“ > „Information“	403
19.1.2.2.2	Podmenu „Information“ > „Runtime Version“	404
19.1.2.2.3	Podmenu „Information“ > „Webserver Version“	404
19.1.2.2.4	Podmenu „Information“ > „State“	404
19.1.2.2.5	Podmenu „Information“ > „Number of Tasks“	405
19.1.2.2.6	Podmenu „Information“ > „Project Details“	405
19.1.2.2.7	Podmenu „Information“ > „Tasks“	405
19.1.2.2.8	Podmenu „Tasks“ > „Task n“	406
19.1.2.2.9	Podmenu „PLC Runtime“ > „General Configuration“	406
19.1.2.2.10	Podmenu „General Configuration“ > „PLC Runtime Version“	407
19.1.2.2.11	Podmenu „General Configuration“ > „Home Dir On SD Card“	407
19.1.2.2.12	Podmenu „PLC Runtime“ > „WebVisu“	408
19.1.2.3	Menu „Networking“	409
19.1.2.3.1	Podmenu „Networking“ > „Host-/Domain Name“	409
19.1.2.3.2	Podmenu „Host-/Domain Name“ > „Hostname“	410

19.1.2.3.3	Podmenu „Host-/Domain Name“ > „Domain Name“	410
19.1.2.3.4	Podmenu „Networking“ > „TCP/IP“	410
19.1.2.3.5	Podmenu „TCP/IP“ > „IP Address“	411
19.1.2.3.6	Podmenu „IP Address“ > „Xn“	411
19.1.2.3.7	Podmenu „TCP/IP“ > „Default Gateway“	412
19.1.2.3.8	Podmenu „Default Gateway“ > „Default Gateway n“	412
19.1.2.3.9	Podmenu „TCP/IP“ > „DNS Server“	413
19.1.2.3.10	Podmenu „Networking“ > „Ethernet“	413
19.1.2.3.11	Podmenu „Ethernet“ > „Switch Configuration“	414
19.1.2.3.12	Podmenu „Ethernet“ > „Ethernet Ports“	414
19.1.2.3.13	Podmenu „Ethernet Ports“ > „Interface Xn“	415
19.1.2.4	Podmenu „Firewall“	416
19.1.2.4.1	Podmenu „Firewall“ > „General Configuration“	417
19.1.2.4.2	Podmenu „General Configuration“ > „Interface xxx“	418
19.1.2.4.3	Podmenu „Firewall“ > „MAC Address Filter“	420
19.1.2.4.4	Podmenu „MAC Address Filter“ > „MAC address filter whitelist“	421
19.1.2.4.5	Podmenu „MAC address filter whitelist“ > „Add new / No (n)“	421
19.1.2.4.6	Podmenu „Firewall“ > „User Filter“	422
19.1.2.4.7	Podmenu „User Filter“ > „Add New / No (n)“	423
19.1.2.5	Menu „Clock“	424
19.1.2.6	Menu „Administration“	425
19.1.2.6.1	Podmenu „Administration“ > „Users“	426
19.1.2.6.2	Podmenu „Administration“ > „Create Image“	426
19.1.2.7	Menu „Package Server“	427
19.1.2.7.1	Podmenu „Package Server“ > „Firmware Backup“	427
19.1.2.7.2	Podmenu „Firmware Backup“ > „Auto Update Feature“	428
19.1.2.7.3	Podmenu „Firmware Backup“ > „Destination“	428
19.1.2.7.4	Podmenu „Package Server“ > „Firmware Restore“	429
19.1.2.7.5	Podmenu „Firmware Restore“ > „Select Package“	429
19.1.2.7.6	Podmenu „Package Server“ > „System Partition“	430
19.1.2.8	Menu „Mass Storage“	431
19.1.2.8.1	Podmenu „Mass Storage“ > „SD Card“	431
19.1.2.9	Menu „Software Uploads“	432
19.1.2.10	Menu „Ports and Services“	433
19.1.2.10.1	Podmenu „Ports and Services“ > „Telnet“	434
19.1.2.10.2	Podmenu „Ports and Services“ > „FTP“	434
19.1.2.10.3	Podmenu „Ports and Services“ > „FTPS“	435
19.1.2.10.4	Podmenu „Ports and Services“ > „HTTP“	435
19.1.2.10.5	Podmenu „Ports and Services“ > „HTTPS“	436
19.1.2.10.6	Podmenu „Ports and Services“ > „NTP“	436
19.1.2.10.7	Podmenu „Ports and Services“ > „SSH“	437
19.1.2.10.8	Podmenu „Ports and Services“ > „TFTP“	437
19.1.2.10.9	Podmenu „Ports and Services“ > „DHCPD“	438
19.1.2.10.10	Podmenu „DHCPD“ > „Xn“	438
19.1.2.10.11	Podmenu „Ports and Services“ > „DNS“	439
19.1.2.10.12	Podmenu „Ports and Services“ > „IOCHECK PORT“	440
19.1.2.10.13	Podmenu „Ports and Services“ > „Modbus TCP“	440
19.1.2.10.14	Podmenu „Ports and Services“ > „Modbus UDP“	441
19.1.2.10.15	Podmenu „Ports and Services“ > „OPC UA“	441

19.1.2.10.16	Podmenu „...“ > „Firewall Status“	442
19.1.2.10.17	Podmenu „Ports and Services“ > „PLC Runtime Services“	443
19.1.2.10.18	Podmenu „PLC Runtime Services“ > „CODESYS 2“	444
19.1.2.10.19	Podmenu „PLC Runtime Services“ > „e!RUNTIME“	445
19.1.2.11	Menu „SNMP“	446
19.1.2.11.1	Podmenu „SNMP“ > „General SNMP Configuration“	446
19.1.2.11.2	Podmenu „SNMP“ > „SNMP v1/v2c Manager Configuration“	446
19.1.2.11.3	Podmenu „SNMP“ > „SNMP v1/v2c Trap Receiver Configuration“	447
19.1.2.11.4	Podmenu „SNMP“ > „SNMP v3 Configuration“	447
19.1.2.11.5	Podmenu „SNMP“ > „(Secure)SNMP firewalling“	449
19.2	Budowa danych procesowych	450
19.2.1	Moduły wejść dwustanowych	451
19.2.1.1	2-kanalowe moduły wejść dwustanowych	451
19.2.1.2	8-kanalowe moduły wejść dwustanowych	451
19.2.1.3	16-kanalowe moduły wejść dwustanowych	451
19.2.2	Moduły wyjść dwustanowych	452
19.2.2.1	2-kanalowe moduły wyjść dwustanowych	452
19.2.2.2	2-kanalowe moduły wyjść dwustanowych z diagnostyką i danymi wejściowymi	452
19.2.2.3	4-kanalowe moduły wyjść dwustanowych	453
19.2.2.4	4-kanalowe moduły wyjść dwustanowych z diagnostyką i danymi wejściowymi	453
19.2.2.5	8-kanalowe moduły wyjść dwustanowych	453
19.2.2.6	8-kanalowe moduły wyjść dwustanowych z diagnostyką i danymi wejściowymi	454
19.2.2.7	16-kanalowe moduły wyjść dwustanowych	454
19.2.3	Moduły wejść analogowych	455
19.2.3.1	2-kanalowe moduły wejść analogowych	455
19.2.3.2	4-kanalowe moduły wejść analogowych	455
19.2.3.3	Moduł pomiaru mocy 3-fazowy	455
19.2.4	Moduły wyjść analogowych	457
19.2.4.1	2-kanalowe moduły wyjść analogowych	457
19.2.4.2	4-kanalowe moduły wyjść analogowych	457
19.2.5	Funkcyjne moduły I/O	458
19.2.5.1	Interfejsy szeregowo z alternatywnym formatem danych	458
19.2.5.2	Moduł interfejsu SSI	459
19.2.5.3	Moduł pomiaru odległości i kąta	459
19.2.5.4	Liczniki	459
19.2.5.5	Moduł gateway CAN	461
19.3	Biblioteki CODESYS V2	462
19.3.1	Biblioteki ogólne	462
19.3.1.1	Biblioteki systemowe CODESYS	462
19.3.1.2	SysLibFile.lib	463
19.3.1.3	SysLibFileAsync.lib	464
19.3.1.4	SysLibRtc.lib	465
19.3.1.5	BusDiag.lib	465
19.3.1.6	mod_com.lib	465
19.3.1.7	SerComm.lib	466
19.3.1.8	WagoConfigToolLIB.lib	466

19.3.1.9	WagoLibCpuUsage.lib	487
19.3.1.10	WagoLibDiagnosticIDs.lib	487
19.3.1.11	WagoLibLed.lib	487
19.3.1.12	WagoLibNetSnmp.lib	487
19.3.1.13	WagoLibNetSnmpManager.lib	488
19.3.1.14	WagoLibSSL.lib	488
19.3.1.15	WagoLibTerminalDiag.lib	489
19.3.2	Biblioteki do integracji CANopen i CANLayer2	490
19.3.2.1	WagoCANLayer2_02.lib	490
19.3.2.2	WagoCANopen_02.lib	490
19.3.2.3	WagoCANopenDiag.lib	491
Spis ilustracji.....		492
Spis tabel		496

1 Wskazówki dotyczące dokumentacji

Wskazówka



Zachować dokumentację!

Niniejsza dokumentacja jest częścią produktu. Dlatego należy ją przechowywać przez cały czas użytkowania produktu. Dokumentację tę należy przekazać kolejnemu właścicielowi lub użytkownikowi produktu. Należy również zapewnić aktualizację dokumentacji o pojawiające się uzupełnienia.

1.1 Zakres obowiązywania

Niniejsza dokumentacja odnosi się do sterownika „PFC200 G2 2ETH M12 CAN XTR” (750-8213/040-010).

Niniejsza dokumentacja odnosi się do wersji od FW 03.06.09(18) i nowszych.

1.2 Prawa autorskie

Niniejsza dokumentacja, wraz ze wszystkimi zawartymi w niej ilustracjami, jest chroniona prawami autorskimi. Wszelkie zastosowanie niniejszej dokumentacji niezgodne z przepisami prawa autorskiego jest zabronione. Reprodukacja, tłumaczenie na inne języki, jak również archiwizacja elektroniczna i fototechniczna i modyfikacja wymagają pisemnej zgody ze strony firmy WAGO GmbH & Co. KG, Minden. Nieprzestrzeganie tego zalecenia upoważnia do wnoszenia roszczeń odszkodowawczych.

1.3 Prawa własności

W niniejszej dokumentacji wykorzystano znaki towarowe firm trzecich. Marki te zestawiono w tym rozdziale. Tym samym w dalszej części dokumentacji zrezygnowano ze stosowania znaków „®” i „™”.

- Adobe® i Acrobat® są zarejestrowanymi markami Adobe Systems Inc.
- AS-Interface® jest zarejestrowaną marką AS-International Association.
- BACnet® jest zarejestrowaną marką American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc. (ASHRAE).
- *Bluetooth*® jest zarejestrowanym znakiem towarowym Bluetooth SIG, Inc.
- CiA® i CANopen® są zarejestrowanymi markami CAN in AUTOMATION – International Users and Manufacturers Group e. V.
- DALI jest zarejestrowaną marką Digital Illumination Interface Alliance (DiiA).
- EtherCAT® jest zarejestrowaną marką i opatentowaną technologią Beckhoff Automation GmbH.
- EtherNet/IP™ jest zarejestrowaną marką Open DeviceNet Vendor Association, Inc (ODVA).
- EnOcean® jest zarejestrowaną marką EnOcean GmbH.
- IO-Link jest zarejestrowaną marką PROFIBUS Nutzerorganisation e.V.
- KNX® jest zarejestrowaną marką KNX Association cvba.
- Linux® jest zarejestrowaną marką Linus Torvalds.
- LON® jest zarejestrowaną marką Echelon Corporation.
- Modbus® jest zarejestrowaną marką Schneider Electric, z licencją dla Modbus Organization, Inc.
- PROFIBUS® jest zarejestrowaną marką Siemens AG.
- PROFINET® jest zarejestrowaną marką Siemens AG.
- QR Code jest zarejestrowaną marką DENSO WAVE INCORPORATED.
- Subversion® jest zarejestrowaną marką Apache Software Foundation.
- Windows® jest zarejestrowaną marką Microsoft Corporation.

1.4 Symbole

NIEBEZPIECZEŃSTWO



Niebezpieczeństwo obrażeń ciała!

Wskazuje na bezpośrednie zagrożenie o wysokim stopniu ryzyka, które w przypadku braku wyeliminowania może doprowadzić do śmierci lub poważnych obrażeń ciała.

NIEBEZPIECZEŃSTWO



Niebezpieczeństwo porażenia prądem elektrycznym!

Wskazuje na bezpośrednie zagrożenie o wysokim stopniu ryzyka, które w przypadku braku wyeliminowania może doprowadzić do śmierci lub poważnych obrażeń ciała.

OSTRZEŻENIE



Ostrzeżenie przed obrażeniami ciała!

Wskazuje na potencjalne zagrożenie o średnim stopniu ryzyka, które w przypadku braku wyeliminowania może skutkować śmiercią lub poważnymi obrażeniami ciała.

OSTROŻNIE



Ostrożnie, możliwość wystąpienia obrażeń ciała!

Wskazuje na potencjalne zagrożenie o niskim stopniu ryzyka, które w przypadku braku wyeliminowania może spowodować niewielkie lub umiarkowane obrażenia ciała.

UWAGA



Uwaga, możliwość wystąpienia szkód materialnych!

Wskazuje na prawdopodobieństwo wystąpienia zagrożenia, które w przypadku braku wyeliminowania może doprowadzić do powstania szkód materialnych.

ESD



Ostrzeżenie przed szkodami materialnymi w następstwie wyładowań elektrostatycznych!

Wskazuje na prawdopodobieństwo wystąpienia zagrożenia, które w przypadku braku wyeliminowania może doprowadzić do powstania szkód materialnych.

Wskazówka



Ważna wskazówka

Wskazuje na prawdopodobieństwo nieprawidłowego funkcjonowania, które w przypadku braku wyeliminowania nie prowadzi jednak do szkód materialnych.

Informacja



Dodatkowa informacja

Odsyła do dalszych informacji, niestanowiących istotnej części dokumentacji (np. do informacji zawartych na stronie www).

1.5 Zastosowane systemy liczbowe

Tabela 1: Zastosowane systemy liczbowe

System liczbowy	Przykładowy nr kat.	Uwaga
Dziesiętny	100	Zwykły zapis
Szesnastkowy	0x64	Notacja szesnastkowa
Binarny	'100' '0110.0100'	Zapis w apostrofach, półbajt oddzielony kropką

1.6 Sposoby zapisu

Tabela 2: Sposoby zapisu

Czcionka	Znaczenie
<i>kursywa</i>	Nazwy ścieżek i plików są zapisywane kursywą, np.: <i>C:\Programy\Oprogramowanie WAGO</i>
Menu	Punkty menu są pogrubione, np.: Zapisz
>	Znak „większy od” między dwiema nazwami oznacza wybór określonego punktu menu, np.: Plik > Nowy
Pole edycji	Nazwy pól do wprowadzania lub wyboru danych są przedstawiane pogrubioną czcionką, np.: Początek zakresu pomiarowego
„wartość“	Wartości wprowadzane lub wybierane są zapisywane w cudzysłowie, np.: w polu Początek zakresu pomiarowego wprowadź wartość „4 mA”.
[Przycisk]	Nazwy przycisków znajdujących się w polach dialogowych są przedstawione pogrubioną czcionką i ujęte są w nawias kwadratowy, np. [Wprowadzanie]
[Klawisz]	Nazwy klawiszy na klawiaturze są przedstawione pogrubioną czcionką i ujęte są w nawias kwadratowy, np. [F5]

2 Ważne objaśnienia

Rozdział ten zawiera wyłącznie zestawienie najważniejszych zasad bezpieczeństwa oraz wskazówek. Zostaną one także przedstawione w poszczególnych rozdziałach. W celu ochrony przed obrażeniami ciała oraz zapobiegania uszkodzeniom urządzeń, konieczne jest staranne zapoznanie się ze wskazówkami dotyczącymi bezpieczeństwa oraz ich przestrzeganie.

2.1 Podstawy prawne

2.1.1 Zastrzeżenie prawa do zmian technicznych

Firma WAGO GmbH & Co. KG zastrzega sobie prawo do zmian. W przypadku udzielania patentu lub ochrony wzoru użytkowego, wszystkie prawa są zastrzeżone dla WAGO GmbH & Co. KG. Produkty obce są wymieniane bez podawania informacji o prawach patentowych. Dlatego nie można wykluczyć istnienia tego rodzaju praw.

2.1.2 Kwalifikacje personelu

Wszystkie prace przy urządzeniach WAGO I/O System 750 mogą być wykonywane wyłącznie przez wykwalifikowanych elektryków z odpowiednią wiedzą fachową w zakresie techniki automatyzacji. Osoby te muszą znać aktualne normy i wytyczne dotyczące AKPiA.

Wszelkie ingerencje w układ sterowania wolno wykonywać wyłącznie specjalistom, dysponującym odpowiednią wiedzą z zakresu programowania PLC.

2.1.3 Stosowanie serii 750 zgodne z przeznaczeniem

Interfejsy sieciowe, sterowniki oraz moduły I/O modularnego systemu o nazwie WAGO I/O System 750 służą do odczytu sygnałów dwustanowych i analogowych z czujników i wystawiania ich dla elementów wykonawczych lub przesyłania do nadrzędnych układów sterowania. Przy użyciu sterowników możliwe jest ich (wstępne) przetwarzanie.

Produkt ma stopień ochrony IP20 i jest przeznaczony do zastosowania w suchych pomieszczeniach. Charakteryzuje się on ochroną przed dotykiem oraz wnikaniem ciał stałych o wielkości $\geq 12,5$ mm, lecz brakiem ochrony przed wnikaniem wody. Produkt jest otwartym urządzeniem elektrycznym. Może być używany wyłącznie w osłonach (montowanych fabrycznie obudowach lub rozdzielniach), spełniających wymagania opisane w rozdziale „Wskazówki dotyczące bezpieczeństwa”.

Zastosowanie produktu bez środków ochronnych w środowisku, w którym może wystąpić wilgoć, kurz, żrące opary, gazy lub promieniowanie jonizujące, traktowane jest jako użytkowanie niezgodne z przeznaczeniem.

Produkt jest przeznaczony do zastosowania w instalacjach automatyki. Nie jest wyposażony we własne zintegrowane zabezpieczenie rozłączające. Dlatego odpowiednie zabezpieczenie rozłączające należy stworzyć po stronie instalacji.

Używanie produktu w pomieszczeniach mieszkalnych bez dodatkowych środków jest dozwolone tylko wówczas, gdy spełniają one wymagania dotyczące granic emisji (emisje zakłóceń) zgodnie z EN 61000-6-3.

Odpowiednie informacje znajdują się w rozdziale „Opis urządzenia” > „Normy i dyrektywy” podręcznika dotyczącego zastosowanego produktu.

Zastosowanie WAGO I/O System 750 w przestrzeniach zagrożonych wybuchem wymaga specjalnej obudowy ochronnej, zgodnie z dyrektywą 2014/34/WE.

Należy uwzględnić warunki stosowania!

Dodatkowo należy pamiętać, że konieczne jest uzyskanie świadectwa badania typu, potwierdzającego prawidłowy montaż systemu w obudowie lub szafie sterowniczej.

Wdrożenie funkcji bezpieczeństwa, takich jak wyłączniki awaryjne lub monitorowanie drzwi bezpieczeństwa, może być realizowane tylko przez moduły F-I/O modułarnego systemu WAGO I/O System 750. Tylko te bezpieczne moduły F-I/O zapewniają bezpieczeństwo funkcjonalne, zgodnie z najnowszymi standardami międzynarodowymi. Bezreakcyjne moduły wyjściowe WAGO mogą być sterowane za pomocą funkcji bezpieczeństwa.

2.1.4 Stan techniczny urządzeń

Urządzenia są dostarczane na potrzeby danego zastosowania, w sprzętowej i programowej konfiguracji fabrycznej. Nie zawierają żadnych części, które wymagają od użytkownika konserwacji czy napraw. Wykonanie następujących czynności powoduje wyłączenie odpowiedzialności WAGO GmbH & Co. KG:

- naprawy
- wprowadzanie zmian w sprzęcie lub oprogramowaniu, które nie są opisane w instrukcji obsługi
- użycie komponentów niezgodnie z ich przeznaczeniem

Więcej szczegółów można znaleźć w postanowieniach umowy. Prośby i zapytania dotyczące zmiany konfiguracji lub nowej konfiguracji osprzętu i oprogramowania należy kierować do firmy WAGO GmbH & Co. KG.

2.2 Wskazówki dotyczące bezpieczeństwa

Przy zabudowie urządzenia w instalacji oraz w trakcie jego instalacji należy przestrzegać następujących zasad bezpieczeństwa:

NIEBEZPIECZEŃSTWO Nie pracować przy urządzeniach znajdujących się pod napięciem!



Przed rozpoczęciem montażu, usuwania usterek lub prac konserwacyjnych należy zawsze odłączyć urządzenie od zasilania.

NIEBEZPIECZEŃSTWO Zabudować produkt w odpowiedniej obudowie!



Produkt jest otwartym urządzeniem elektrycznym. Produkt należy zabudować w odpowiedniej obudowie. Obudowa powinna:

- gwarantować, że maks. dopuszczalny stopień zanieczyszczenia nie zostanie przekroczony,
 - gwarantować odpowiednią ochronę przed dotykiem,
 - zapewniać wystarczającą ochronę przed promieniowaniem UV,
 - zapobiegać rozprzestrzenianiu się ognia poza obudowę,
 - zapewniać odporność na obciążenia mechaniczne.
 - pozwalać na dostęp tylko upoważnionemu personelowi i otwierać się wyłącznie przy użyciu narzędzi.
-

NIEBEZPIECZEŃSTWO Zapewnić odpowiednie zabezpieczenie rozłączające i ochronę przed przetężeniem!



Urządzenie jest przeznaczone do zastosowania w instalacjach automatyki. Nie jest wyposażone we własne zintegrowane zabezpieczenie rozłączające. Podłączone instalacje muszą być zabezpieczone. Dlatego po stronie instalacji należy przewidzieć odpowiednie zabezpieczenie rozłączające i ochronę przed przetężeniem.

NIEBEZPIECZEŃSTWO Przestrzegać przepisów dotyczących zapobiegania wypadkom!



W trakcie montażu, uruchamiania, eksploatacji, konserwacji i usuwania usterek należy zawsze przestrzegać przepisów dotyczących zapobiegania wypadkom, właściwych dla danego urządzenia/układu.

NIEBEZPIECZEŃSTWO**Podłączać urządzenie zgodnie z przepisami!**

W celu wyeliminowania zagrożeń personelu oraz usterek instalacji przewody transmisji danych i zasilające należy układać zgodnie z obowiązującymi normami, pamiętając o odpowiednim usytuowaniu przyłączy. Należy przestrzegać zasad kompatybilności elektromagnetycznej dla danego zastosowania.

OSTRZEŻENIE**Zasilanie wyłącznie napięciem SELV/PELV!**

Wszystkie sygnały i zasilacze po stronie obiektowej, podłączane do sterownika XTR (750-8213/040-010) muszą być zasilane napięciem SELV/PELV!

OSTRZEŻENIE**Nie dotykać gorących powierzchni!**

Podczas pracy powierzchnia obudowy może się nagrzewać. Jeśli urządzenie pracowało w otoczeniu o wysokiej temperaturze, przed dotknięciem należy poczekać, aż ostygnie.

UWAGA**Zapewnić odpowiedni styk z szyną montażową!**

Aby zachować właściwości EMC i zapewnić właściwe działanie urządzenia, konieczny jest odpowiedni, elektryczny styk między urządzeniem a szyną montażową.

UWAGA**Wymienić wadliwe lub uszkodzone urządzenia!**

Wadliwe lub uszkodzone urządzenia (np. ze zdeformowanymi stykami) należy wymienić.

UWAGA**Chronić urządzenia przed materiałami o właściwościach pełzających i izolacyjnych!**

Urządzenia nie są odporne na materiały o właściwościach pełzających i izolacyjnych, jak np. aerozole, silikony, trójglicerydy (składnik kremu do rąk). Jeżeli nie da się wykluczyć obecności tych substancji w pobliżu urządzeń, należy umieścić urządzenia w obudowie odpornej na działanie ww. środków. Generalnie do obsługi urządzeń należy używać czystych narzędzi i materiałów.

UWAGA**Czyścić wyłącznie przy użyciu dozwolonych materiałów!**

Obudowę i zabrudzone styki należy czyścić propanolem.

UWAGA**Nie stosować sprayu do styków!**

Nie należy stosować sprayu do styków, gdyż w połączeniu z zanieczyszczeniami może on pogorszyć jakość miejsca styku.

UWAGA



Unikać zmian biegunowości!

Należy unikać zmiany biegunowości przewodów transmisji danych i zasilających, gdyż może to spowodować uszkodzenia urządzenia.

ESD



Unikać wyładowań elektrostatycznych!

W urządzeniu zintegrowane są komponenty elektroniczne, które mogą zostać zniszczone przez wyładowania elektrostatyczne w następstwie dotknięcia. Należy stosować środki ochrony przed wyładowaniami elektrostatycznymi zgodnie z normą DIN EN 61340-5-1/-3. Przy obsłudze urządzenia należy pamiętać o odpowiednim uziemieniu otoczenia (osoby, stanowisko pracy oraz opakowanie).

UWAGA



Nie stosować w sieciach telekomunikacyjnych!

Urządzenia ze złączem ETHERNET/RJ-45 należy używać wyłącznie w sieciach LAN. Nie należy ich łączyć z sieciami telekomunikacyjnymi, jak np. z liniami telefonicznymi analogowymi lub cyfrowymi (ISDN).

UWAGA



Pomiar izolacji przeprowadzić wyłącznie przy użyciu napięcia stałego (DC)!

Moduły po stronie magistrali systemowej i obiektowej są sprzężone pojemnościowo z szyną montażową. Jeśli moduł I/O jest zamontowany na szynie, założenie napięcia przemiennego między szyną montażową a co najmniej jednym z tych dwóch potencjałów może spowodować jego zniszczenie. Dlatego test izolacji należy przeprowadzić wyłącznie przy użyciu napięcia stałego (DC). Przed ponownym przyłożeniem napięcia pomiarowego doprowadzić do całkowitego rozładowania urządzenia, aby nie uszkodzić modułu I/O.

2.3 Warunki licencji dla zastosowanych pakietów oprogramowania

Firmware sterownika „PFC200 G2 2ETH M12 CAN XTR“ (750-8213/040-010) zawiera otwarte oprogramowanie.

Warunki licencji dla zastosowanych pakietów oprogramowania zapisane są w formie tekstowej w sterowniku. Można je znaleźć na stronie WBM „Legal Information“ > „Open Source Software“.

Kod źródłowy z warunkami licencji dla otwartego oprogramowania można otrzymać także na życzenie od firmy WAGO GmbH & Co. KG. Zamówienie należy wysłać na adres support@wago.com z tematem wiadomości „Controller Board Support Package“.

2.4 Specjalne warunki zastosowania urządzeń ETHERNET

Tam gdzie nie ma specjalnych uwarunkowań, urządzenia ETHERNET można stosować w sieciach lokalnych. Przy wykorzystaniu urządzeń ETHERNET należy przestrzegać następujących zasad bezpieczeństwa:

- Komponentów systemu sterowania oraz sieci sterowniczych nie należy łączyć bezpośrednio z otwartą siecią, na przykład Internetem lub siecią biurową. WAGO zaleca umieszczenie sieci sterowniczych za firewallem.
- Aby zredukować niebezpieczeństwo cyberataku i tym samym zwiększyć cyberbezpieczeństwo, wszystkie porty i usługi w komponentach systemu sterowania, które nie są wykorzystywane przez aplikację (np. dla WAGO-I/O-CHECK i CODESYS) należy zamykać. Porty i usługi dobrze jest otwierać tylko na czas uruchamiania lub konfiguracji.
- Fizyczny i elektroniczny dostęp do wszystkich komponentów automatyki należy ograniczyć do kręgu osób upoważnionych.
- Przed pierwszym uruchomieniem należy koniecznie zmienić ustawione standardowo hasła! W ten sposób redukuje się ryzyko ingerencji osób nieupoważnionych w system.
- Używane hasła należy regularnie zmieniać! W ten sposób redukuje się ryzyko ingerencji osób nieupoważnionych w system.
- W przypadku konieczności zdalnego dostępu do komponentów systemu sterowania i sieci sterowniczej, należy korzystać z sieci „Virtual Private Network“ (VPN).
- Należy regularnie przeprowadzać analizę zagrożeń. Pozwala to na sprawdzenie, czy podjęte działania odpowiadają wymogom w zakresie ochrony.
- Przy projektowaniu instalacji należy zastosować mechanizmy „Defense-in-depth“ w celu ograniczenia dostępu do indywidualnych produktów i sieci oraz ich kontroli
- Należy uwzględnić ryzyko wynikające z korzystania z chmury! Podczas korzystania z usługi chmury wrażliwe dane powierza się operatorowi chmury na własną odpowiedzialność. W efekcie dostępu z zewnątrz dane mogą być poddane manipulacji, a niezamierzone polecenia mogą mieć niepożądany wpływ na funkcjonalność układu sterowania. W celu ochrony danych należy stosować metody ich szyfrowania oraz przestrzegać zaleceń Federalnego Urzędu ds. Bezpieczeństwa w zakresie techniki informatycznej, zawartych w publikacji „Cloud: Risks and Security Tips“. Na terenie kraju użytkownika należy uwzględnić zalecenia odpowiednich organów, zawarte w porównywalnych publikacjach.

3 Przegląd

Sterownik „PFC200 G2 2ETH M12 CAN XTR“ (750-8213/040-010) jest urządzeniem do automatyzacji, realizującym zadania sterowania typowe dla PLC. Przeznaczony jest on do montażu na szynie i wykorzystuje różne interfejsy.

Sterownik ten jest przeznaczony przede wszystkim do zastosowań w transporcie szynowym i morskim.

Do sterownika można podłączyć wszystkie dostępne moduły I/O wchodzące w skład WAGO I/O Systems 750 XTR. Dzięki temu może on przetwarzać wewnętrznie sygnały analogowe i dwustanowe przychodzące z systemu sterowania lub udostępniać je innym urządzeniom za pośrednictwem zastosowanych interfejsów.

Zadania automatyki można realizować we wszystkich językach zgodnych z IEC 61131-3, zależnie od zastosowanego runtime (CODESYS V2 lub *e!RUNTIME*), za pomocą środowiska programistycznego WAGO-I/O-PRO lub *e!COCKPIT*. W celu zapewnienia maksymalnej wydajności zadań automatyzacji, implementację wykonywania zadań w runtime zoptymalizowano dla Linux® z rozszerzeniami dla czasu rzeczywistego. Oprócz środowiska programistycznego dostępna jest również wizualizacja webowa.

Do programowania zgodnie z IEC 61131-3 w aplikacjach CODESYS sterownik udostępnia w oprogramowaniu CODESYS V2 16 MB pamięci programu (flash) i 64 MB pamięci danych (RAM) oraz 128 kB pamięci nieulotnej (zmienne retain i znaczników w zintegrowanej pamięci NVRAM).

Do programowania zgodnie z IEC 61131-3 w aplikacjach CODESYS sterownik udostępnia w oprogramowaniu *e!RUNTIME* 32 MB pamięci programu (flash) i 128 MB pamięci danych (RAM) oraz 128 kB pamięci nieulotnej (zmienne retain i znaczników w zintegrowanej pamięci NVRAM).

Dwa porty do sieci ETHERNET w formie złącz M12 oraz zintegrowany switch umożliwiają tworzenie połączeń sieciowych:

- w sieci o topologii liniowej ze wspólnym adresem MAC i IP dla obu portów lub
- w dwóch osobnych sieciach ze wspólnym adresem MAC i własnymi adresami IP dla każdego portu.

Oba interfejsy obsługują:

- 10BASE-T / 100BASE-TX
- full duplex / half duplex
- autonegocjację

- Auto-MDI(X) (automatyczne przełączanie między uplink i crossover)

Na potrzeby wymiany danych procesowych zaimplementowane są następujące interfejsy magistrali obiektowej:

- Modbus TCP Master/Slave
- Modbus UDP Master/Slave
- CANopen Master/Slave

W sterowniku zestawiane są wszystkie sygnały wejściowe z czujników. Po podłączeniu sterownika sieciowego rozpoznaje on wszystkie dołączone do węzła moduły I/O i tworzy lokalny obraz procesu. W każdym węźle można w dowolny sposób uszeregować moduły I/O zarówno dla sygnałów analogowych (wymiana danych w postaci słowa), jak i dwustanowych (bitowa wymiana danych).

Wskazówka



Brak bezpośredniego dostępu z sieci obiektowej do obrazu procesu modułów I/O!

Potrzebne dane z obrazu procesu magistrali systemowej muszą być wyraźnie zmapowane w programie sterującym na dane w obrazie procesu sieci obiektowej i na odwrót! Bezpośredni dostęp nie jest możliwy!

Konfiguracja sieci obiektowej możliwa jest, w zależności od zastosowanego systemu runtime (CODESYS V2 lub **e!RUNTIME**), za pomocą oprogramowania do konfiguracji sterowników WAGO-I/O-PRO lub **e!COCKPIT**.

Do konfiguracji służy także system zarządzania przez WWW (WBM). Obejmuje on różne dynamiczne strony HTMP, na których można wyświetlić m.in. informacje o konfiguracji i statusie sterownika. System WBM jest zapisany w urządzeniu i można go otworzyć oraz obsługiwać w przeglądarce internetowej. Możliwe jest również przechowywanie własnych stron HTML w zaimplementowanym systemie plików lub bezpośrednio uruchamianie programów.

Zainstalowana fabrycznie wersja firmware bazuje na systemie Linux ze specjalnymi rozszerzeniami czasu rzeczywistego z RT-Preempt patch. Oprócz różnych programów pomocniczych w sterowniku zainstalowane są następujące programy użytkowe:

- SNMP Server/Client
- Telnet Server
- serwer FTP, FTPS (tylko połączenia jednoznaczne)
- SSH Server/Client
- Web Server

- NTP Client
- BootP i DHCP Client
- DHCP Server
- DNS Server
- środowisko systemowe (CODESYS V2 lub *e!RUNTIME*, z możliwością przełączania)

Dane procesowe są przetwarzane w sterowniku zgodnie z IEC 61131-3. Efektem działania sterownika jest wysterowanie wyjść (elementów wykonawczych) i/lub udostępnienie obrazu procesu poprzez sieć do systemu nadrzędnego.

Wskazówka**Karta pamięci nie wchodzi w zakres dostawy!**

Należy pamiętać, że sterownik jest dostarczany bez karty pamięci. Aby korzystać z karty pamięci, należy ją zamówić osobno.

Ze sterownika można korzystać również bez rozszerzenia o kartę pamięci (stosowanie karty pamięci jest opcjonalne).

Wskazówka**Stosować tylko zalecane karty pamięci!**

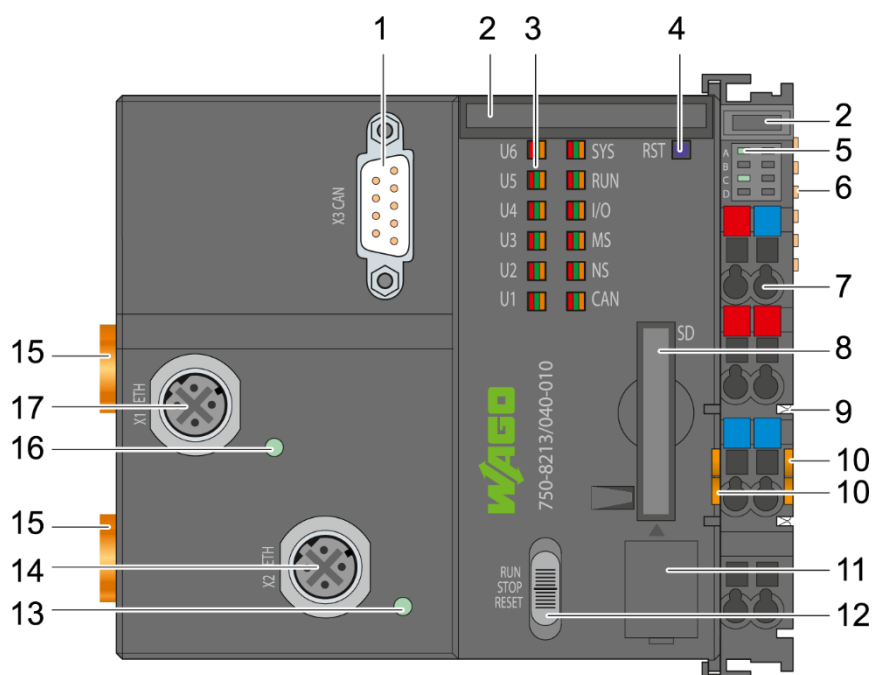
Należy stosować wyłącznie karty pamięci SD z oferty WAGO (nr kat. 758-879/000-001 i 758-879/000-2108), ponieważ są one przeznaczone do zastosowań przemysłowych w trudnych warunkach środowiskowych i do użytku w tym urządzeniu.

Nie ma gwarancji kompatybilności z innymi dostępnymi w sprzedaży nośnikami pamięci.

4 Dane

4.1 Budowa sprzętu

4.1.1 Widok



Ilustracja 1: Widok

Tabela 3: Opis ilustracji „Widok“

Poz.	Opis	Patrz rozdział
1	Złącze sieci obiektowej – CANopen	„Złącza“ > „Złącza sieci CANopen – X3“
2	Możliwość opisu (Mini-WSB)	---
3	Sygnalizacja LED – system	„Elementy sygnalizacyjne“ > „Elementy sygnalizacyjne sieć obiektowa/system“
4	Przycisk RESET (w zagłębieniu)	„Elementy obsługi“ > „Przycisk resetu“
5	Sygnalizacja LED – zasilanie	„Elementy sygnalizacyjne“ > „Elementy sygnalizacyjne dla zasilania“
6	Styki magistrali systemowej	„Złącza“ > „Styki magistrali systemowej/magistrala systemowa“
7	Zaciski CAGE CLAMP® do zasilania	„Złącza“ > „Zaciski CAGE CLAMP®“
8	Gniazdo na kartę pamięci	„Gniazdo karty pamięci“
9	Styki magistrali obiektowej do zasilania podłączonych modułów I/O	„Złącza“ > „Styki magistrali obiektowej/zasilanie magistrali obiektowej“
10	Uchwyt zwalniający blokadę	„Montaż“ > „Dodawanie urządzeń“ „Demontaż“ > „Usuwanie urządzeń“
11	Złącze serwisowe (pod klapką)	„Złącza“ > „Złącze serwisowe“
12	Przełącznik trybu pracy	„Elementy obsługi“ > „Przełącznik trybu pracy“
13	Wskaźnik LED – złącze ETHERNET X2	„Elementy sygnalizacyjne“ > „Elementy sygnalizacyjne dla sieci“
14	Złącze ETHERNET X2	„Złącza“ > „Złącza sieciowe“
15	Blokady ryglujące	„Montaż“ > „Dodawanie urządzeń“ „Demontaż“ > „Usuwanie urządzeń“
16	Wskaźnik LED – złącze ETHERNET X1	„Elementy sygnalizacyjne“ > „Elementy sygnalizacyjne dla sieci“
17	Złącze ETHERNET X1	„Złącza“ > „Złącza sieciowe“

4.1.2 Nadruk

Na nadruku z przodu urządzenia można znaleźć:

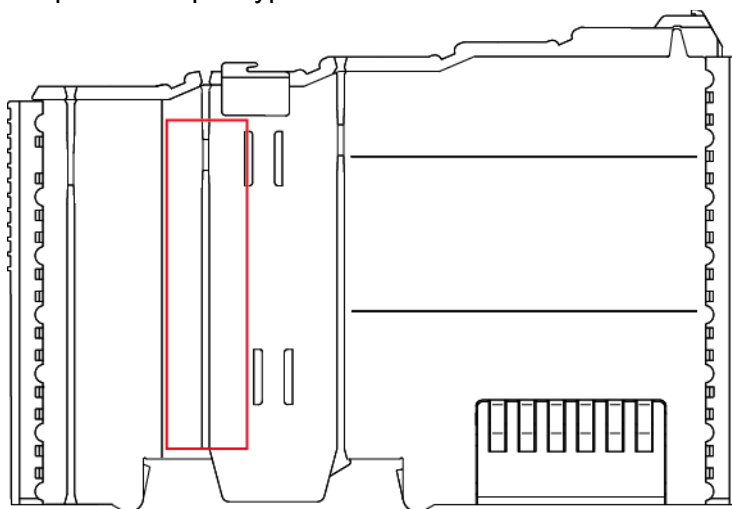
- nazwę urządzenia,
- listę elementów sygnalizacyjnych, złącz i elementów obsługi,
- numer produkcyjny wraz z danymi dotyczącymi wersji sprzętu i firmware

Na nadruku z boku widnieją:

- dane producenta,
- obłożenie zacisków,
- numer produkcyjny,
- informacje o aprobatkach.

4.1.2.1 Numer produkcyjny

Numer produkcyjny informuje o ustawieniach fabrycznych urządzenia, bezpośrednio po wyprodukowaniu.



Ilustracja 2: Miejsce na numer produkcyjny

Numer produkcyjny na nadruku z boku składa się z dwóch wierszy. Umieszczony jest po lewej stronie uchwytu zwalniającego blokadę. Pierwsze 10 znaków dłuższego wiersza numeru produkcyjnego zawiera ciąg liczb składający się z numeru wersji oraz daty.

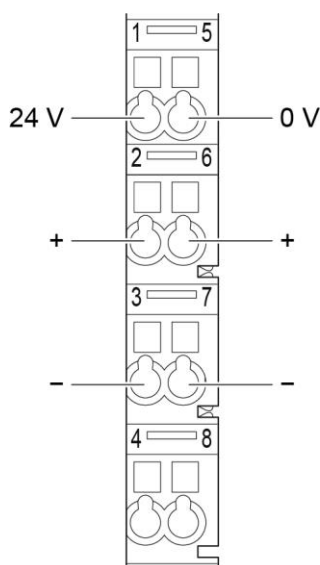
Przykład elementów składowych tego wiersza: 0114010101...

01	14	01	01	01	(dalsze miejsca)
TT	RR	FW	HW	FL	-
tydzień kalenda- rzowy	rok	wersja firmware	wersja sprzętu	wersja firmware loader	informacje wewnętrzne

Kolejność wierszy może być różna w zależności od roku produkcji, istotna jest jednak zawsze ich długość. Druga część tego wiersza oraz wiersz krótszy zawierają wewnętrzne informacje producenta.

4.1.3 Złącza

4.1.3.1 Oprzewodowanie



Ilustracja 3: Zaciski CAGE CLAMP®

Tabela 4: Opis ilustracji „Zaciski CAGE CLAMP®“

Złącze	Nazwa	Opis
1	24 V	Napięcie zasilania systemowego +24 V
2	+	Napięcie magistrali obiektowej U_V
3	-	Napięcie magistrali obiektowej 0 V
5	0 V	Napięcie zasilania systemowego 0 V
6	+	Napięcie magistrali obiektowej U_V
7	-	Napięcie magistrali obiektowej 0 V

Wskazówka



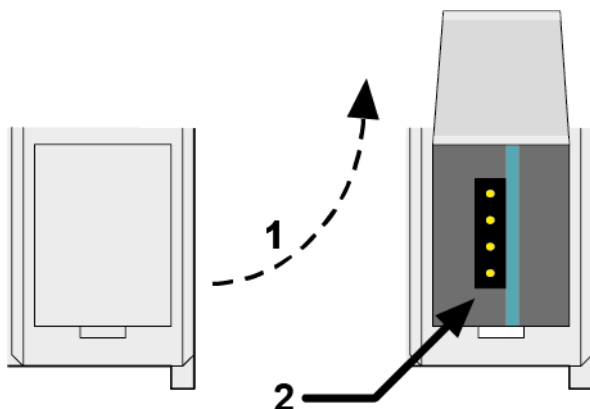
W celu użytkowania zgodnego z normami przestrzegać dodatkowych przepisów dotyczących zasilania!

W celu użytkowania zgodnego z normami w sterowaniu stacjami, w zastosowaniach telecontrol lub przy eksploatacji wymagającej certyfikatów morskich należy pamiętać o dodatkowych przepisach dotyczących zasilania, zawartych w rozdziale „Podłączanie urządzeń” > ... > „Dodatkowe przepisy dotyczące zasilania“!

4.1.3.2 Złącze serwisowe

Złącze serwisowe umieszczone jest pod klapką.

Jest ono wykorzystywane do komunikacji z WAGO-I/O-CHECK i „WAGO Ethernet Settings“



Ilustracja 4: Złącze serwisowe (klapka złącza serwisowego opuszczona i uniesiona)

Tabela 5: Złącze serwisowe

Numer	Opis
1	Otwieranie pokrywy
2	Złącze serwisowe

UWAGA

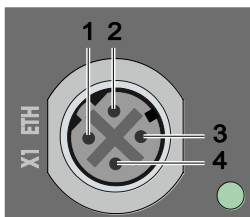


Urządzenie musi być odłączone od napięcia!

W celu uniknięcia uszkodzenia urządzenia przewód komunikacyjny należy podłączać i odłączać tylko wówczas, gdy urządzenie jest odłączone od napięcia!

Do 4-biegunowego wtyku, znajdującego się pod klapką, należy podłączyć przewód konfiguracyjny o numerze katalogowym 750-920, 750-923 lub adapter funkcyjny WAGO o numerze katalogowym 750-921.

4.1.3.3 Złącza sieciowe

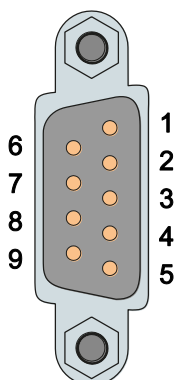


Ilustracja 5: Złącza sieciowe – X1, X2

Tabela 6: Opis ilustracji „Złącza sieciowe – X1, X2“

Nr	PIN	Sygnal	Opis
1	1	TX_P	Transmit Data +
2	2	RX_P	Receive Data +
3	3	TX_N	Transmit Data –
4	4	RX_N	Receive Data –

4.1.3.4 CANopen



Ilustracja 6: Złącze sieci obiektowej CANopen – X3

Tabela 7: Opis ilustracji „Złącze sieci obiektowej CANopen – X3“

Styk	Sygnal	Opis
1	-	niewykorzystane
2	CAN_L	CAN Signal Low
3	GND	uziemiaenie
4	-	niewykorzystane
5	Drain Shield	podłączanie ekranu
6	-	niewykorzystane
7	CAN_H	CAN Signal High
8	-	niewykorzystane
9	CAN_V+	niewykorzystane

Separacja galwaniczna między siecią CANopen i elektroniką realizowana jest przez przetworniki DC/DC i optoseparatory w złączu sieci obiektowej.

Ekran przewodu musi być podłączony do styku CAN Shield. W urządzeniu zacisk ten odseparowany od ziemi (styk z szyną montażową) rezystancją o wartości 1 MΩ). Niskoomowe połączenie ekranu z ziemią może być realizowane tylko zewnętrznie (np. poprzez moduł zasilający). Należy dążyć do centralnego uziemienia całego ekranowania przewodu magistralowego sieci CANopen.

Aby ograniczyć zjawisko odbicia sygnałów, na obu końcach przewodu CANopen musi znajdować się terminacja.

Wskazówka



Pamiętać o terminacji sieci!

Segment sieci CANopen musi mieć terminację po obu stronach!

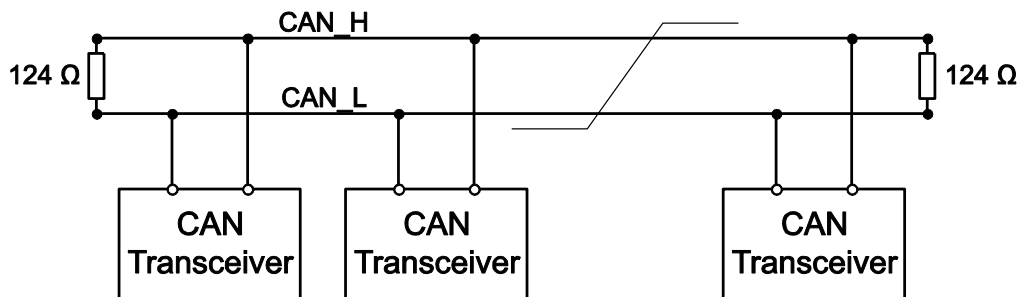
Nie należy stosować więcej niż 2 terminacji na sieć!

Na odcinkach będących odejściami lub odgałęzieniami nie należy używać terminacji!

Praca bez właściwej terminacji sieci CANopen może prowadzić do błędów w transmisji.

Wskazówka**Pamiętać o dopuszczalnej mocy strat rezystorów!**

W normalnym trybie pracy wystarczą rezystory 1/4 W. Przy zwarcu (zasilanie 24 V względem przewodu sieciowego) rezystor zostaje obciążony mocą strat (prąd wyjściowy zwarcia transceivera* napięcie zasilania). Rezystor musi być przystosowany do takich strat mocy.

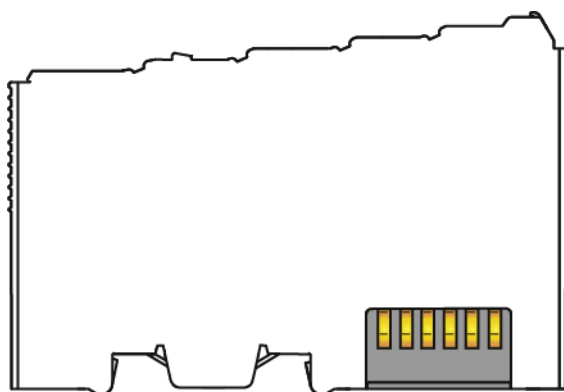


Ilustracja 7: Standardowe złącze sieci CANopen

4.1.4 Połączenia systemowe

4.1.4.1 Styki magistrali systemowej

Komunikacja pomiędzy sterownikiem sieciowym a modułami I/O oraz zasilanie elektroniki modułów I/O odbywa się przez magistralę systemową. Połączenie z magistralą systemową tworzy 6 połączonych, samoczyszczących styków sprężynowych.



Ilustracja 8: Styki magistrali systemowej

UWAGA



Nie kłaść modułów I/O stykami do podłoża!

W celu uniknięcia zanieczyszczeń i zadrapań nie wolno kłaść modułów I/O połączanymi stykami do podłoża.

ESD



Pamiętać o wyrównaniu potencjałów w otoczeniu!

Urządzenia są wyposażone w elementy elektroniczne, które przy wyładowaniach elektrostatycznych mogą zostać zniszczone. Podczas użytkowania urządzenia należy zwrócić uwagę na wyrównanie potencjałów w otoczeniu (ludzie, stanowisko robocze i opakowanie). Nie wolno dotykać części przewodzących prąd, np. styków magistrali systemowej.

UWAGA



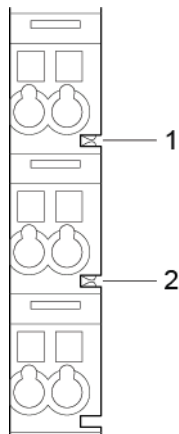
Nie przekraczać maksymalnego prądu sumarycznego dla modułów I/O (5 V) przez styki magistrali systemowej!

Nie należy przekraczać maksymalnej dopuszczalnej wartości prądu sumarycznego, potrzebnego do zasilania modułów I/O przez wewnętrzną magistralę systemową. Dopuszczalny prąd sumaryczny podany jest w danych technicznych jednostki głównej i komponentów sieciowych. Większe wartości mogą uszkodzić styki zasilające wewnętrzną magistralę systemową i spowodować przekroczenie górnej granicy dopuszczalnej temperatury.

Przy konfiguracji systemu należy zwrócić uwagę, aby maksymalny dopuszczalny prąd sumaryczny nie został przekroczony. Przy większym zapotrzebowaniu na prąd należy zastosować dodatkowy zasilacz magistrali, ponownie podający napięcie dla zasilania systemowego (5 V)!

4.1.4.2 Styki magistrali obiektowej

Sterownik 750-8213/040-010 jest wyposażony w 2 samoczynzące styki magistrali obiektowej, służące do przekazywania napięcia magistrali obiektowej do podłączonych modułów I/O. Są to styki sprężynowe.



Ilustracja 9: Styki magistrali obiektowej

Tabela 8: Opis ilustracji „Styki magistrali obiektowej“

Styk	Typ	Funkcja
1	Styk sprężynowy	Przekazywanie potencjału (UV) dla magistrali obiektowej
2	Styk sprężynowy	Przekazywanie potencjału (0 V) dla magistrali obiektowej

OSTRZEŻENIE Ryzyko zranienia stykami nożowymi z ostrymi krawędziami!



Ponieważ styki nożowe mają bardzo ostre krawędzie, istnieje ryzyko zranienia w przypadku nieostrożnej obsługi modułów I/O. Nie należy dotykać styków nożowych.

UWAGA



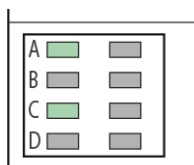
Nie przekraczać maksymalnych wartości zasilania obiektowego!

Maksymalny prąd, mogący płynąć przez magistralę obiektową, wynosi 10 A. Większe prądy mogą uszkodzić styki magistrali obiektowej i spowodować przekroczenie górnej granicy dopuszczalnej temperatury.

Przy konfiguracji systemu należy zwrócić uwagę, aby maksymalny dopuszczalny prąd nie został przekroczony. Przy większym zapotrzebowaniu na prąd należy zastosować dodatkowy moduł zasilający, ponownie podający napięcie dla zasilania obiektowego.

4.1.5 Elementy sygnalizacyjne

4.1.6 Elementy sygnalizacyjne dla zasilania



Ilustracja 10: LED dla zasilania

Tabela 9: Opis ilustracji „LED dla zasilania“

Nazwa	Kolor	Opis
A	zielony/wył.	status napięcia zasilania systemowego
C	zielony/wył.	status napięcia sieci obiektowej

4.1.7 Elementy sygnalizacyjne dla sieci/systemu

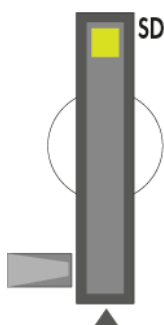
U6   SYS
 U5   RUN
 U4   I/O
 U3   MS
 U2   NS
 U1   CAN

Ilustracja 11: LED dla systemu / sieci obiektowej

Tabela 10: Opis ilustracji „LED dla systemu/sieci obiektowej“

Nazwa	Kolor	Opis
SYS	czerw./ziel. pomar./wył.	status systemu
RUN	czerw./ziel. pomar./wył.	status programu PLC
I/O	czerw./ziel. pomar./wył.	status wewnętrznej magistrali systemowej
MS	czerw./ziel. pomar./wył.	status modułu
NS	czerw./ziel. pomar./wył.	brak funkcji
CAN	czerw./ziel. pomar./wył.	status CANopen
U6	czerw./ziel. pomar./wył.	LED 6 użytkownika, możliwość programowania za pomocą bloków funkcyjnych do sterowania wskaźnikami LED w ramach bibliotek WAGO
U5	czerw./ziel. pomar./wył.	LED 5 użytkownika, możliwość programowania za pomocą bloków funkcyjnych do sterowania wskaźnikami LED w ramach bibliotek WAGO
U4	czerw./ziel. pomar./wył.	LED 4 użytkownika, możliwość programowania za pomocą bloków funkcyjnych do sterowania wskaźnikami LED w ramach bibliotek WAGO
U3	czerw./ziel. pomar./wył.	LED 3 użytkownika, możliwość programowania za pomocą bloków funkcyjnych do sterowania wskaźnikami LED w ramach bibliotek WAGO
U2	czerw./ziel. pomar./wył.	LED 2 użytkownika, możliwość programowania za pomocą bloków funkcyjnych do sterowania wskaźnikami LED w ramach bibliotek WAGO
U1	czerw./ziel. pomar./wył.	LED 1 użytkownika, możliwość programowania za pomocą bloków funkcyjnych do sterowania wskaźnikami LED w ramach bibliotek WAGO

4.1.8 Elementy sygnalizacyjne dla gniazda na kartę pamięci

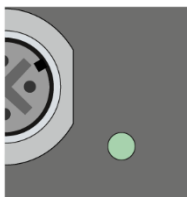


Ilustracja 12: LED gniazda karty pamięci

Tabela 11: Opis ilustracji „LED gniazda karty pamięci“

Nazwa	Kolor	Opis
SD	żółty/wył.	status karty pamięci

4.1.9 Elementy sygnalizacyjne dla sieci



Ilustracja 13: LED LNK (obok gniazd M12)

Tabela 12: Opis ilustracji „LED LNK (obok gniazd M12)“

Nazwa	Kolor	Opis
LNK	zielony	nawiązano połączenie
	wył.	brak połączenia

4.1.10 Elementy obsługi

4.1.10.1 Przełącznik trybu pracy



Ilustracja 14: Przełącznik trybu pracy

Funkcja przełącznika trybu pracy jest zależna od aktywowanego systemu runtime (CODESYS V2 lub **e!RUNTIME**).

Dla systemu runtime CODESYS V2 przełącznik trybu pracy ma następujące funkcje:

Tabela 13: Przełącznik trybu pracy

Pozycja	Uruchamianie	Funkcja
RUN	pozostający na danej pozycji	Praca normalna Aplikacja CODESYS V2 działa.
STOP	pozostający na danej pozycji	Stop Aplikacja CODESYS V2 zatrzymana.
RESET	powracający do pozycji wyjściowej	Gorący reset lub zimny reset (zależnie od długości przytrzymania przycisku, patrz rozdział „Uruchamianie” > „Wyzwalanie funkcji RESET”)

Za pomocą przycisku RESET można uruchamiać też inne funkcje.

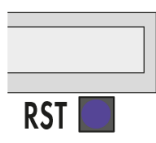
Dla systemu runtime **e!RUNTIME** przełącznik trybu pracy ma następujące funkcje:

Tabela 14: Przełącznik trybu pracy

Pozycja	Uruchamianie	Funkcja
RUN	pozostający na danej pozycji	Praca normalna Aplikacje e!RUNTIME działają.
STOP	pozostający na danej pozycji	Stop Wszystkie aplikacje e!RUNTIME zatrzymane.
RESET	powracający do pozycji wyjściowej	Gorący reset lub zimny reset (zależnie od długości przytrzymania przycisku, patrz rozdział „Uruchamianie” > „Wyzwalanie funkcji RESET”)

Za pomocą przycisku RESET można uruchamiać też inne funkcje.

4.1.10.2 Przycisk RESET



Ilustracja 15: Przycisk resetu

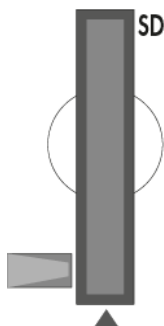
Przycisk RESET znajduje się w zagłębieniu, które uniemożliwia jego niezamierzone użycie. Jest to przycisk o krótkim skoku i niewielkiej sile docisku, wynoszącej od 1,1 N do 2,1 N (110 gf ... 210 gf).

Można go uruchomić dowolnym, nadającym się do tego celu przedmiotem (np. długopisem).

W zależności od pozycji przełącznika trybu pracy przycisk RESET może realizować różne funkcje:

- czasowe ustawianie stałych adresów IP (tryb „Fixed IP Address“, patrz rozdział „Uruchamianie“ > „Ustawianie adresu IP“ > „Czasowe ustawienie stałego adresu IP“)
- reset programowy (restart) (patrz rozdział „Uruchamianie“ > „Wyzwalanie funkcji RESET“ > „Reset programowy (restart)“)
- przywracanie ustawień fabrycznych (Factory-Reset, patrz rozdział „Serwis“ > „Zmiany firmware“ > „Factory Reset“)

4.1.11 Gniazdo karty pamięci



Ilustracja 16: Gniazdo karty pamięci SC

Gniazdo karty pamięci SD znajduje się na frontowej ścianie urządzenia. Karta pamięci jest blokowana w obudowie za pomocą mechanizmu push/push. Wkładanie i wyciąganie karty zostało opisane w rozdziale „Serwis” > „Wkładanie i wyjmowanie karty pamięci”!

Karta pamięci chroniona jest pokrywą. Pokrywa jest plombowana.

Wskazówka



Karta pamięci nie wchodzi w zakres dostawy!

Należy pamiętać, że sterownik jest dostarczany bez karty pamięci. Aby korzystać z karty pamięci, należy ją zamówić osobno. Ze sterownika można korzystać również bez rozszerzenia o kartę pamięci (stosowanie karty pamięci jest opcjonalne).

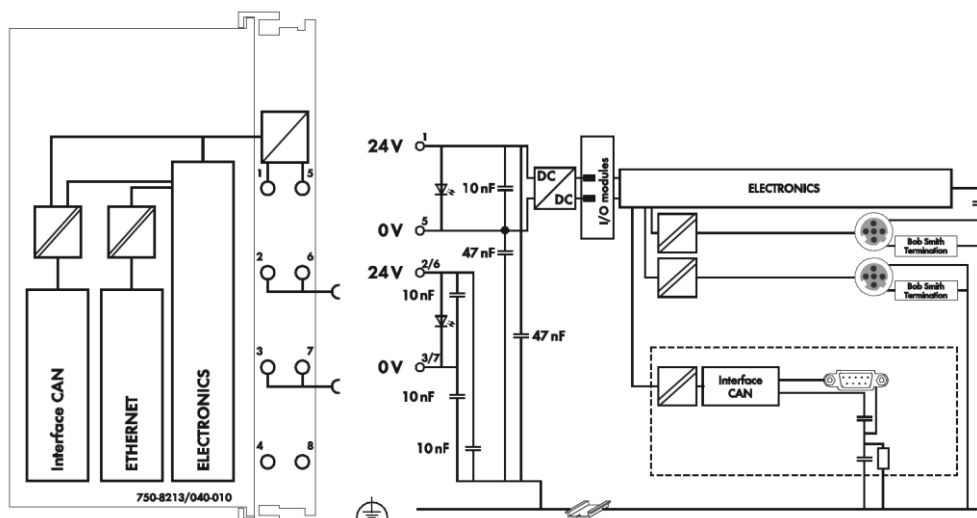
Wskazówka



Stosować tylko zalecane karty pamięci!

Należy stosować wyłącznie karty pamięci SD z oferty WAGO (nr kat. 758-879/000-001 i 758-879/000-2108), ponieważ są one przeznaczone do zastosowań przemysłowych w trudnych warunkach środowiskowych i do użytku w tym urządzeniu. Nie ma gwarancji kompatybilności z innymi dostępnymi w sprzedaży nośnikami pamięci.

4.2 Schemat połączeń wewnętrznych



Ilustracja 17: Schemat połączeń wewnętrznych

4.3 Dane techniczne

4.3.1 Dane urządzenia

Tabela 15: Dane techniczne – urządzenie

Szerokość	112 mm
Głębokość (od górnej krawędzi szyny)	71,9 mm
Wysokość	100 mm
Masa	214 g
Stopień ochrony	IP20

4.3.2 Dane systemowe

Tabela 16: Dane techniczne – dane systemowe

CPU	Cortex A8, 1 GHz
System operacyjny	Linux® czasu rzeczywistego z RT-Preemption-patch
Gniazdo karty pamięci	Mechanizm typu push-push, pokrywa plombowana
Typ karty pamięci	SD i SDHC maks. 32 GB (Niezawodne działanie gwarantowane jest tylko przy użyciu kart pamięci WAGO 758-879/000-001 i 758-879/000-2108.)

4.3.3 Zasilanie

Tabela 17: Dane techniczne – zasilanie

Pobór prądu z magistrali systemowej (5 V DC)	510 mA DC
Prąd sumaryczny dla modułów I/O (5 V DC)	1700 mA DC
Prąd sumaryczny dla zasilania systemowego	1700 mA DC
Prąd wyjściowy typ. przy obciążeniu nominalnym (24 V DC)	550 mA DC
Czas awarii zasilania zgodnie z IEC 61131-2	zależny od zewnętrznego buforowania
Napięcie zasilania	
System	24 V DC poprzez dołączane przewody (zacisk CAGE CLAMP®)
Obiekt	24 V DC • zasilanie poprzez dołączane przewody (zacisk CAGE CLAMP®) • doprowadzanie przez styki magistrali obiektowej
Ograniczenie obciążenia w warunkach laboratoryjnych	18 V ... 31,2 V (17,4 V ... 31,2 V) ¹⁾
przy temperaturze otoczenia -40°C ... +55°C	18 V ... 28,8 V (17,4 V ... 28,8 V) ¹⁾
przy temperaturze otoczenia +55°C ... +70°C	18 V ... 26,4 V (17,4 V ... 26,4 V) ¹⁾
dolna wartość graniczna dla wszystkich zakresów temperatur	-27,5% ¹⁾
Sprawność zasilacza typ. przy obciążeniu nominalnym	90%
Znamionowe napięcie udarowe	1 kV

¹⁾ w tym tętnienia resztkowe 15%

Wskazówka



Dla zasilania systemowego zastosować zewnętrzne buforowanie!

W celu zabezpieczenia na wypadek awarii zasilania, zasilanie magistrali systemowej, a w razie potrzeby także zasilanie obiektowe, powinny być buforowane.

Ponieważ zapotrzebowanie na prąd zależy od węzła sieciowego, buforowanie nie zostało zaimplementowane w urządzeniu.

Aby uzyskać czas awarii zasilania zgodny z IEC 61131-2 (1 ms lub 10 ms), należy obliczyć buforowanie odpowiednie dla danego węzła sieciowego, a następnie dołożyć zewnętrznie urządzenie zasilające.

4.3.4 Zegar

Tabela 18: Dane techniczne – zegar

Dryft – zegar systemowy (25°C)	20 ppm
Dryft – RTC (25°C)	3 ppm
Czas buforowania RTC (25°C)	30 dni

4.3.5 Programowanie

Tabela 19: Dane techniczne – programowanie

Tabela 15. Dane techniczne programowania		
Programowanie	CODESYS V2	WAGO-I/O-PRO V2.3
	e!RUNTIME	e!COCKPIT
IEC 61131-3		KOP, FUP (CFC), ST, AS
Konfiguracja pamięci CODESYS 2		
pamięć programu (flash)		16 MB
pamięć danych (RAM)		64 MB
pamięć nieulotna (NVRAM, retain + znaczniki)		128 kB
Konfiguracja pamięci e!RUNTIME		
pamięć programu i danych		60 Mb (przydzielana dynamicznie)
pamięć nieulotna (NVRAM, retain + znaczniki)		128 kB
nieulotne zmienne maks.	CODESYS V2	10 000
	e!RUNTIME	brak danych

Wskazówka Zastosowanie pamięci wewnętrznej



Pamięć wewnętrzna (flash) jest przeznaczona do przechowywania programu aplikacji. Usługi o wysokiej aktywności zapisu, takie jak np. rejestracja danych, nie są dozwolone!

4.3.6 Magistrala systemowa

Tabela 20: Dane techniczne – magistrala systemowa

Tabela 26. Dane techniczne – magistrala systemowa		
Liczba modułów I/O (w węźle)		64
z przedłużaczem magistrali		250
Maks. obraz procesu wejść i wyjść	CODESYS V2	1 000 słów
	e!RUNTIME	brak danych

4.3.7 ETHERNET

Tabela 21: Dane techniczne – ETHERNET

ETHERNET		2 × M12 D-kodowane (tryb przełączany lub oddzielny)
Medium transmisji		skrętka S-UTP, 100 Ω, Cat 5, maks. długość przewodu 100 m
Prędkość transmisji		10/100 Mb/s; 10Base-T/100Base-TX
Protokoły		DHCP, DNS, SNTP, FTP, FTPS (tylko połączenia jednoznaczne), SNMP, HTTP, HTTPS, SSH, MODBUS (TCP, UDP)
MODBUS – obraz procesu wejść i wyjść maks.	CODESYS V2	1000 słów, dodatkowo dostęp przez sieć MODBUS do pamięci znaczników (patrz rozdział „MODBUS“ > ... > „Pamięć znaczników“)
	e!RUNTIME	32 000 słów

Wskazówka



Brak bezpośredniego dostępu z sieci obiektowej do obrazu procesu modułów I/O!

Potrzebne dane z obrazu procesu magistrali systemowej muszą być wyraźnie zmapowane w programie sterującym na dane w obrazie procesu sieci obiektowej i na odwrót! Bezpośredni dostęp nie jest możliwy!

4.3.8 CANopen

Tabela 22: Dane techniczne – CANopen

CANopen – obraz procesu wejść i wyjść maks.	2000 słów

Wskazówka



Brak bezpośredniego dostępu z sieci obiektowej do obrazu procesu modułów I/O!

Potrzebne dane z obrazu procesu magistrali systemowej muszą być wyraźnie zmapowane w programie sterującym na dane w obrazie procesu sieci obiektowej i na odwrót! Bezpośredni dostęp nie jest możliwy!

4.3.9 Technika podłączania przewodu

Tabela 23: Dane techniczne – oprzewodowanie

Technika podłączania przewodu	CAGE CLAMP®
Przekrój przewodu	0,25 mm ² ... 2,5 mm ² / AWG 24 ... 14
Długość odizolowania przewodu	8 mm ... 9 mm / 0,33 in

Tabela 24: Dane techniczne – styki magistrali obiektowej

Styki magistrali obiektowej	Styk sprężynowy, samoczyszczący, połączany

Tabela 25: Dane techniczne – styki magistrali systemowej

Styki magistrali systemowej	Styki ślizgowe, samoczyszczące, połączane

4.3.10 Warunki mechaniczne

Tabela 26: Dane techniczne – warunki mechaniczne

Odporność na wibracje	maks. 5g *)

*) Przestrzegać warunków dotyczących montażu.

4.3.11 Warunki klimatyczne

Tabela 27: Dane techniczne – warunki klimatyczne

Temperatura otoczenia, praca	-40°C ... +70°C
Temperatura otoczenia, przechowywanie	-40°C ... +85°C
wilgotność względna *)	95%
Praca w zależności od wysokości n.p.m. bez zmiany parametrów temp. ze zmianą parametrów temp. maks.	0 m ... 2000 m 2000 m ... 5000 m: 0,5 K na 100 m 5000 m
Narażenie na wpływ substancji szkodliwych	zgodnie z IEC 60068-2-42 i IEC 60068-2-43
maks. koncentracja substancji szkodliwych przy wilgotności względnej < 75%	SO ₂ ≤ 25 ppm H ₂ S ≤ 10 ppm
Warunki specjalne	Przy określaniu dopuszczalnego zakresu temperatury dla przewodu przyłączeniowego należy uwzględnić pozycję montażu i natężenie prądu, ponieważ temperatura zacisków może wynosić maksymalnie 25 K (przy 10 A) więcej od oczekiwanej temperatury otoczenia.

*) dopuszczalna krótkotrwała kondensacja zgodnie z klasą 3K7 / IEC EN 60721-3-3 przy zastosowaniu E-DIN 40046-721-3 (oprócz opadów nanoszonych wiatrem, wody i oblodzenia)

UWAGA**Ograniczony zakres temperatur przy montażu w pozycji pionowej!**

Przy montażu w pozycji pionowej nie wolno przekraczać temperatury otoczenia wynoszącej maksymalnie 65°C! Nieprzestrzeganie tego zalecenia nie zapewnia prawidłowej pracy urządzenia lub może spowodować jego uszkodzenie.

4.4 Aprobaty

Informacja



Dodatkowe informacje na temat aprobat

Szczegółowe informacje na temat aprobat znajdują się w dokumencie „Przegląd aprobat WAGO I/O System 750”. Można go znaleźć na stronie internetowej: www.wago.com → POBIERZ → Dokumentacja → Opis systemu.

Sterownikowi „PFC200 G2 2ETH M12 CAN XTR” (750-8213/040-010) przyznano następujące aprobaty:



Znak zgodności



UL E175199 for
use in Ordinary
Location

Sterownikowi „PFC200 G2 2ETH M12 CAN XTR” (750-8213/040-010) przyznano następujące aprobaty Ex:



UL E198726 for Use in Hazardous Locations
Cl I, Div 2, Group A, B, C, D, T4



TÜV 17 ATEX 193969 X
II 3 G Ex ec IIC T4 Gc
IECEX TUN 16.0046X
Ex ec IIC T4 Gc

Sterownikowi „PFC200 G2 2ETH M12 CAN XTR” (750-8213/040-010) przyznano następujące aprobaty morskie:



Temperature:	D (cold test with -40°C/16 h)
Humidity:	B
Vibration:	B (vibration test with acceleration amplitude 5.0g)
EMC:	B
Enclosure:	A

Dla sterownika „PFC200 G2 2ETH M12 CAN XTR“ (750-8213/040-010)
w przygotowaniu są następujące aprobaty morskie:



ABS (American Bureau of Shipping)



LR (Lloyd's Register)

Env. 1, 2, 3, 4

Informacja



Dodatkowe informacje na temat aprobat morskich

Dodatkowe informacje znajdują się w rozdziale „Dodatkowe przepisy dotyczące zasilania“.

4.5 Normy i dyrektywy

Sterownik „PFC200 G2 2ETH M12 CAN XTR“ (750-8213/040-010) spełnia wymagania następujących norm i dyrektyw:

Tabela 28: Normy i warunki użytkowania dla zastosowań w ochronie przeciwwybuchowej

ATEX zgodnie z dyrektywą 2014/34/UE	
Wymagania ogólne	
EN 60079-0	Urządzenia elektryczne z grupy II
Wymagania dotyczące urządzeń o różnych rodzajach budowy przeciwwybuchowej	
EN 60079-7	Urządzenia elektryczne o budowie przeciwwybuchowej "e" z poziomem zabezpieczenia "ec"
EN 60079-15	Urządzenia elektryczne o budowie przeciwwybuchowej "n" z poziomem zabezpieczenia "nC"
IECEx Certificates of Conformity	
Wymagania ogólne	
IEC 60079-0	Urządzenia elektryczne z grupy II
Wymagania dotyczące urządzeń o różnych rodzajach budowy przeciwwybuchowej	
EC 60079-7	Urządzenia elektryczne o budowie przeciwwybuchowej "e" z poziomem zabezpieczenia "ec"
IEC 60079-15	Urządzenia elektryczne o budowie przeciwwybuchowej "n" z poziomem zabezpieczenia "nC"

Tabela 29: Warunki klimatyczne i mechaniczne, przemysł stoczniowy

Norma	Wartość pomiarowa
Transport	
EN 60870-2-2	Ct2(2k4) (z wyjątkiem opadów/wody/wilgoci)
Mechaniczne warunki środowiskowe	
EN 61850-3	spełnia
EN 60870-2-2	Bm
EN 60721-3-1	1M3
EN 60721-3-3	3M5
EN 60068-2-6	przyspieszenie 5g
IEC 60068-2-27, udary mechaniczne	15g, 11 ms, 1000 uderów w każdej osi i kierunku, półsinusoidalnie
	25g, 6 ms, 1000 uderów w każdej osi i kierunku, półsinusoidalnie
EN 50155 EN 61373	wibracje: kategoria 1, klasa A i B
	udar 5g, 30 ms: kategoria 1, klasa A i B
Warunki klimatyczne	
EN 61850-3	spełnia
EN 60721-3-1	1K5 (oprócz opadów i oblodzenia)
EN 60721-3-3	3K7 (oprócz opadów nanoszonych wiatrem, wody i oblodzenia)
EN 60870-2-2	C3 (oprócz opadów nanoszonych wiatrem i oblodzenia)
EN 50155	OT4 (-40 ... +70°C)
Przemysł stoczniowy (mechaniczne/klimatyczne warunki środowiskowe i EMC)	
przemysł stoczniowy ^{*)}	temperatura: D (chłodzenie -40°C/16 h) wilgotność względna: B wibracja: B (badanie odporności na wibracje przy przyspieszeniu 5,0g) EMC: B obudowa: A

^{*)} Lista aprobat morskich znajduje się w rozdziale „Aprobaty”.

Sterownik 750-8213/040-010 spełnia następujące normy EMC, o ile normy te dotyczą sterownika:

Tabela 30: EMC – normy produktowe i techniczne

EN 61000-6-1	Kompatybilność elektromagnetyczna (EMC) – Część 6-1: Normy ogólne – Odporność w środowiskach: mieszkalnym, handlowym i lekko uprzemysłowionym
EN 61000-6-2	Kompatybilność elektromagnetyczna (EMC) – Część 6-2: Normy ogólne – Odporność w środowiskach przemysłowych
EN 61000-6-3	Kompatybilność elektromagnetyczna (EMC) – Część 6-3: Normy ogólne – Normy emisji w środowiskach: mieszkalnym, handlowym i lekko uprzemysłowionym
EN 61000-6-4	Kompatybilność elektromagnetyczna (EMC) Część 6-4: Normy ogólne – Normy emisji w środowiskach przemysłowych
EN 61000-6-5	Kompatybilność elektromagnetyczna (EMC) – Część 6-5: Normy ogólne – Odporność urządzeń i urządzeń stosowanych w elektrowniach oraz stacjach łączeniowych
EN 61850-3	Systemy i sieci komunikacyjne automatyzacji przedsiębiorstw elektroenergetycznych – Część 3: Wymagania ogólne.
EN 60870-2-1	Urządzenia i systemy zdalnego sterowania – Część 2: Warunki pracy – Sekcja 2: Warunki środowiskowe (klimatyczne, mechaniczne i inne oddziaływania nielektryczne)
EN 61131-2	Sterowniki programowalne – Część 2: Wymagania i badania dotyczące sprzętu
EN 60255-26	Przełączniki pomiarowe i urządzenia zabezpieczeniowe – Część 26: Wymagania dotyczące kompatybilności elektromagnetycznej
IEEE 1613	Environmental and testing requirements for communications networking devices installed in electric power substations
IEEE 1613.1	IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Transmission and Distribution Facilities
IEEE 1613a	Environmental and testing requirements for communications networking devices installed in electric power substations – Amendment 1: Adding of one definition, dc power supply requirements (5.1), and annex E – History

Tabela 31: EMC – odporność na zakłócenia

Norma	Wartość pomiarowa
Wyładowania elektrostatyczne	
• EN 61000-4-2	8 kV (kontakt)
• IEEE C37.90.3	8 kV (powietrze)
Pola elektromagnetyczne o wysokiej częstotliwości	
• EN 61000-4-3	20 V/m (80 MHz ... 1 GHz)
• IEEE C37.90.2	10 V/m (1 GHz ... 6 GHz)
Elektryczne szybkozmienne/impulsowe stany przejściowe/Burst	
• EN 61000-4-4	4 kV
• IEEE C37.90.1	
Napięcia udarowe/Surge	
• EN 61000-4-5	1 kV (przewód/przewód) 2 kV (przewód/ziemia)
Zakłócenia przewodzone, indukowane przez pola o częstotliwości radiowej	
• EN 61000-4-6	10 V (150 kHz ... 80 MHz)
Pola magnetyczne o częstotliwości sieci elektroenergetycznej	
• EN 61000-4-8	300 A/m długotrwale / 1000 A/m dla 1 s
Impulsowe pola magnetyczne	
• EN 61000-4-9	300 A/m
Pola magnetyczne oscylacyjne tłumione	
• EN 61000-4-10	100 A/m
Zapady napięcia, krótkie przerwy i zmiany napięcia	
• EN 61000-4-11	nie dotyczy
Tłumione przebiegi sinusoidalne	
• EN 61000-4-12	1 kV (przewód/przewód) 2 kV (przewód/ziemia)
Wyższe harmoniczne i interharmoniczne	
• EN 61000-4-13	nie dotyczy
Asymetryczne zaburzenia przewodzone	
• EN 61000-4-16	30 V długotrwale 300 V dla 1 s
Obecność składowej zmiennej w stałym napięciu zasilającym	
• EN 61000-4-17	15%
Tłumiony przebieg oscylacyjny	
• EN 61000-4-18	1,25 kV (przewód/przewód)
• IEEE C37.90.1	2,5 kV (przewód/ziemia)
Zapady napięcia, krótkie przerwy i zmiany napięcia występujące w przyłączy zasilającym prądu stałego	
• EN 61000-4-29	patrz rozdział „Zasilacze“
Wyższe harmoniczne	

Tabela 31: EMC – odporność na zakłócenia

Norma	Wartość pomiarowa
• przemysł stoczniowy ^{*)}	maks. 2 W DC: 3 V _{sk} , AC: 10% do 15. harmoniczej 10% ... 1% dla 15. do 100. harmoniczej 1% dla 100. do 200. harmoniczej

^{*)} Lista aprobat morskich znajduje się w rozdziale „Aprobaty”.

Tabela 32: EMC – emisja zakłóceń

Norma	Wartość pomiarowa *)
Obudowa emisja zakłóceń	
• EN 55032 klasa B	30 dB(μV/m), QP, 30 MHz ... 230 MHz 37 dB(μV/m), QP, 230 MHz ... 1 GHz 70 dB(μV/m), Peak, 1 GHz ... 3 GHz 50 dB(μV/m), AV, 1 GHz ... 3 GHz 74 dB(μV/m), Peak, 3 GHz ... 6 GHz 54 dB(μV/m), AV, 3 GHz ... 6 GHz
• EN 55011 klasa A • EN 55032 klasa A	40 dB(μV/m), QP, 30 MHz ... 230 MHz 47 dB(μV/m), QP, 230 MHz ... 1 GHz 76 dB(μV/m), Peak, 1 GHz ... 3 GHz 56 dB(μV/m), AV, 1 GHz ... 3 GHz 80 dB(μV/m), Peak, 3 GHz ... 6 GHz 60 dB(μV/m), AV, 3 GHz ... 6 GHz
• przemysł stoczniowy**) (klasa B)	80 dB(μV/m) ... 50 dB(μV/m), QP, 150 kHz ... 300 kHz 50 dB(μV/m) ... 34 dB(μV/m), QP, 0,3 MHz ... 30 MHz 54 dB(μV/m), QP, 30 MHz ... 2 GHz 24 dB(μV/m), QP, 156 MHz ... 165 MHz
• przemysł stoczniowy**) (klasa A)	80 dB(μV/m) ... 50 dB(μV/m), QP, 150 kHz ... 30 MHz 60 dB(μV/m) ... 54 dB(μV/m), QP, 30 MHz ... 100 MHz 54 dB(μV/m), QP, 100 MHz ... 2 GHz 24 dB(μV/m), QP, 156 MHz ... 165 MHz
Przewodzona emisja zakłóceń – przyłączenie do zasilania prądem przemiennym	
• EN 55032 klasa B	nie dotyczy
• EN 55011 klasa A	nie dotyczy
Przewodzona emisja zakłóceń – przyłączenie do zasilania	
• przemysł stoczniowy**) (klasa B)	96 dB(μV) ... 50 dB(μV), 10 kHz ... 150 kHz 60 dB(μV) ... 50 dB(μV), 150 kHz ... 350 kHz 50 dB(μV), 0,35 MHz ... 30 MHz
• przemysł stoczniowy**) (klasa A)	120 dB(μV) ... 69 dB(μV), 10 kHz ... 150 kHz 79 dB(μV), 150 kHz ... 500 kHz 73 dB(μV), 0,5 MHz ... 30 MHz
Przewodzona emisja zakłóceń – przyłączenie do zasilania prądem stałym	
• EN 55032 klasa A	79 dB(μV) QP, 0,15 MHz ... 0,5 MHz 66 dB(μV) AV, 0,15 MHz ... 0,5 MHz 73 dB(μV) QP, 0,5 MHz ... 30 MHz 60 dB(μV) AV, 0,5 MHz ... 30 MHz

*) QP = Quasi Peak Detector; AV = Average Detector

**) W przypadku ewentualnych różnic proszę uwzględnić dane z rozdziału „Aprobaty” (dotyczy aprobat dla EMC A lub EMC B).

Tabela 33: Normy i warunki użytkowania do zastosowań kolejowych (EN 50155:2017)

Wymaganie	Spełniona klasa/norma
4.3 Środowiskowe warunki pracy	
4.3.1 Wysokość n.p.m.	AX (EN 50125-1)
4.3.2 Temperatura pracy	OT4
4.3.3 Rozszerzona temperatura pracy przy włączaniu	ST1
4.3.4 Szybkie zmiany temperatury	H1
4.3.5 Udry i wibracje	1B (EN 61373)
4.3.7 Wilgotność względna	95% (EN 50125-1)
5.1 Zasilanie	
5.1.1.2 Zakres napięcia stałego	
min. napięcie długotrwałe	$0,725 \times U_n$ ($0,7 \times U_n$ zapewnić poprzez odpowiedni zasilacz zewnętrzny)
maks. napięcie długotrwałe	$1,25 \times U_n$
5.1.1.3 Tymczasowe wahania napięcia stałego	
min. napięcie	$0,725 \times U_n$ ($0,6 \times U_n$ zapewnić poprzez odpowiedni zasilacz zewnętrzny)
maks. napięcie	$1,4 \times U_n$
5.1.1.4 Przerwy w zasilaniu	S1
5.1.3 Klasy przełączania zasilacza	zapewnić poprzez odpowiedni zasilacz zewnętrzny
5.2.3 Kompatybilność elektromagnetyczna	EN 50121-3-2
5.2.6 Izolacja	EN 50124-1; Kategoria przepięć OV2
6.2 Okres użytkowania	LX
10.7 Lakierowanie ochronne do PCB z wyposażeniem	PC2
11.3 Wymagania dotyczące reakcji na ogień	EN 45545-2, Poziom zagrożenia HL3
12 Dokumentacja	zgodnie z załącznikiem G
Wartości MTBF (wg MIL-HDBK-217-F2)	dostępne, dostarczane na życzenie dla konkretnych projektów

WAGO spełnia standardy jakościowe zgodnie z certyfikatem **IRIS**.

5 Opis funkcjonowania

5.1 Sieć

5.1.1 Konfiguracja interfejsów

Interfejsy X1 i X2 sterownika połączone są ze zintegrowanym, konfigurowalnym 3-portowym switchem, którego trzeci port połączony jest z CPU.

Dwa interfejsy i konfigurowalny switch umożliwiają tworzenie połączeń:

- w jednej wspólnej sieci ze wspólnym adresem IP dla obu interfejsów lub
- w dwóch osobnych sieciach z własnym adresem IP dla każdego interfejsu.

Przyporządkowanie fizycznych interfejsów (portów) odbywa się przez wirtualne Bridge i może być konfigurowane np. za pomocą WBM.

Bridge	Port	
	X1	X2
1		
2		

Ilustracja 18: Przykład przyporządkowania interfejsów przez WBM

Dla interfejsu X1 można ustawić czasowo stały adres IP (tryb „Fix IP-Address“). Ustawienia tego dokonuje się za pomocą przycisku resetu (patrz rozdział „Uruchamianie“ > ...> „Czasowe ustawienie stałego adresu IP“).

Czasowe ustawienie adresu IP nie ma wpływu na ustawiony wcześniej tryb.

5.1.1.1 Praca w trybie przełącznym

Przy pracy w trybie przełącznym uwzględniane są ustawienia TCP/IP jak adres IP lub maska podsieci dla X1 i X2.

Przy włączaniu trybu przełącznego ustawienia X1 przejmowane są jako nowa wspólna konfiguracja dla X1 i X2.

Urządzenie nie jest już więc dostępne przez adres IP ustawiony wcześniej dla X2. Fakt ten należy uwzględnić w aplikacjach CODESYS, wykorzystujących do komunikacji X2.

5.1.1.2 Praca przy rozłączonych interfejsach sieciowych

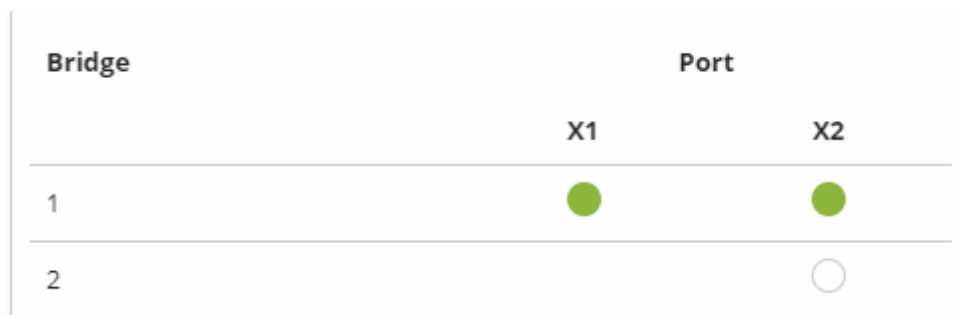
W przypadku pracy przy rozłączonych interfejsach sieciowych oba interfejsy ETHERNET można konfigurować i używać osobno.

Przy przełączaniu na pracę z osobnymi interfejsami sieciowymi interfejs X2 instalowany jest w oparciu o wartości z ostatniego ustawienia. Połączenia realizowane przez interfejs X1 zostają utrzymane.

Przy pracy z osobnymi interfejsami i tymczasowo ustawionym stałym adresem IP urządzenie dostępne jest nadal przez ustawiony adres IP dla interfejsu X2.

5.1.1.3 Przykłady przyporządkowania MAC-ID i adresów IP

Wspólna sieć ze wspólnym adresem IP dla obu złączy



Ilustracja 19: 1 bridge z 2 portami

Tabela 34: Przyporządkowanie MAC-ID i adresów IP dla 1 bridge'a z 2 portami

Bridge	MAC-ID	Adres IP	Port	MAC-ID	Port	MAC-ID
1	01	1	X1	02	X2	03

Dwie oddzielne sieci z osobnymi adresami IP dla każdego złącza.



Ilustracja 20: 2 bridge z portami 1/1

Tabela 35: Przyporządkowanie MAC-ID i adresów IP dla 2 bridge'ów z portami 1/1

Bridge	MAC-ID	Adres IP	Port	MAC-ID	Port	MAC-ID
1	01	1	X1	01		
2	02	2			X2	02

5.1.2 Bezpieczeństwo sieci

5.1.2.1 Użytkownicy i hasła

Sterownik zawiera kilka grup użytkowników, które mogą być wykorzystywane do realizacji różnych zadań.

Dla wszystkich użytkowników ustawione są standardowe hasła. Zaleca się ich zmianę przy pierwszym rozruchu!

Wskazówka Zmiana haseł



Ustawione fabrycznie, standardowe hasła podane w niniejszej instrukcji obsługi nie stanowią wystarczającego zabezpieczenia! Hasła należy zmieniać stosownie do potrzeb!

5.1.2.1.1 Usługi i użytkownicy

W tabeli poniżej wyszczególniono usługi chronione hasłem oraz odpowiadających im użytkowników.

Tabela 36: Usługi i użytkownicy

Usługa	Użytkownik					
	WBM		Linux®			SNMP
	admin	user	root	admin	user	
Web Based Management (WBM)	X	X				
Konsola Linux®			X	X	X	
Console Based Management (CBM)			X			
CODESYS				X		
Telnet			X	X	X	
FTP			X	X	X	
FTPS			X	X	X	
SSH			X	X	X	
SNMP						X

5.1.2.1.2 Grupa użytkowników WBM

WBM ma własną administrację użytkownika. Występujący tu użytkownicy są ze względów bezpieczeństwa odseparowani od pozostałych grup w systemie.

Tabela 37: Użytkownicy WBM

Użytkownik	Uprawnienia	Standardowe hasło
admin	pełne (administrator)	wago
user	ograniczone	user
guest	tylko wyświetlanie	---

Wskazówka



Rozszerzone uprawnienia użytkowników WBM

Użytkownicy WBM „admin” i „user” posiadają uprawnienia wykraczające poza WBM, aby mieć możliwość konfigurowania systemu i instalacji oprogramowania.

Wskazówka



Zmiana haseł

Ustawione fabrycznie, standardowe hasła podane w niniejszej instrukcji obsługi nie stanowią wystarczającego zabezpieczenia! Hasła należy zmieniać stosownie do potrzeb!

Więcej informacji zawarto w rozdziale „Zarządzanie użytkownikami WBM”.

5.1.2.1.3 Grupa użytkowników Linux®

Grupa Linux® obejmuje właściwych użytkowników systemu operacyjnego, wykorzystywanych także przez większość serwisów.

Tabela 38: Użytkownicy Linux®

Użytkownik	Charakterystyka	Katalog home	Standardowe hasło
root	Superuser	/root	wago
admin	Użytkownik CODESYS	/home/admin	wago
user	Zwykły użytkownik	/home/user	user

Hasła dla tych użytkowników można konfigurować poprzez połączenie terminalowe.

Wskazówka



Zmiana haseł

Ustawione fabrycznie, standardowe hasła podane w niniejszej instrukcji obsługi nie stanowią wystarczającego zabezpieczenia! Hasła należy zmieniać stosownie do potrzeb!

5.1.2.1.4 Grupa użytkowników SNMP

Usługa SNMP ma własne zarządzanie użytkownikami. W ustawieniach fabrycznych nie ma założonych żadnych użytkowników.

5.1.2.2 Uwierzytelnianie serwera WWW

Strony WBM sterownika można otwierać za pomocą protokołu HTTP lub HTTPS. Preferowany jest HTTPS, gdyż wykorzystuje on protokół TLS. Protokół TLS zabezpiecza komunikację poprzez kodowanie i uwierzytelnienie.

Standardowe ustawienie sterownika umożliwia zaawansowane kodowanie, wykorzystuje jednak tylko zwykłe metody uwierzytelnienia. Ponieważ uwierzytelnianie odgrywa kluczową rolę dla wszystkich bezpiecznych kanałów komunikacyjnych, zdecydowanie zaleca się bezpieczniejszy rodzaj uwierzytelnienia. Bazą uwierzytelnienia jest certyfikat bezpieczeństwa zapisany w sterowniku. Domyślną lokalizacją certyfikatu bezpieczeństwa jest `/etc/lighttpd/https-cert.pem`.

W ustawieniu fabrycznym sterownik używa generycznego certyfikatu bezpieczeństwa w formacie x509. Aby umożliwić bezpieczne uwierzytelnienie, generyczny certyfikat bezpieczeństwa należy zastąpić specyficznym dla danego urządzenia.

5.1.2.2.1 Szyfrowanie TLS

Podczas nawiązywania połączenia HTTPS przeglądarka internetowa i serwer WWW negocjują wersję TLS i metodę kryptograficzną.

Poprzez grupę „TLS Configuration” strony WBM „Security” można przełączać dopuszczone przez HTTPS procedury kryptograficzne i użyteczne wersje TLS.

Możliwe są ustawienia „Strong” i „Standard”.

Przy ustawieniu „Strong” serwer internetowy zezwala tylko na wersję TLS 1.2 i na silne algorytmy. Starsze oprogramowanie i starsze systemy operacyjne mogą nie obsługiwać protokołu TLS 1.2 i algorytmów szyfrowania.

Ustawienie „Standard” zezwala na wersje TLS 1.0, TLS 1.1, TLS 1.2, a także metody kryptograficzne, które obecnie nie są już uważane za bezpieczne. Użycie jest zalecane tylko w przypadku zgodności wstecznej ze starszymi systemami.

Informacja



Techniczna dyrektywa TR-02102 BSI

Zasady dotyczące ustawienia „Strong” są oparte na wytycznej technicznej TR-02102 Federalnego Urzędu ds. Bezpieczeństwa Informacji. Wytyczne można znaleźć w Internecie pod adresem: <https://www.bsi.bund.de> > „Publikacje” > „Wytyczne techniczne”.

Informacja**Wytyczne BSI dotyczące migracji do TLS 1.2**

Wytyczne Federalnego Urzędu ds. Bezpieczeństwa Informacji dotyczące migracji do TLS 1.2 zawierają „matryce zgodności”, które określają, które oprogramowanie jest zgodne z TLS 1.2.

Przewodnik można znaleźć w Internecie pod adresem:

<https://www.bsi.bund.de> > „Topics“ > „Standards and Criteria“ > „Minimum Standards“.

5.1.2.3 Certyfikaty Root

Przy komunikacji szyfrowanej przez TLS w celu sprawdzania wiarytelności partnera komunikacyjnego stosowane są certyfikaty Root.

Certyfikat Root, który został sygnowany przez urząd certyfikacji, służy do weryfikacji ważności wszystkich certyfikatów, wystawionych przez ten urząd certyfikacji.

Bazę dla uwierzytelnienia usług podłączonych przez Internet (np. dostawca skrzynki elektronicznej, usługi chmury) tworzą zapisane w sterowniku certyfikaty Root (Root-CA Bundle).

Standardowym miejscem ewidencji certyfikatów Root jest:
`/etc/ssl/certs/ca-certificates.crt`.

Plik zawiera certyfikaty udostępnione przez Mozilla. Listę certyfikatów Root i okres ich ważności można sprawdzić pod następującym adresem:

<https://hg.mozilla.org/releases/mozilla-release/raw-file/79f079284141/security/nss/lib/ckfw/builtins/certdata.txt>

Certyfikaty Root można aktualizować przez aktualizację pliku:
`/etc/ssl/certs/ca-certificates.crt` w sterowniku (patrz rozdział „Serwis” > „Aktualizacja certyfikatów Root”).

5.1.3 Konfiguracja sieci

5.1.3.1 Nazwa hosta/nazwa domeny

Bez konfiguracji nazwy hosta sterownik otrzymuje standardową nazwę, w skład której wchodzi ostatnie trzy wartości adresu MAC sterownika, np. „PFx00-A1A2A3”. Nazwa ta obowiązuje do momentu skonfigurowania nazwy hosta lub dostarczenia jej przez DHCP do sterownika (informacje na temat konfiguracji sterownika patrz rozdział „Uruchamianie” > „Konfiguracja”). Przy ustawianiu nazwy hosta należy pamiętać, że nazwa dostarczona przez odpowiedź DHCP jest natychmiast aktywowana i zastępuje nazwę standardową. Przy kilku interfejsach sieciowych z DHCP zawsze obowiązuje ostatnia otrzymana nazwa hosta. Jeśli ma obowiązywać tylko nazwa skonfigurowana, administrator sieci musi tak dostosować konfigurację aktywnego serwera DHCP, aby w odpowiedzi DHCP nie były wysyłane nazwy hosta.

Standardowa lub skonfigurowana nazwa hosta staje się znów aktywna, gdy interfejsy sieciowe zostają przestawione na statyczne adresy IP lub gdy w odpowiedzi DHCP nie nadeszła jeszcze nazwa hosta.

Nazwa domeny podlega tym samym mechanizmom co nazwa hosta. Różnica polega na tym, że nie ma standardowej nazwy domeny. Nazwa domeny pozostaje pusta dopóty, dopóki nie zostanie skonfigurowana lub dostarczona przez DHCP.

5.1.3.2 Routing

W ramach konfiguracji TCP/IP sterownik dopuszcza ustawienie tras statycznych, IP-Masquerading i Port-Forwarding. Konfiguracja bram domyślnych odbywa się przy zastosowaniu tras statycznych, ponieważ brama domyślna jest szczególnym przypadkiem trasy statycznej.

Urządzenie w sieci wysyła do bramy wszystkie pakiety danych dla systemów, znajdujących się poza swoją siecią lokalną. Ta brama może przesyłać te pakiety dalej tak, aby dotarły do systemu docelowego. Aby możliwe było osiągnięcie różnych systemów docelowych, konieczna może być konfiguracja kilku bram. Konfiguracji tej dokonuje się przez dodanie parametrów routingu. Parametr routingu składa się z następujących danych:

- Destination Address
- Destination Mask
- Gateway Address
- Gateway Metric

Na podstawie ustawień systemu docelowego, takich jak Destination Address i Destination Mask, podejmowana jest decyzja, do której bramy ma być skierowany pakiet danych. System docelowy może być określony pojedynczym

adresem IP lub zakresem adresów. Dla pakietu danych, który ma być przesłany, wybierany jest zawsze ten parametr routingu, który wykazuje najbardziej specyficzne parametry lub Destination Address i Destination Mask. Brama domyślna odpowiada najmniej specyficznemu parametrowi routingu. Wszystkie pakiety danych o adresie docelowym (Destination Address) i adresie maski (Destination Mask), dla których nie istnieje specyficzny parametr routingu, wysyłane są do tej bramy domyślnej.

Default Gateway

Jeśli w oknie „Destination Address” ustawiona jest wartość „default”, definiowana jest brama docelowa, zwana też trasą docelową (Default Route). W oknie „Destination Mask” powinna być wpisana wartość „0.0.0.0”.

Route

Jeśli w oknie „Destination Address” wpisany jest adres IP lub zakres adresów, wszystkie pakiety danych, skierowane pod ten adres lub zakres adresów, wysyłane są na wpisany adres bramy.

Jeśli adres IP bramy leży poza zakresem adresów osiągalnym dla sterownika, odpowiednia trasa nie zostaje aktywowana.

Każdemu parametrowi routingu przyporządkowana jest metryka.

Jeśli ustawionych jest kilka parametrów routingu dla tego samego adresu docelowego i maski docelowej, na podstawie metryki ustalany jest priorytet między poszczególnymi parametrami. Parametry o niskiej metryce mają w tym przypadku pierwszeństwo w stosunku do parametrów o wyższej metryce.

Metryka skonfigurowanych parametrów routingu może zostać dla sterownika zadana. Standardowa wartość metryki wynosi 20. Oprócz ręcznej konfiguracji tras można także ustawiać bramy domyślne za pomocą odpowiedzi DHCP. Wszystkie bramy domyślne nadesłane przez DHCP otrzymują niezmiennie metrykę o wartości 10.

Przykład metryki:

Sterownik pobiera konfigurację IP przez serwer DHCP i otrzymuje adres IP oraz maskę sieci 192.168.1.10/24. Ponadto w sterowniku ustawia się ręcznie bramę z adresem IP 192.168.1.2 oraz metryką o wartości 20. A więc pakiety danych sieciowych, w przypadku których dla adresu docelowego nie istnieje specyficzny parametr routingu, sterownik wysyła do bramy 192.168.1.2. Serwer DHCP musi przy rozdziale oprócz adresu IP i maski sieci uwzględnić także bramę docelową 192.168.1.1. Ta brama domyślna zostaje opatrzona przez sterownik metryką o wartości 10. Dzięki temu brama domyślna otrzymana za pośrednictwem DHCP ma priorytet w stosunku do bram skonfigurowanych ręcznie.

Poprzez parametry routingu konfiguruje się, do których bram wysyłane są pakiety danych sieciowych. Jeśli sterownik pracuje w trybie „Switched” i posiada tylko jeden interfejs sieciowy, cała komunikacja sieciowa odbywa się poprzez ten interfejs. Jeśli sterownik pracuje w trybie „Seperated” lub zawiera modem, wyposażony jest w kilka interfejsów sieciowych. Dzięki temu pakiet danych może docierać do sterownika poprzez jeden interfejs sieciowy i opuszczać go przez drugi. Ta funkcja przekazywania danych między różnymi interfejsami sieciowymi

powinna zostać w sposób jednoznaczny udostępniona i jest w ustawieniach fabrycznych dezaktywowana. W celu aktywacji funkcji przekazywania danych do kolejnego sterownika należy aktywować „Routing enabled entirely” w grupie „General Routing Configuration”. W tym przypadku sterownik może pełnić funkcję routera.

Aby przekierować komunikację sieciową przez router, należy pamiętać, że nie tylko router, ale także punkty końcowe komunikacji muszą otrzymać odpowiednie parametry routingu. Parametry routingu punktów końcowych muszą zapewniać, że żądane pakiety danych sieciowych są wysyłane przez router zarówno podczas nawiązywania połączenia, jak i podczas odpowiedzi.

Przykład dla trasy hosta:

Trasa hosta to trasa do pojedynczego hosta. W poniższym przykładzie należy podać trasę do hosta o adresie IP 192.168.1.2. Trasa ma przebiegać przez bramę dostępną przez adres 10.0.1.3. Aby w sterowniku połączonym z bramą skonfigurować trasę do hosta docelowego, należy wprowadzić następujące ustawienia:

Destination Address:	192.168.1.2	Adres IP docelowego hosta
Destination Mask:	255.255.255.255	Maska podsieci pojedynczego hosta
Gateway Address:	10.0.1.3	Adres IP bramy
Gateway Metric:	20	Priorytet trasy

Przykład dla trasy sieci:

Trasa sieci to trasa do podsieci, zawierającej kilka hostów. W poniższym przykładzie należy podać trasę do podsieci o adresie IP 192.168.1.0. Trasa ma przebiegać przez bramę dostępną przez adres 10.0.1.3. Aby w sterowniku połączonym z bramą skonfigurować trasę do sieci docelowej, należy wprowadzić następujące ustawienia:

Destination Address:	192.168.1.0	Adres IP sieci docelowej
Destination Mask:	255.255.255.0	Maska podsieci sieci docelowej
Gateway Address:	10.0.1.3	Adres IP bramy
Gateway Metric	20	Priorytet trasy

Oprócz konfiguracji tras statycznych sterownik obsługuje IP-Masquerading. Funkcję tę można aktywować dla wybranych interfejsów sieciowych sterownika. Pakiety danych opuszczające sterownik przez interfejs sieciowy, dla którego aktywowana jest funkcja IP-Masquerading, otrzymują jako adres nadawcy adres IP interfejsu sieciowego. Gdy pakiety danych są przesyłane przez sterownik dalej, sieć znajdująca się za sterownikiem zostaje ukryta pod jednym adresem.

Ponadto sterownik dopuszcza konfigurację parametrów Port-Forwarding. Przy Port-Forwarding nadpisane zostają adres docelowy i port docelowy dla pakietu danych, który dotarł do sterownika przez skonfigurowany wcześniej interfejs sieciowy. Dzięki temu możliwe jest przekazywanie dalej pakietów danych przez sterownik do innych adresów i portów. Funkcję przesyłania dalej pakietów można skonfigurować dla protokołów UDP i TCP.

5.1.4 Usługi sieciowe

5.1.4.1 DHCP Client

Poprzez usługę DHCP Client sterownik może pobierać parametry sieci z zewnętrznego urządzenia DHCP master.

Pobierane są następujące parametry:

- adres IP
- maska podsieci
- router/gateway
- nazwa hosta
- domena
- serwer DNS
- serwer NTP

W przypadku parametrów takich jak adres IP, maska podsieci i router/gateway parametry zapisuje się dla każdego interfejsu ETHERNET.

Nazwa hosta i domena zapisywane są zgodnie z zasadą LIFO (Last In First Out). Stosowane są zawsze ustawienia ostatniego odebranego komunikatu DHCP OFFER.

Parametry serwera DNS i NTP zapisywane są centralnie do globalnego użytku. Wszystkie przekazane parametry zostają zapisane.

5.1.4.2 DHCP Server

Oferowana przez sterownik usługa DHCP Server służy do automatycznej konfiguracji adresów IP urządzeń w tej samej podsieci. Zazwyczaj w danym momencie w podsieci może być aktywny tylko jeden serwer DHCP.

Dla serwera DHCP można ustawić następujące parametry:

- sama usługa (aktywna/nieaktywna)
- zakres dynamicznie nadawanych adresów IP
- czas ważności (Lease Time) dynamicznie nadawanych adresów IP
- lista statycznych przyporządkowań adresów IP do adresów MAC

W trybie „switched” ustawienia te mogą być wprowadzane wspólnie dla wszystkich interfejsów sieciowych, a w trybie „separated” definiowane są dla każdego z interfejsów sieciowych osobno.

Ustawienia wprowadza się np. w WBM na stronie „DHCP Configuration”.

Oprócz adresu IP serwer DHCP przekazuje także inne parametry. Ich pełną listę zawiera poniższa tabela.

Tabela 39: Lista parametrów wysyłanych przez DHCP.

Parametr	Znaczenie
IP address	Adres IP z dopuszczalnego zakresu adresów; zakres ten można konfigurować w WBM. Na podstawie adresu MAC urządzenia wysyłającego zapytanie (client) i zakresu adresów serwer DHCP ustala adres IP, który zostaje przesłany do tego urządzenia. Tak długo, jak skonfigurowany zakres adresów nie zostaje zmieniony i nie występują ograniczenia w przydzielaniu adresów IP, serwer DHCP będzie przydzielał urządzeniom wysyłającym zapytanie zawsze te same adresy IP. Jeśli zgłasza się urządzenie, dla którego adresu MAC został w WBM skonfigurowany stały adres IP, ten adres zostaje mu przydzielony. Przydzielony w ten sposób stały adres IP nie może leżeć poza zakresem dostępnych adresów IP. W celu identyfikacji urządzenia wysyłającego zapytanie, zamiast adresu MAC może zostać nadana także nazwa hosta.
Subnet mask	Przesłana zostaje maska podsieci konfigurowana w ustawieniach sieciowych serwera DHCP dla danej sieci lokalnej. Maska podsieci i adres IP określają dostępny zakres adresów IP w sieci lokalnej.
Broadcast address	Adres IP, za pomocą którego pakiet IP może być równocześnie wysłany do wszystkich urządzeń w podsieci.
Lease time	Określa czas ważności parametrów nadanych przez DHCP dla urządzenia w sieci; urządzenie jest zobowiązane przez protokół do wysłania ponownego zapytania po upływie połowy czasu ważności ustawień sieciowych. Lease time jest konfigurowany w WBM.
Host name	Nazwa sieci jest przesyłana do urządzenia. Zazwyczaj urządzenie wysyła swoją nazwę wraz z zapytaniem o adres IP. Wykorzystywana jest ona potem przez serwer DHCP w odpowiedziach.
Name server	Serwer DHCP przekazuje swój własny adres IP jako serwer DNS do urządzenia w sieci.

Tabela 39: Lista parametrów wysyłanych przez DHCP.

Parametr	Znaczenie
Default gateway	Serwer DHCP przekazuje swój własny adres IP jako bramę domyślną do urządzenia w sieci. Brama domyślna wykorzystywana jest do komunikacji z urządzeniami znajdującymi się poza siecią lokalną.

Nie wszystkie parametry można ustawić w WBM. Jeśli dla istniejących parametrów mają być ustawione inne wartości lub nadane kolejne parametry przez DHCP, serwer DHCP musi zostać skonfigurowany ręcznie. W przypadku sterownika usługa serwera DHCP przejmowana jest przez program „dnsmasq”. W celu ustawienia konfiguracji należy za pomocą wiersza poleceń Linux®, dostosować w edytorze plik „/etc/dnsmasq.d/dnsmasq_default.conf”.

5.1.4.3 DNS Server

Oferowana przez sterownik usługa DNS Server służy do automatycznego przyporządkowania nazw hosta do adresów IP urządzeń. Serwer DNS przejmuje od serwera DHCP nazwy i adresy IP urządzeń w lokalnej sieci. Zapytania o nazwy nielocalne, na przykład z Internetu, serwer DNS przekazuje do nadrzędnego serwera DNS, o ile taki został skonfigurowany i jest dostępny.

Dla serwera DNS można ustawić następujące parametry:

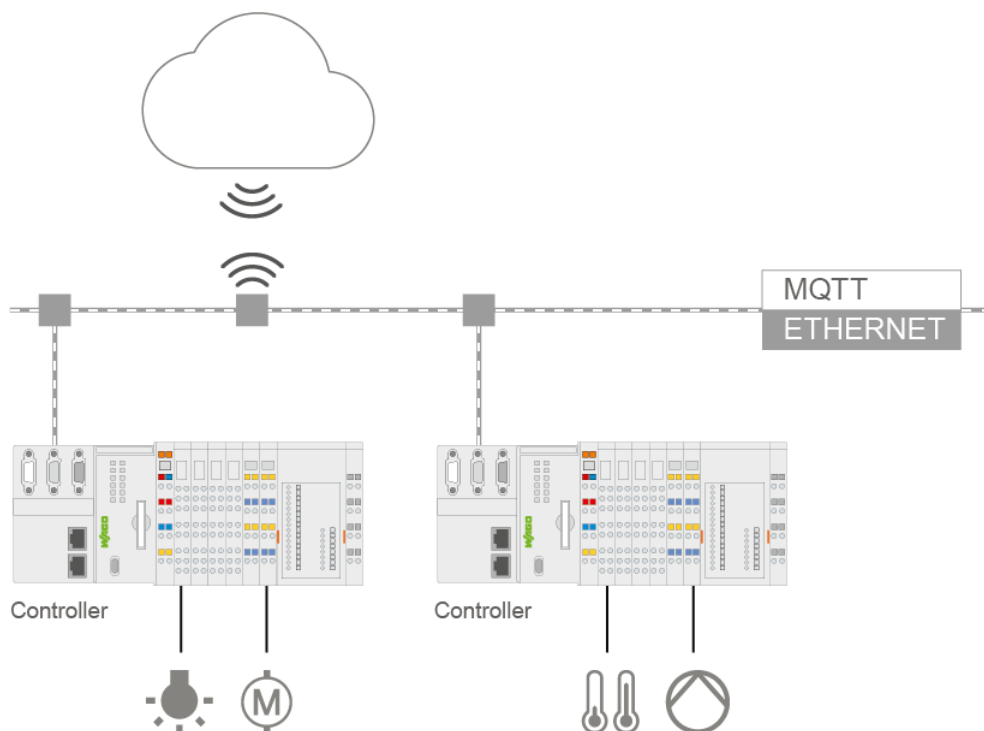
- sama usługa (aktywna/nieaktywna)
- rodzaj dostępu do przyporządkowań
 - w trybie „Proxy” zapytania są buforowane (optymalizacja natężenia przepływu)
 - w trybie „Relay” zapytania są przesyłane bezpośrednio do nadrzędnego serwera DNS.
- lista zawierająca maksymalnie 15 statycznych przyporządkowań adresów IP do nazw hosta
Jeśli wykorzystywana jest tylko nazwa hosta, zostaje ona rozszerzona o skonfigurowaną lub domyślną nazwę domeny w celu zapewnienia zgodności z budową nazwy FQDN.

Ustawienia wprowadza się np. w WBM na stronie „Configuration of DNS Service”.

5.1.5 Funkcjonalność Cloud Connectivity

Dzięki funkcjonalności Cloud Connectivity i bibliotece IEC sterownik może służyć jako brama dla aplikacji w zakresie Internet-of-Things (IoT). Sterownik może zbierać dane ze wszystkich podłączonych urządzeń i poprzez wbudowany interfejs ETHERNET lub moduł sieci komórkowej łączyć się z Internetem i wysyłać dane do chmury.

Usługę chmury można ustawić; do wyboru jest m.in. Microsoft Azure, Amazon Web Services i IBM Cloud.



Ilustracja 21: Podłączenie sterownika do usługi chmury (przykład)

Dane przenoszone są ze sterownika do chmury w formacie JSON. Połączenie można zaszyfrować przez TLS (patrz rozdział „Opis funkcji” > ... > „Szyfrowanie TLS”).

Ustawienia dotyczące funkcjonalności Cloud Connectivity, które należy wprowadzić w sterowniku, można znaleźć w rozdziale „Uruchamianie” > ... > „Konfiguracja za pomocą Web-Based-Management (WBM)”.

Parametry komunikacyjne konfiguruje się w WBM, a dane wymieniane między chmurą a sterownikiem konfiguruje się za pomocą bibliotek do **e!COCKPIT** lub CODESYS 2.3.

Wskazówka



Uwzględnić ryzyko wynikające z korzystania z chmury!

Podczas korzystania z usługi chmury wrażliwe dane powierza się operatorowi chmury na własną odpowiedzialność. W efekcie dostępu z zewnątrz dane mogą być poddane manipulacji, a niezamierzone polecenia mogą mieć niepożądany wpływ na funkcjonalność układu sterowania.

Aby chronić dane, należy stosować metody ich szyfrowania oraz przestrzegać zaleceń Federalnego Urzędu ds. Bezpieczeństwa w zakresie techniki informatycznej, zawartych w publikacji „Cloud: Risks and Security Tips”.

Na terenie kraju użytkownika należy uwzględnić zalecenia odpowiednich organów, zawarte w porównywalnych publikacjach.

Informacja



Uwzględnić dodatkową dokumentację!

Szczegółowy opis pakietu oprogramowania Cloud Connectivity ze sterownikiem i informacje na temat programowania PLC znaleźć można w instrukcji A500920 w zakładce „Pobierz” na stronie www.wago.com.

Informacja



Uwzględnić wymagane ustawienia dotyczące ochrony danych i bezpieczeństwa!

Przed zastosowaniem funkcjonalności Cloud Connectivity należy zapoznać się z zagadnieniami ochrony danych i bezpieczeństwa, omówionymi w stosownym podręczniku. Można go znaleźć w zakładce „Pobierz” na stronie www.wago.com.

5.1.5.1 Komponenty pakietu oprogramowania Cloud Connectivity

Tabela 40: Komponenty pakietu oprogramowania Cloud Connectivity

Komponenty	Opis
e!COCKPIT: WagoAppCloud	Biblioteki IEC do tworzenia aplikacji PLC. Bloki funkcyjne umożliwiają wysyłanie i odbieranie danych między PLC i chmurą. Zmienne dotyczące transmisji danych można definiować.
CODESYS 2.3: WagoLibCloud	

5.2 Funkcja karty pamięci

Wskazówka Stosować tylko zalecane karty pamięci!



Należy stosować wyłącznie karty pamięci SD z oferty WAGO (nr kat. 758-879/000-001 i 758-879/000-2108), ponieważ są one przeznaczone do zastosowań przemysłowych w trudnych warunkach środowiskowych i do użytku w tym urządzeniu.
Nie ma gwarancji kompatybilności z innymi dostępnymi w sprzedaży nośnikami pamięci.

Karta pamięci jest opcjonalna i spełnia rolę dodatkowego obszaru zapisu – oprócz pamięci wewnętrznej lub dysku w sterowniku sieciowym. Na karcie pamięci można zapisać program użytkowy, dane użytkownika, kod źródłowy projektu lub ustawień urządzenia, a tym samym przekopiować istniejące już dane projektu i programy na jeden lub kilka sterowników sieciowych.

Wskazówka Dezaktywować ochronę przed zapisem!



Aby był możliwy zapis danych na karcie pamięci, należy dezaktywować ochronę przed zapisem, odpowiednio ustawiając suwak. Jest on umieszczony na dłuższej stronie karty pamięci.

Po włożeniu karty pamięci jest ona widoczna pod /media/sd w strukturze katalogu wewnętrznego systemu plików w sterowniku. Dzięki temu kartę pamięci można stosować jako pamięć wymienną również na komputerze PC.

Sposób działania karty pamięci w trybie normalnej pracy oraz możliwe usterki w czasie stosowania karty pamięci zostały opisane w kolejnych rozdziałach, zgodnie z kolejnością eksploatacji karty.

5.2.1 Formatowanie

Wskazówka Pamiętać o sformatowaniu karty pamięci!



Należy mieć na uwadze, że karty pamięci ≤ 2 GB są często sformatowane za pomocą systemu plików „FAT16” i w katalogu głównym mogą pomieścić maksymalnie 512 bajtów. Przy większej liczbie bajtów niż 512 należy utworzyć podkatalog lub sformatować kartę pamięci za pomocą „FAT32” lub „NTFS”.

Wskazówka Dostęp do karty pamięci z CODESYS możliwy tylko przy użyciu FAT16, FAT32 lub NTFS!



Aby użytkownik CODESYS „admin” (patrz rozdział „Sieć” > „Bezpieczeństwo sieci” > „Użytkownicy i hasła” > „Usługi i użytkownicy”) mógł mieć dostęp do danych, umieszczonych na karcie pamięci, musi być ona sformatowana w systemie FAT16, FAT32 lub NTFS.
Przy zastosowaniu formatów systemu plików dla Linux EXT2 lub EXT3 dostęp do plików wymaga uprawnień „Root”. Dostęp przez CODESYS jest niemożliwy.

5.2.2 Bezpieczeństwo danych

Z myślą o bezpieczeństwie i możliwości przywrócenia danych sterownik wyposażony jest w funkcję „Backup” i „Restore”.

Odpowiednie ustawienia wprowadza się na stronie WBM lub przez menu CBM „Backup” i „Restore”; tu także realizuje się te funkcje.

Ustawić można nośnik pamięci (pamięć wewnętrzna lub karta SD) oraz miejsce zapisu w sieci.

Ponadto wybiera się dane, które mają być zabezpieczone lub przywrócone:

- projekt CODESYS („PLC Runtime Projekt”, projekt bootowalny)
- ustawienia urządzenia („Settings”)
- system operacyjny sterownika („System”)
- wszystkie poprzednie („All”, widoczne tylko wtedy, gdy nie są zapisane w sieci)

Wskazówka



Uwzględnić wersję firmware!

Przywrócenie systemu operacyjnego sterownika (opcja „System”) jest dopuszczalne i możliwe tylko wtedy, gdy wersje firmware w czasie tworzenia kopii zapasowej i przywracania są identyczne.

W razie potrzeby należy pominąć przywracanie systemu operacyjnego sterownika lub dopasować wcześniej uprzednio wersję firmware sterownika do wersji firmware w momencie tworzenia kopii zapasowej.

5.2.2.1 Funkcja „Backup”

Funkcja „Backup” pozwala zapisywać pliki wewnętrznej pamięci oraz ustawienia urządzeń na karcie pamięci podczas pracy.

Dostęp do funkcji „Backup” można uzyskać za pośrednictwem strony WBM „Firmware Backup” lub menu CBM „Firmware Backup”.

Jako nośnik docelowy można wybrać sieć lub kartę pamięci (jeśli jest włożona).

Pliki wewnętrznego dysku są zapisywane na wybranym nośniku docelowym w katalogu media/sd/copy i odpowiednich podkatalogach.

Informacje, które nie są dostępne w sterowniku sieciowym w formie plików, są zapisane w formacie XML w katalogu media/sd/settings.

Gdy jako nośnik docelowy zostanie wybrana karta pamięci, wskaźnik LED umieszczony nad gniazdem karty pamięci będzie podczas zapisu migał na żółto.

Ustawienia urządzenia oraz pliki z wewnętrznego dysku zostają następnie zapisane na docelowym nośniku.

Sterownik oferuje funkcję automatycznej aktualizacji. Jeśli funkcja ta zostanie aktywowana przed zabezpieczeniem danych na karcie pamięci, a sterownik będzie bootowany z tej karty, dane zostaną automatycznie odtworzone w wewnętrznej pamięci sterownika.

Wskazówka**Do sieci można skopiować tylko jeden package!**

Jeśli jako miejsce docelowe ustawiona jest opcja „Network“, dla każdego procesu zapisu można wybrać tylko jeden package.

Wskazówka**Brak funkcji „Backup“ dla karty pamięci!**

Nie ma możliwości utworzenia kopii zapasowej karty pamięci w wewnętrznej pamięci flash.

Wskazówka**Uwzględnić czas backupu**

Tworzenie plików backup może potrwać kilka minut. Aby skrócić ten czas, należy przed rozpoczęciem tworzenia kopii zapasowych zatrzymać program CODESYS.

5.2.2.2 Funkcja Restore

Za pomocą funkcji Restore można podczas pracy ładować pliki oraz ustawienia urządzeń z karty pamięci do pamięci wewnętrznej.

Dostęp do funkcji Restore można uzyskać przez stronę WBM „Firmware Restore“ lub menu CBM „Firmware Restore“.

Jako nośnik źródłowy można wybrać sieć lub kartę pamięci (jeśli jest włożona).

Gdy jako nośnik źródłowy zostanie wybrana karta pamięci, wskaźnik LED umieszczony nad gniazdem karty pamięci będzie podczas ładowania migał na żółto.

Podczas ładowania dane z katalogu media/sd/copy medium źródłowego zostaną skopiowane do odpowiednich katalogów pamięci wewnętrznej.

Urządzenie dysponuje aktywną i nieaktywną partycją root. Zabezpieczenie systemu zapisywane jest w partycji nieaktywnej. Restart następuje z nowo nagranej partycji. Jeśli procedura startu może być zakończona, aktywowana zostaje nowa partycja. W przeciwnym razie przy kolejnym bootowaniu wykorzystana zostanie stara partycja.

Po restarcie następuje automatyczne załadowanie projektu boot oraz automatyczne aktywowanie ustawień. To, czy projekt bootowalny załadowany zostanie z wewnętrznego dysku, czy z karty SD, zależy od ustawionej opcji „Bootproject location“ na stronie WBM „General PLC Runtime Configuration“.

Wskazówka	Rozmiar danych nie może przekraczać rozmiaru pamięci wewnętrznej! Należy pamiętać, że rozmiar danych w katalogu media/sd/copy nie może przekraczać rozmiaru wewnętrznego dysku.
	
Wskazówka	Przywracanie możliwe tylko z wewnętrznej pamięci! Jeśli urządzenie było bootowane z karty pamięci, przywrócenie firmware nie jest możliwe.
	
Wskazówka	Reset przez przywracanie Reset można wykonać przez przywrócenie systemu, ustawień lub CODESYS!
	
Wskazówka	Utrata połączenia w wyniku przywracania Jeśli przy przywracaniu zmienią się parametry połączenia ETHERNET, WBM nie będzie mógł nawiązać połączenia z urządzeniem. Trzeba wtedy ponownie otworzyć WBM, wpisując w pasku adresu poprawny adres IP urządzenia.
	

5.2.3 Wkładanie karty pamięci podczas pracy

Węzeł sieciowy i program PLC są uruchomione.

Kartę pamięci wkłada się do pracującego urządzenia.

W normalnym trybie pracy karta pamięci zostanie włączona do systemu plików sterownika sieciowego jako dysk.

Nie są inicjowane automatyczne procesy kopiowania.

LED nad kartą pamięci miga w czasie dostępu na żółto.

Karta pamięci jest teraz gotowa do pracy i dostępna pod /media/sd.

5.2.4 Wyjmowanie karty pamięci podczas pracy

Węzeł sieciowy i program PLC są uruchomione, a karta pamięci jest włożona.

Kartę pamięci wyjmuje się z pracującego urządzenia.

Wskazówka**Dane mogą zostać utracone w czasie zapisywania!**

Należy pamiętać, że w razie wyjęcia karty pamięci podczas zapisu dane zostaną utracone.

LED nad kartą pamięci miga w czasie próby dostępu na żółto.

Sterownik pracuje następnie bez karty pamięci.

5.2.5 Ustawienia katalogu Home dla systemu runtime

Standardowo katalog Home dla systemu runtime znajduje się w wewnętrznej pamięci sterownika. W katalogu Home zapisywany jest między innymi istniejący aktualnie projekt boot.

Za pomocą WBM można przełożyć katalog Home dla systemu runtime na kartę pamięci, aby zyskać więcej pamięci dla dużego projektu boot lub innych plików.

Ustawienie można realizować zaznaczając pole wyboru opcji „Home directory on memory card enabled” na stronie WBM „PLC Runtime”. Zostaje ono przejęte po kliknięciu przycisku **[Submit]** i realizowane po następnym restarcie. Pliki ze starego katalogu Home nie są kopiowane do nowego.

Po przełączeniu projekt musi być załadowany na nowo a projekt boot założony od nowa.

Należy pamiętać, że pod żadnym pozorem nie wolno wyjmować karty pamięci, dopóki znajduje się na niej katalog Home. Przy działającej aplikacji mogłoby to spowodować niekontrolowane zawieszenie się sterownika.

Przenoszenie katalogu Home jest bezskuteczne, jeśli sterownik został uruchomiony z karty pamięci. Stan konfiguracji jest zapisywany, jednak jego realizacja następuje dopiero po skopiowaniu zawartości karty pamięci do pamięci wewnętrznej.

5.2.6 Ładowanie projektu bootowalnego

Istniejący projekt bootowalny ładowany jest w zależności od ustawień w katalogu Home dla systemu runtime. Poniższa tabela pokazuje możliwe rezultaty:

Tabela 41: Ładowanie projektu bootowalnego

Projekt bootowalny zostaje zapisany w wewnętrznej pamięci flash.	Wetknięta karta pamięci z projektem bootowalnym	Zaznaczona opcja „Home directory on memory card enabled“	Projekt bootowalny zostaje załadowany ...
nie	nie	nie	nie, brak projektu bootowalnego
		tak	nie, brak projektu bootowalnego
	tak	nie	nie, brak projektu bootowalnego w wewnętrznej pamięci flash
		tak	tak, z karty pamięci
tak	nie	nie	tak, z wewnętrznej pamięci flash
		(tak) niedozwolona	nie, niedozwolona kombinacja, ponieważ dla tego ustawienia nie może istnieć projekt bootowalny w wewnętrznej pamięci flash.
	tak	nie	tak, z wewnętrznej pamięci flash
		(tak) niedozwolona	nie, niedozwolona kombinacja, ponieważ dla tego ustawienia nie może istnieć projekt bootowalny w wewnętrznej pamięci flash.

5.3 Elementy oprogramowania wymagające licencji

Dla sterownika 2. generacji (750-821x/xxx-xxx) dostępne są komponenty programowe systemu runtime **e!RUNTIME**, podlegające kontroli licencji (licencje runtime).

Licencjonowanie można przeprowadzić przy użyciu **e!COCKPIT**. Odpowiednią instrukcję można znaleźć w dokumentacji do **e!COCKPIT**.

Produktywne i nieograniczone czasowo zastosowanie licencjonowanych komponentów programowych wymaga posiadania klucza licencyjnego. Przez 30 dni można korzystać z komponentów oprogramowania także bez klucza licencyjnego. Do okresu testowego wliczają się tylko dni rzeczywistego użytkowania. Po upływie okresu testowego dostęp bez klucza licencyjnego nie jest możliwy.

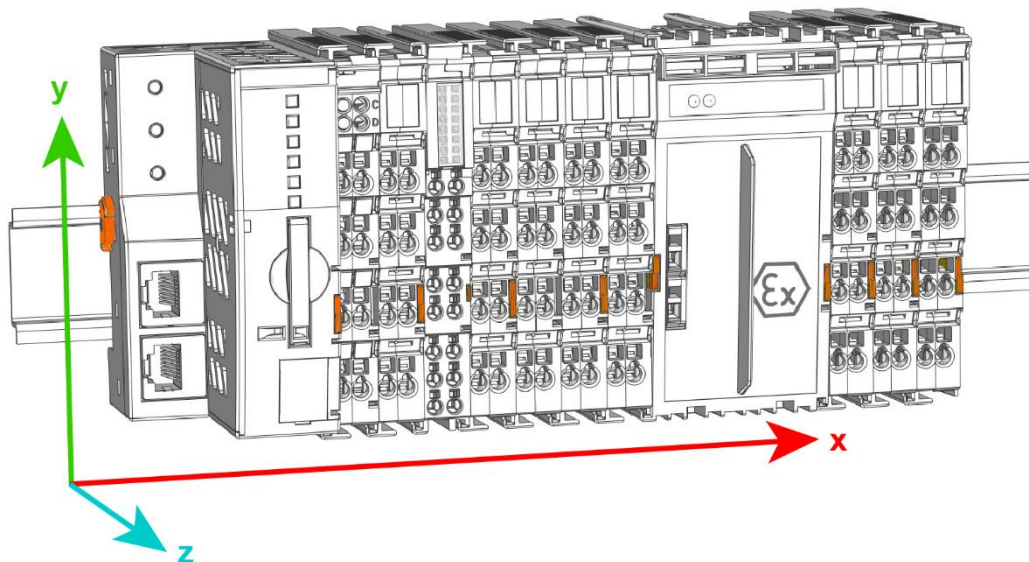
Status licencji („Trwa okres testowy“ lub „Okres testowy upłynął“) sygnalizowany jest przez sterownik za pomocą LED SYS.

Podczas instalowania oprogramowania zawierającego licencjonowane komponenty w **e!COCKPIT** pojawia się informacja o liczbie dni pozostałych do wygaśnięcia licencji.

6 Montaż

6.1 Pozycja montażu

6.1.1 Układ współrzędnych



Ilustracja 22: Układ współrzędnych: szerokość (x), wysokość (y), głębokość (z)

- Szerokość = wymiar wzdłuż osi x = poziomo w zasadniczej pozycji montażu, równoległe do osi szyny montażowej
- Wysokość = wymiar wzdłuż osi y = pionowo w zasadniczej pozycji montażu
- Głębokość = wymiar wzdłuż osi z = poziomo w zasadniczej pozycji montażu, prostopadłe do osi szyny montażowej

Wskazówka



Zmiana układu współrzędnych

W dokumentacji produktowej opublikowanej przed rokiem 2021 zamieniona była wysokość (y) z głębokością (z)!

6.1.2 Przegląd pozycji montażu

Dla WAGO I/O System 750 XTR dopuszcza się następujące pozycje montażu:

- zasadnicza pozycja montażu (poziomo od lewej)
- pozycja montażu na dole
- pozycja montażu w pionie od góry
- pozycja montażu w pionie od dołu

Nominal mounting position (horizontal left)



Floor mounting position



Vertical top mounting position



Vertical bottom mounting position



Ilustracja 23: Pozycje montażu

Wskazówka



Przy montażu pionowym używać blokady końcowej!

W przypadku „pozycji montażu w pionie u góry” oraz „pozycji montażu w pionie u dołu” pod węzłem sieciowym zamontować dodatkowo blokadę końcową, aby zabezpieczyć węzeł sieciowy przed ześlizgnięciem się.

nr katalogowy WAGO 249-116	blokada końcowa na TS 35, szer. 6 mm
nr katalogowy WAGO 249-117	blokada końcowa na TS 35, szer. 10 mm
nr katalogowy WAGO 249-197	blokada końcowa na TS 35, szer. 14 mm; wzmocniona

6.2 Konstrukcja

Maksymalna długość węzła sieciowego bez interfejsu sieciowego/sterownika wynosi 780 mm wraz z modułem końcowym. Szerokość modułu końcowego to 12 mm; pozostałe moduły I/O są więc rozmieszczone na długości maksymalnie 768 mm.

Przykłady:

- Do jednego interfejsu sieciowego/sterownika można dołączyć 64 moduły wejść i wyjść o szerokości 12 mm.
- Do jednego interfejsu sieciowego/sterownika można dołączyć 32 moduły wejść i wyjść o szerokości 24 mm.

Wyjątek:

Liczba podłączonych modułów I/O zależy poza tym od typu interfejsu sieciowego/sterownika, który został zastosowany. I tak na przykład maksymalna liczba modułów I/O, jakie można podłączyć do interfejsu sieciowego/sterownika PROFIBUS DP/V1 to 63 moduły I/O bez pasywnych modułów I/O i modułu końcowego.

UWAGA



Przestrzegać maksymalnej długości węzła sieciowego!

Maksymalna długość węzła bez interfejsu/sterownika sieciowego nie może przekroczyć długości 780 mm.

Przestrzegać także ograniczeń dla poszczególnych interfejsów/sterowników sieciowych.

6.3 Montaż na szynie

6.3.1 Właściwości szyny montażowej

Wszystkie komponenty systemu można zamontować bezpośrednio na szynie zgodnie z EN 60175 (TS 35, DIN Rail 35).

UWAGA



Nie stosować szyn nie pochodzących od WAGO bez zezwolenia!

WAGO dostarcza znormalizowane szyny montażowe, przeznaczone do zastosowania z WAGO I/O System. W przypadku stosowania innych szyn należy skontaktować się z WAGO GmbH & Co. KG w celu przeprowadzenia badania technicznego i uzyskania stosownego zezwolenia.

Szyny montażowe mają różne właściwości mechaniczne i elektryczne. W celu optymalnej zabudowy systemu na szynie należy przestrzegać następujących warunków:

- Materiał musi być odporny na korozję.

- Większość komponentów wyposażonych jest w przewodzącą stopkę połączoną z szyną montażową, służącą do odprowadzania wpływów elektromagnetycznych. W celu uniknięcia korozji ten ocynowany styk szyny nie może tworzyć z szyną ogniwa galwanicznego, wytwarzającego różnicę napięć przekraczającą 0,5 V (roztwór soli kuchennej 0,3% w temperaturze 20°C).
- Szyna musi być optymalnie kompatybilna ze zintegrowanymi w systemie środkami EMC oraz ekranowaniem przez styki modułu I/O.
- Należy wybrać szynę o wystarczającej stabilności i ew. zastosować kilka punktów montażowych (co 20 cm), aby uniknąć wygięcia lub obrócenia się szyny.
- W celu zagwarantowania bezpiecznego osadzenia komponentów nie wolno zmieniać geometrii szyny. W szczególności przy skracaniu i montażu nie wolno ścisnąć ani wyginać szyny.
- Podczas montażu komponentów stopka zatrzaskowa zahacza profil szyny. W przypadku szyn o wysokości 7,5 mm punkty montażowe (złącza śrubowe) pod węzłem należy zagłębić w szynie (wkręty z łbem wpuszczanym lub nity zamykane jednostronnie).
- Metalowe sprężyny znajdujące się na dole obudowy muszą mieć niskoomowy styk z szyną (jak największa powierzchnia styku).

6.3.2 Szyny montażowe WAGO

Szyny montażowe WAGO spełniają wymagania elektryczne i mechaniczne.

Tabela 42: Szyny montażowe WAGO

Nr katalogowy	Opis
210-112 /-113	35 × 7,5; 1 mm stal chromowana na niebiesko; z perforacją lub bez
210-197 /-114	35 × 15; 1,5 mm stal chromowana na niebiesko; z perforacją lub bez
210-118	35 × 15; 2,3 mm stal chromowana na niebiesko; bez perforacji
210-198	35 × 15; 2,3 mm miedź; bez perforacji
210-196	35 × 8,2; 1,6 mm aluminium, bez perforacji

Przy obciążeniach wibracjami > 4g należy przestrzegać następujących wskazówek montażowych:

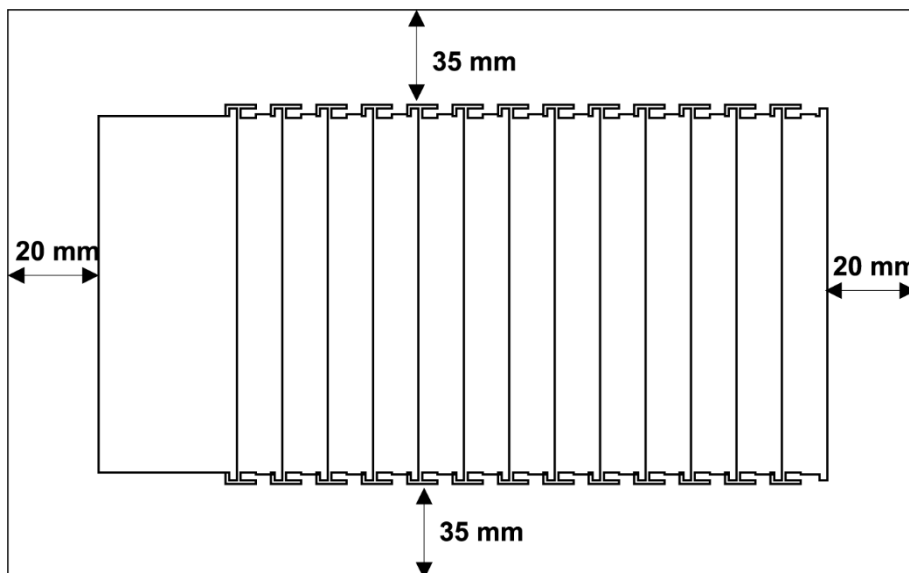
- Szynę montażową należy zamocować za pomocą śrub z łbem kulistym lub nitów, umieszczonych co najmniej co 60 mm, z uwzględnieniem 12-milimetrowego rastra (odpowiadającego szerokości modułu).
- Długość przewodu między miejscem mechanicznego mocowania przewodu i miejscem podłączenia przewodu powinna być jak najkrótsza.
- W celu stabilizacji należy zastosować blokadę końcową 249-197.
- Przy zastosowaniu PFC200 750-8202/040-00x należy użyć szyn montażowych nieperforowanych. Alternatywnie można zastosować wzmocnienia w odstępach co najmniej 1,5 mm.
- Przy zastosowaniu PFC200 750-8206/040-00x i 750-821x/040-010 należy użyć szyn montażowych nieperforowanych ze wzmocnieniami w odstępach co najmniej 2,3 mm.

Tabela 43: Szyny montażowe WAGO dopuszczone do zastosowania z XTR PFC200 przy obciążeniu wibracjami >4g

Nr katalogowy	750-8202/040-00x	750-8206/040-00x	750-821x/040-010
210-113	x	—	—
210-114	x	—	—
210-197	x	—	—
210-118	x	x	x

6.4 Odstępy

W całym węźle sieciowym należy przestrzegać odstępów od sąsiadujących ze sobą komponentów, kanałów kablowych oraz ścianek obudowy/ramy.



Ilustracja 24: Odstępy

Odstępy stwarzają przestrzeń potrzebną na odprowadzanie ciepła i montaż lub oprzewodowanie. Odstępy od kanałów kablowych ograniczają zakłócenia elektromagnetyczne ze strony przewodów.

OSTRZEŻENIE Minimalne odstępów zgodnie z IEC 60079-14!



Należy przestrzegać zalecanych minimalnych odstępów między obwodami iskrobezpiecznymi i nieiskrobezpiecznymi zgodnie z IEC 60079-14.

6.5 Kolejność montażu

Interfejsy sieciowe, sterowniki oraz moduły I/O WAGO I/O System 750 montuje się zatraskowo bezpośrednio na szynie zgodnie z EN 60175 (TS 35).

Pewny montaż i połączenie uzyskuje się dzięki zastosowaniu systemu pióro-wpust. Automatyczna blokada zapewnia stabilne mocowanie na szynie.

Zaczynając od interfejsu sieciowego/sterownika dołącza się jeden po drugim moduły I/O zgodnie z projektem. Błędy w projektowaniu węzła dotyczące grup potencjałów (połączenia przez styki magistrali obiektowej) są łatwe do rozpoznania dzięki mechanicznej blokadzie, uniemożliwiającej dołączanie modułów I/O o większej liczbie styków zasilania obiektowego za modułami I/O z mniejszą ich liczbą (wspomniana blokada jest skuteczna wyłącznie w przypadku, gdy moduły I/O łączone są jeden za drugim od interfejsu / sterownika).

OSTRZEŻENIE Ryzyko zranienia stykami nożowymi z ostrymi krawędziami!



Ponieważ styki nożowe mają bardzo ostre krawędzie, istnieje ryzyko zranienia w przypadku nieostrożnej obsługi modułów I/O. Nie należy dotykać styków nożowych.

UWAGA



Moduły I/O montować na szynie wyłącznie w zalecanej kolejności!

Wszystkie moduły I/O wyposażone są po prawej stronie we wpusty na styki nożowe. W niektórych modułach I/O wpusty te są zamknięte od góry. W ich przypadku nie ma możliwości wetknięcia od góry tych modułów I/O, które po lewej stronie mają w tym miejscu styki nożowe. To mechaniczne kodowanie pozwala zapobiec błędom, których efektem może być zniszczenie komponentów. Dlatego moduły I/O należy wtykać wyłącznie od prawej strony i od góry.

Wskazówka



Pamiętać o zakończeniu magistrali!

Na końcu węzła sieciowego należy zawsze stosować moduł końcowy 750-600/040-00x! Moduł końcowy musi być stosowany we wszystkich węzłach z interfejsami/sterownikami sieciowymi WAGO-I/O-SYSTEM 750 XTR w celu zagwarantowania prawidłowej transmisji danych!

Wskazówka



Zwiększona odporność na zakłócenia!

Eksploatacja modułów I/O XTR w zgodzie z normami obowiązującymi w aplikacjach energetycznych, kolejowych, morskich lub wykorzystujących komunikację radiową wymaga zastosowania filtra magistrali obiektowej 750-624/040-001 lub filtra magistrali obiektowej/systemowej 750-626/040-000.

Wskazówka



Konfiguracja mieszana

Konfiguracja mieszana (standardowe moduły I/O i moduły XTR) w jednym węźle jest możliwa wtedy, gdy grupy modułów I/O są odseparowane galwanicznie od strony obiektowej, czyli są zasilane z separacją galwaniczną.

6.6 Montaż urządzeń

NIEBEZPIECZEŃSTWO



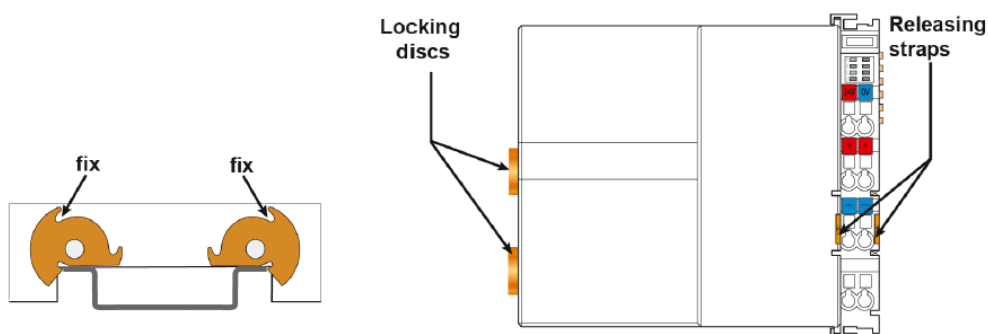
Nie pracować przy urządzeniach znajdujących się pod napięciem!

Niebezpieczne napięcie elektryczne może spowodować porażenie prądem elektrycznym i oparzenia. Przed rozpoczęciem montażu, instalacji, usuwania usterek lub prac konserwacyjnych należy zawsze odłączać urządzenie od zasilania.

6.6.1 Montaż sterownika

1. Przy wymianie zamontowanego już sterownika ustawić nowy sterownik w taki sposób, aby przez pióro i wpust był on połączony z kolejnym modułem I/O.
2. Zamontować zatrzaskowo sterownik na szynie.
3. Przekręcić obie blokady ryglujące ostrzem śrubokręta do momentu, aż zahaczą o szynę montażową (patrz następna ilustracja). W ten sposób sterownik zostaje zabezpieczony przed przechyleniem się na szynie.

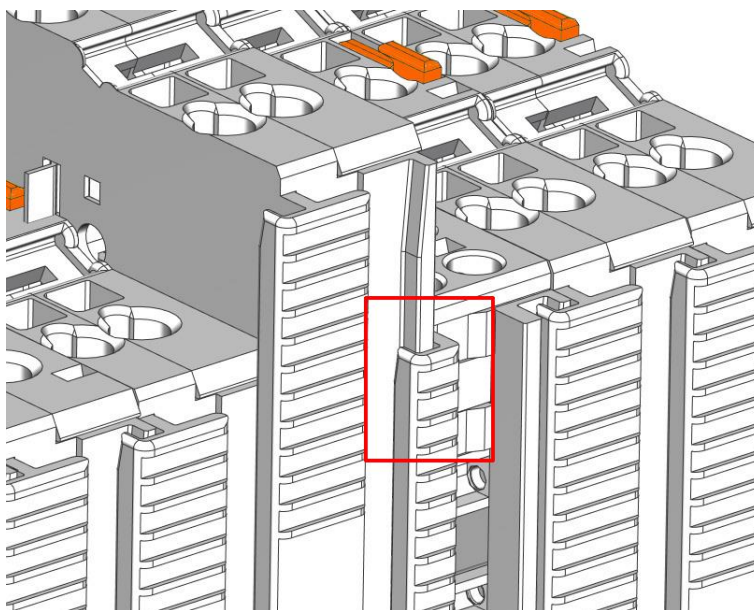
W momencie zatrzaskowego montażu sterownika zapewnione zostają połączenia elektryczne styków magistrali systemowej i styków magistrali obiektowej (o ile są dostępne) z kolejnym modułem I/O.



Ilustracja 25: Blokada montażowa sterownika

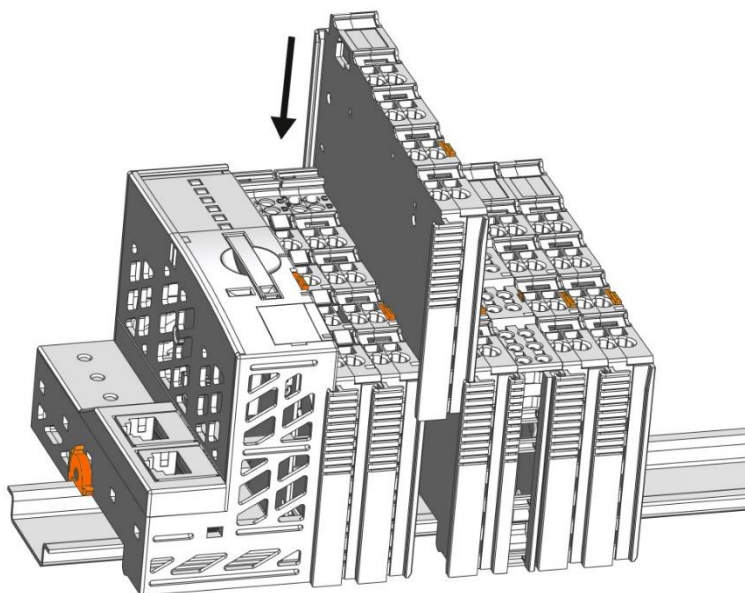
6.6.2 Dodawanie modułów I/O

1. Moduł I/O umieść w takiej pozycji, aby przez wpust i pióro był połączony z poprzednim i ewentualnie następnym komponentem.



Ilustracja 26: Wkładanie modułu I/O (przykład)

2. Wcisnąć moduł I/O do węzła, aż zatrzaśnie się na szynie.



Ilustracja 27: Montaż zatraskowy modułu I/O (przykład)

3. Sprawdzić, czy moduł I/O jest stabilnie zamocowany na szynie i w węźle. Moduł I/O nie może być ustawiony krzywo lub pod kątem.

W momencie zatraskowego montażu modułu I/O zapewnione zostają połączenia elektryczne styków magistrali systemowej i obiektowej (o ile są dostępne) z jednostką główną lub z poprzednim i ewentualnie kolejnym modułem I/O.

7 Podłączanie urządzeń

7.1 Styki magistrali obiektowej / zasilanie sieci obiektowej

OSTRZEŻENIE Ryzyko zranienia stykami nożowymi z ostrymi krawędziami!



Ponieważ styki nożowe mają bardzo ostre krawędzie, istnieje ryzyko zranienia w przypadku nieostrożnej obsługi modułów I/O. Nie należy dotykać styków nożowych.

Po prawej stronie większości interfejsów sieciowych/sterowników i niektórych modułów I/O umieszczone są tak zwane styki mocy.

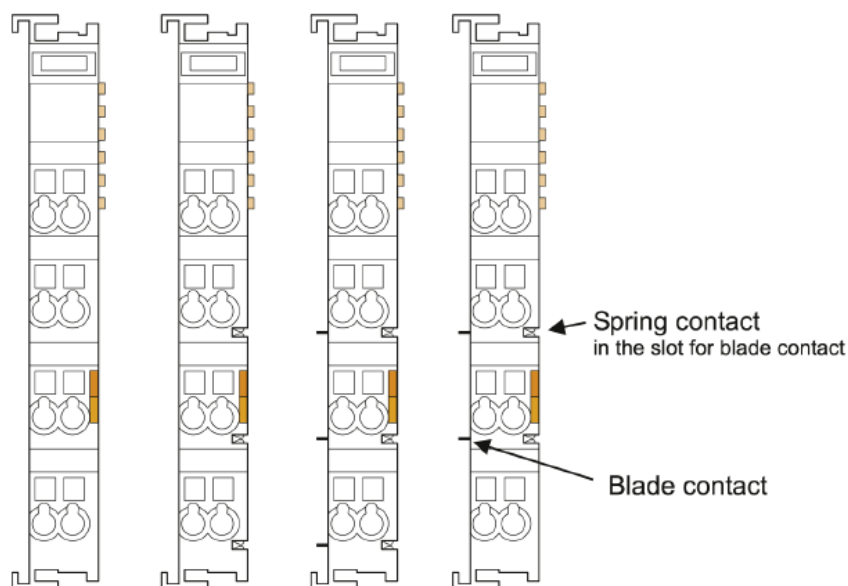
Styki mocy łączą potencjały zasilające magistrali obiektowej.

Są to styki sprężynowe, chronione przed dotykiem bezpośrednim.

Po lewej stronie modułów I/O umieszczone są odpowiednie styki nożowe.

Power jumper contacts

Blade	0	0	3	2
Spring	0	3	3	2



Ilustracja 28: Przykłady rozmieszczenia styków mocy

7.2 Podłączanie przewodów do CAGE CLAMP®

Zaciski CAGE CLAMP® WAGO są przeznaczone do podłączania przewodów jedno-, wielodrutowych i linkowych.

UWAGA



Dostosować przekroje przewodów do obciążenia!

Prąd zasilający może wynosić maksymalnie 10 A. Przekroje przewodów muszą być wystarczające dla maksymalnego obciążenia prądowego wszystkich zasilanych modułów I/O.

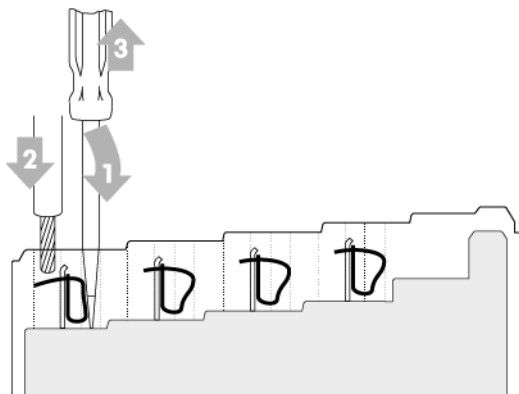
Wskazówka



Do każdego zacisku CAGE CLAMP® podłączać tylko jeden przewód!

Należy podłączać tylko jeden przewód do każdego zacisku CAGE CLAMP®. Niedozwolone jest podłączanie kilku przewodów do jednego zacisku.

W przypadku gdy wymagane jest podłączenie kilku przewodów, należy dokonać rozdzielenia potencjału na zewnątrz (np. za pomocą złączek przełotowych WAGO).



Ilustracja 29: Podłączanie przewodów do CAGE CLAMP®

1. W celu otwarcia zacisku CAGE CLAMP® wprowadzić przyrząd montażowy do otworu powyżej zacisku.
2. Wprowadzić przewód do odpowiedniego otworu zacisku.
3. Aby zamknąć zacisk CAGE CLAMP®, wyjąć przyrząd montażowy. W ten sposób przewód zostaje zamocowany.

7.3 Koncepcja zasilania

Magistrala obiektowa i systemowa muszą być zasilane przez zasilacze SELV/PELV.

OSTRZEŻENIE **Możliwe zagrożenie pożarowe na skutek niedostatecznej ochrony przed przetężeniem!**



W razie awarii niedostateczna ochrona przed przetężeniem może grozić pożarem. Zbyt duży przepływ prądu w komponentach może w razie awarii prowadzić do silnego przegrzania, dlatego środki ochrony przed przetężeniem należy zawsze dostosować do oczekiwanej wydajności.

Zasilanie magistrali systemowej i obiektowej w ramach WAGO I/O System 750 realizowane jest przez jednostki główne i moduły zasilające.

W przypadku komponentów pracujących na niskich napięciach można stosować tylko źródła napięcia SELV/PELV.

Jeśli kilka komponentów zasilanych jest z jednego źródła. Powinno ono, stosownie do zastosowanych komponentów, uwzględniać wymogi dotyczące bezpieczeństwa urządzeń elektrycznych. W przypadku komponentów, które mogą być zasilane tylko ze źródeł SELV, wymagania te są wymienione w parametrach technicznych.

Większość komponentów WAGO I/O System 750 XTR nie ma wewnętrznej ochrony przed przeciążeniem. Dlatego dla każdego źródła zasilającego te komponenty należy zastosować zewnętrzne środki ochrony przed przetężeniem, na przykład za pomocą bezpiecznika.

Maksymalny dopuszczalny prąd podano w parametrach technicznych urządzeń.

Do zasilania magistrali obiektowej napięciem 230 V wymagany jest tylko moduł zasilający 750-612/040-000 dla tej grupy potencjałowej.

UWAGA



Zasilanie systemowe tylko z odpowiednim bezpiecznikiem!

Przy braku ochrony przed przetężeniem komponenty elektroniczne mogą zostać uszkodzone.

Stosując bezpiecznik do zabezpieczenia zasilania systemowego przed przepięciem, należy wybrać wariant zwłoczny maks. 2 A.

UWAGA



Zasilanie obiektowe tylko z odpowiednim bezpiecznikiem!

Przy braku ochrony przed przetężeniem komponenty elektroniczne mogą zostać uszkodzone.

Stosując zewnętrzny bezpiecznik do zabezpieczenia zasilania magistrali obiektowej przed przepięciem, należy wybrać wariant 10 A.

7.3.1 Dodatkowe przepisy dotyczące zasilania

WAGO-I/O-SYSTEM 750 XTR może być stosowany także w przemyśle stoczniowym i innych aplikacjach morskich (np. w infrastrukturze przybrzeżnej lub na platformach wiertniczych), jak również w systemach telecontrol. Spełnia szczególne wymagania towarzystw okrętowych jak np. Germanischer Lloyd i Lloyds Register, co zostało potwierdzone licznymi certyfikatami.

Eksplatacja modułów I/O XTR zgodnie z normami obowiązującymi w aplikacjach energetycznych, kolejowych, morskich lub wykorzystujących telecontrol wymaga zastosowania filtra (przeciwprzepięciowego) magistrali obiektowej 750-624/040-00x lub filtra magistrali obiektowej/systemowej 750-626/040-000.

Tabela 44: Filtry zasilania 24 V

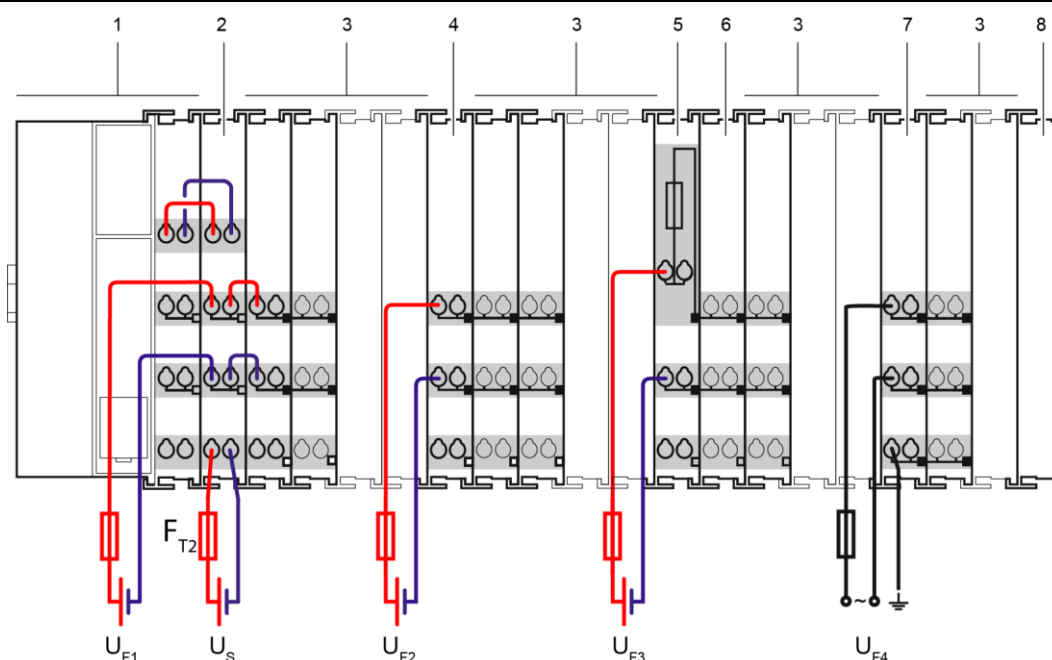
Nr kat.	Nazwa	Opis
750-626/040-000	Filtr zasilania 24 V DC HI XTR	Filtr magistrali obiektowej/systemowej; 24 V DC; podwyższona izolacyjność; XTR.: zasilanie systemowe i obiektowe z filtrem (24 V, 0 V), tzn. dla interfejsu sieciowego/sterownika i dla zasilania systemowego (750-613/040-000)
750-624/040-000	Filtr magistrali obiektowej 24 V DC HI XTR	Filtr (przeciwprzepięciowy) magistrali obiektowej, 24 V DC, podwyższona izolacyjność; XTR: zasilanie obiektowe z filtrem
750-624/040-001	Filtr magistrali obiektowej; 24 V DC; HI; NC; XTR	Filtr (przeciwprzepięciowy) magistrali obiektowej; 24 V DC; podwyższona izolacyjność; bez styków mocy; XTR: zasilanie obiektowe z filtrem

Ponadto należy koniecznie przestrzegać poniższej koncepcji zasilania.

Napięcie zasilania systemowego 24 V interfejsu/sterownika sieciowego musi być przefiltrowane i zabezpieczone przed wystąpieniem przepięć. Zasilanie może być realizowane wyłącznie poprzez filtr magistrali obiektowej/systemowej 750-626/040-000.

Zasilanie urządzeń elektronicznych może być podłączane tylko przez bezpiecznik 2 A, zwłoczny.

Napięcie magistrali obiektowej 24 V również musi być zabezpieczone przed wystąpieniem przepięć. Zasilanie może być realizowane przy użyciu filtra (przeciwprzepięciowego) magistrali obiektowej 750-624/040-00x lub filtra magistrali obiektowej/systemowej 750-626/040-000.



Ilustracja 30: Koncepcja zasilania

Tabela 45: Opis ilustracji „Koncepcja zasilania“

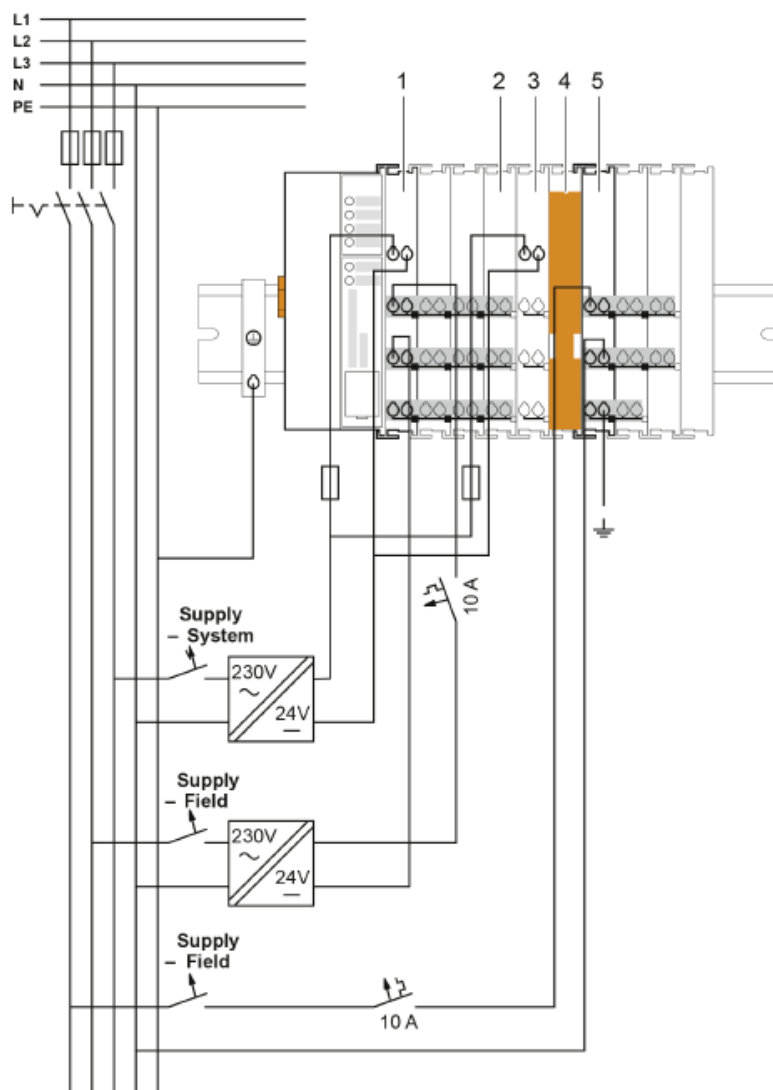
Poz.	Znaczenie
1	Interfejs/sterownik sieciowy XTR
2	Filtr zasilania; 24 V DC; podwyższona izolacyjność; XTR (750-626/040-000)
3	Moduły I/O XTR
4	Filtr (przeciwprzepięciowy) magistrali obiektowej; 24 V DC; podwyższona izolacyjność; bez styków mocy; XTR (750-624/040-001)
5	Moduł zasilający bezpiecznikowy; 24 V DC; podstawka bezpiecznika; XTR (750-601/040-000 lub 750-610/040-000)
6	Filtr (przeciwprzepięciowy) magistrali obiektowej; 24 V DC; podwyższona izolacyjność; XTR (750-624/040-000)
7	Moduł zasilający; AC/DC 0 ... 230 V; XTR (750-612/040-000)
8	Moduł końcowy XTR (750-600/040-00x)
Grupy potencjałów	
U _{F1}	Zasilanie obiektowe 1 (24 V DC)
U _S	Zasilanie magistrali systemowej (24 V DC)
U _{F2}	Zasilanie obiektowe 2 (24 V DC)
U _{F3}	Zasilanie obiektowe 3 (24 V DC)
U _{F4}	Zasilanie obiektowe 4 (230 V DC)

7.3.2 Przykład zasilania

Wskazówka Magistralę systemową i magistralę obiektową zasilать z odrębnych obwodów!



Rozdzielenie zasilania obu magistral pozwala na niezakłóconą pracę węzła w przypadku zwarcia po stronie elementów wykonawczych.



Ilustracja 31: Przykład zasilania dla interfejsów/sterowników sieciowych XTR

Tabela 46: Opis ilustracji „Przykład zasilania”

Poz.	Opis
1	Zasilanie magistrali obiektowej przy interfejsie sieciowym/sterowniku przez zewnętrzny moduł zasilający
2	Moduł zasilający 24 V
3	Moduł zasilający z zasilaniem magistrali systemowej 24 V
4	Zalecany moduł dystansowy
5	Moduł zasilający 230 V

7.3.3 Zasilacze

WAGO I/O System 750 XTR wymaga do zasilania magistrali systemowej napięcia stałego 24 V.

Wskazówka



Zalecenie

Nie wszędzie i nie zawsze zasilanie sieciowe będzie stabilne. Dlatego w celu zagwarantowania jakości napięcia zasilającego należy używać standardowych zasilaczy, zgodnych z normami.

Wskazówka



Dla zasilania systemowego zastosować zewnętrzne buforowanie!

W celu zabezpieczenia na wypadek awarii zasilania, zasilanie magistrali systemowej musi być buforowane. Ponieważ zapotrzebowanie na prąd zależy od węzła sieciowego, buforowanie nie zostało zaimplementowane w urządzeniu.

Aby uzyskać czas awarii zasilania zgodny z IEC 61131-2 (1 ms lub 10 ms), należy obliczyć buforowanie odpowiednie dla danego węzła sieciowego, a następnie dołożyć zewnętrznie urządzenie zasilające.

Dla każdego punktu zasilania magistrali obiektowej należy indywidualnie obliczać zapotrzebowanie na prąd. Należy przy tym uwzględnić wszystkie urządzenia obiektowe i moduły I/O. Zasilanie magistrali obiektowej może mieć również wpływ na moduły I/O, ponieważ stopnie wejściowe i wyjściowe niektórych modułów I/O wymagają zasilania magistrali obiektowej.

Wskazówka



Magistralę systemową i magistralę obiektową zasiląć z odrębnych obwodów!

Rozdzielenie zasilania obu magistral pozwala na niezakłóconą pracę węzła w przypadku zwarcia po stronie elementów wykonawczych.

Informacja



Zasilacze są dostępne w eShopie.

Odpowiednie zasilacze, np. z serii EPSITRON, można znaleźć w eShopie www.wago.com.

7.4 Uziemienie

7.4.1 Uziemienie szyny montażowej

7.4.1.1 Zabudowa na ramie

W przypadku zabudowy na ramie szyna montażowa musi być połączona śrubami z ramą szafy lub obudową przewodzącą prąd. Rama lub obudowa muszą być uziemione. Połączenie elektryczne realizowane jest za pośrednictwem złącza śrubowego. Tym samym szyna montażowa jest uziemiona.

NIEBEZPIECZEŃSTWO Należy zapewnić wystarczające uziemienie!



Należy zapewnić odpowiednie połączenie elektryczne pomiędzy szyną nośną a ramą lub obudową w celu zagwarantowania wystarczających parametrów uziemienia.

7.4.1.2 Budowa izolowana

Budowa izolowana polega na tym, że nie istnieje połączenie pomiędzy konstrukcją szafy a szyną montażową. Odpowiednie uziemienie, zgodnie z krajowymi przepisami, musi zostać zapewnione za pomocą przewodu elektrycznego.

Wskazówka Zalecenie



Optymalna konstrukcja to metalowa, uziemiona płyta montażowa, połączona z szyną montażową połączeniem przewodzącym elektrycznie.

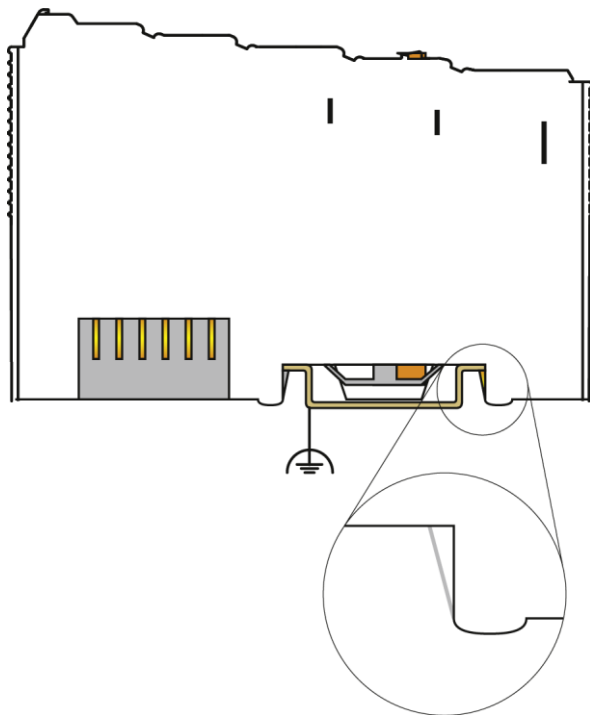
Osobne uziemienie szyny montażowej można łatwo wykonać przy użyciu złączek PE WAGO.

Tabela 47: Złączki PE WAGO

Nr katalogowy	Opis
283-609	1-przewodowa złączka PE łączy przewód ochronny bezpośrednio z szyną montażową; przekrój przewodu: 0,2 mm ² ... 16 mm ² Wskazówka: należy zamówić także ściankę końcową (283-320)

7.4.2 Uziemienie funkcjonalne

Uziemienie funkcjonalne zwiększa odporność na zakłócenia elektromagnetyczne. Niektóre komponenty systemu I/O posiadają specjalny styk uziemiający, odprowadzający zakłócenia elektromagnetyczne do szyny montażowej.



Ilustracja 32: Styk uziemiający (przykład)

Dolne zaciski CAGE CLAMP® modułów zasilających mogą służyć opcjonalnie do podłączenia uziemienia funkcjonalnego po stronie obiektowej. Potencjał ten jest udostępniany modułowi I/O umieszczonemu po prawej stronie przez dolny styk sprężynowy w formie trzech styków magistrali obiektowej. Niektóre moduły I/O wyposażone są w styk nożowy, który może odprowadzić ten potencjał. W ten sposób z modułów I/O umieszczonych po lewej stronie tworzy się grupę potencjałową pod kątem uziemienia funkcjonalnego.

7.5 Ekranowanie

7.5.1 Informacje ogólne

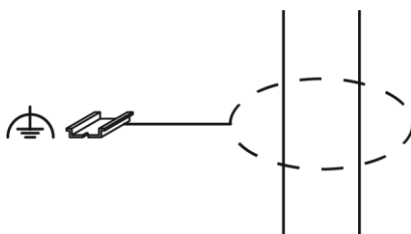
Zastosowanie ekranowanych przewodów zmniejsza negatywny wpływ zakłóceń elektromagnetycznych i polepsza jakość sygnału. Pozwala uniknąć błędów pomiarowych oraz transmisyjnych, spowodowanych między innymi przepięciami.

Wskazówka



Ekran przewodu łączyć z potencjałem uziemienia!

Kompleksowe uziemienie jest konieczne w celu zagwarantowania właściwości technicznych w zakresie dokładności pomiaru. Połączenie ekranu przewodu z potencjałem uziemienia należy wykonywać w miejscu wprowadzenia przewodu do szafy rozdzielczej lub obudowy. W ten sposób zakłócenia rozproszone są odprowadzane i utrzymywane z dala od urządzeń znajdujących się w środku.



Ilustracja 33: Ekran przewodu z potencjałem uziemienia

Wskazówka



Polepszenie ekranowania przez duże powierzchnie styku!

Polepszenie ekranowania można uzyskać, jeżeli połączenie między ekranem a potencjałem uziemienia będzie niskoomowe. W tym celu należy zapewnić dużą powierzchnię styku, np. przez zastosowanie systemu łączenia ekranów WAGO. Jest to zalecane w szczególności w rozległych instalacjach, w których mogą występować prądy wyrównawcze oraz wysokie prądy impulsowe (np. powodowane wyładowaniami atmosferycznymi).

Wskazówka



Chronić przewody danych i sygnałowe przed źródłami zakłóceń!

Przewody danych i sygnałowe należy oddzielać od wszystkich przewodów silnoprądowych i innych źródeł wysokiej emisji elektromagnetycznej (np. przetwornic częstotliwości lub napędów).

7.5.2 Przewody sieci obiektowej

Ekranowanie przewodów sieci obiektowej jest opisane w dyrektywach dotyczących budowy i normach dla poszczególnych systemów sieciowych. Informacje na ten temat może dostarczyć właściwa organizacja specjalizująca się w danej sieci obiektowej lub literatura fachowa.

7.5.3 Ekranowane przewody sygnałowe

Wskazówka



Należy stosować ekranowane przewody sygnałowe!

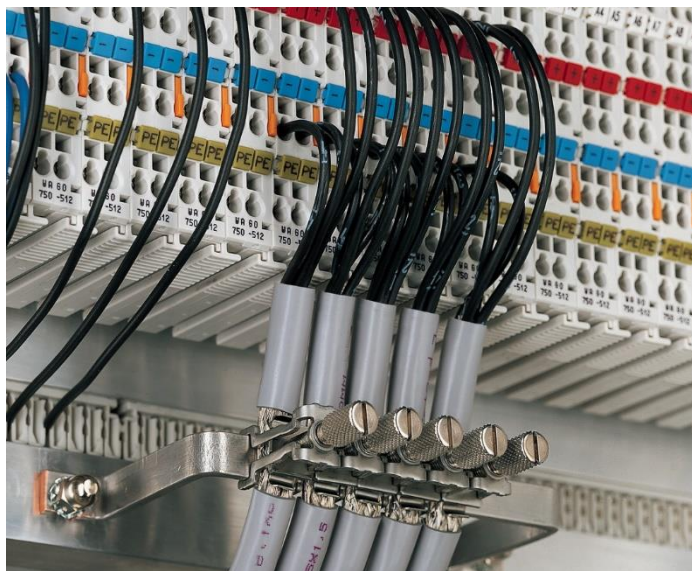
Dla sygnałów analogowych oraz magistralnych, podłączanych do urządzeń wyposażonych w zaciski do podłączania ekranu, należy stosować wyłącznie przewody ekranowane. Tylko w ten sposób można zagwarantować, że dla danego urządzenia zostanie osiągnięty wymagany stopień dokładności również w przypadku zaistnienia zakłóceń działających na przewód sygnałowy.

7.5.4 System łączenia ekranów

W ramach systemu łączenia ekranów WAGO (seria 790) dostępne są obejmy zaciskowe, szyny zbiorcze i różnego typu stopki montażowe. Przy użyciu tych części można wykonywać różne konstrukcje.



Ilustracja 34: Obejmy do ekranów na szynie montażowej (przykład)



Ilustracja 35: 5 obejm do ekranów na szynie zbiorczej (przykład)

8 Uruchamianie

8.1 Włączanie sterownika

Przed włączeniem sterownika należy upewnić się, że:

- sterownik został prawidłowo zamontowany (patrz rozdział „Montaż“),
- wszystkie potrzebne przewody do transmisji danych (patrz rozdział „Złącza“) są podłączone do odpowiednich interfejsów, a ich złącza wtykowe (jeśli takie istnieją) są zamocowane za pomocą śrub,
- zasilanie elektroniki i magistrali obiektowej jest podłączone (patrz rozdział „Złącza“),
- został zamontowany moduł końcowy (750-600) (patrz rozdział „Montaż“),
- zostało zapewnione wyrównanie potencjałów (patrz opis systemu 750-xxx) oraz
- wykonane jest poprawne ekranowanie (patrz opis systemu 750-xxx).

Aby włączyć sterownik oraz podłączone do niego moduły I/O, należy włączyć na zasilaczu napięcie zasilania.

Start sterownika sygnalizowany jest krótkim rozbłyskiem na pomarańczowo wszystkich wskaźników LED. Po kilku sekundach wskaźniki LED SYS sygnalizują pomyślne zakończenie procesu bootowania sterownika.

Równocześnie zostaje uruchomiony system runtime CODESYS 2.3 lub **e!RUNTIME**.

Gdy system zostanie uruchomiony pomyślnie, wskaźniki LED SYS i I/O świecą na zielono.

Gdy w sterowniku zostanie zapisany i uruchomiony program IEC 61131-3, wskaźniki LED RUN świecą na zielono.

Jeśli w sterowniku nie ma zapisanego programu lub przełącznik trybu pracy jest ustawiony na STOP, zostaje to również zasygnalizowane przez LED RUN (patrz rozdział „Diagnostyka“ > ... > „Elementy sygnalizacyjne dla sieci/systemu“).

8.2 Ustalanie adresu IP hosta

Aby host mógł komunikować się ze sterownikiem przez sieć ETHERNET, oba urządzenia muszą znajdować się w tej samej sieci.

W celu ustalenia adresu IP hosta (z systemem operacyjnym Microsoft Windows®) przy użyciu okna poleceń należy postępować w następujący sposób:

1. Otworzyć okno poleceń.
W polu edycji wybrać **Start > Execute... > Open:** (Windows® XP) lub **Search programs/files** (Windows® 7) i wpisać polecenie „cmd” a następnie potwierdzić przyciskiem **[OK]** lub **[Enter]**.
2. Wpisać polecenie „ipconfig” i potwierdzić przyciskiem **[Enter]**.
3. Pojawią się adres IP, maska podsieci i standardowa brama z przynależnymi parametrami.

8.3 Ustawianie adresu IP

W ustawieniach fabrycznych sterownika dla interfejsu ETHERNET (port X1 i port X2) aktywne jest następujące adresowanie IP:

Tabela 48: Fabryczne ustawienie dla adresowania IP interfejsu ETHERNET

Interfejs ETHERNET	Ustawienie fabryczne
X1/X2 (Switched Mode)	Dynamiczne nadawanie adresu IP za pomocą DHCP (Dynamic Host Configuration Protocol)

Aby PC i sterownik mogły się komunikować ze sobą, należy za pomocą jednego z narzędzi do konfiguracji (WBM, WAGO Ethernet Settings, CBM) dopasować adresowanie IP do struktury systemu (patrz rozdział „Konfiguracja”).

Przykład integracji sterownika (192.168.1.17) w istniejącej sieci:

- Adres IP hosta to **192.168.1.2**.
- Sterownik i host muszą znajdować się w tej samej podsieci (niezależnie od adresu IP hosta).
- Aby oba znajdowały się w tej samej podsieci, pierwsze trzy miejsca adresu IP hosta i sterownika przy masce podsieci **255.255.255.0** muszą być zgodne.

Tabela 49: Maska sieci 255.255.255.0

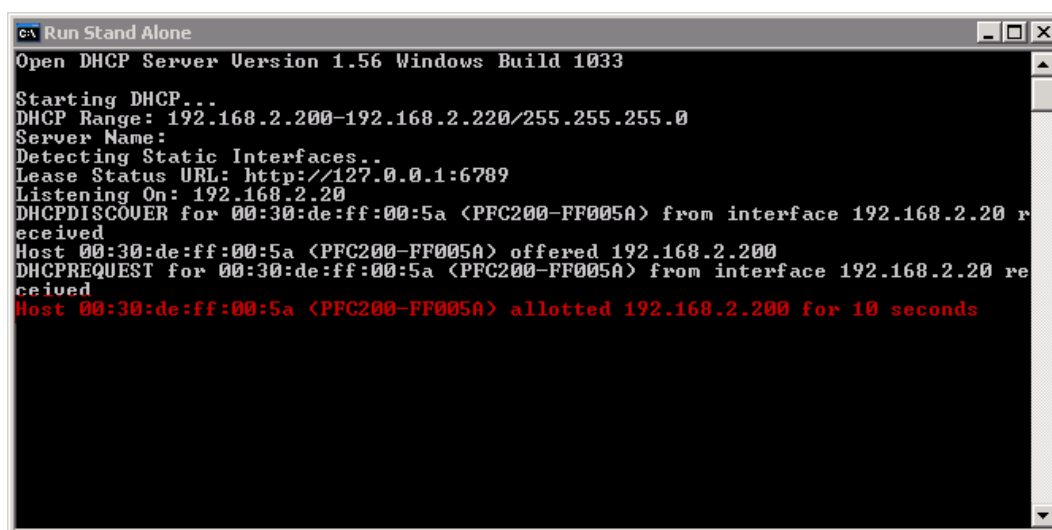
Host PC	Przestrzeń adresowa dla sterownika
192.168.1.2	192.168.1.1 lub 192.168.1.3 ... 192.168.1.254

8.3.1 Przydzielanie adresu IP za pomocą DHCP

Sterownik sam może dynamicznie (DHCP/BootP) pobierać adresy IP z serwera. W przeciwieństwie do stałych adresów IP, adresy przydzielone dynamicznie nie są zapisywane. Dlatego przy każdym restarcie sterownika konieczna jest obecność serwera BootP lub DHCP.

Jeśli adres IP został nadany przez DHCP (ustawienie standardowe), można go ustalić za pomocą ustawień lub informacji z serwera DHCP.

Przykładowa ilustracja przedstawia „Open DHCP”.



```
Run Stand Alone
Open DHCP Server Version 1.56 Windows Build 1033

Starting DHCP...
DHCP Range: 192.168.2.200-192.168.2.220/255.255.255.0
Server Name:
Detecting Static Interfaces..
Lease Status URL: http://127.0.0.1:6789
Listening On: 192.168.2.20
DHCPDISCOVER for 00:30:de:ff:00:5a <PFC200-FF005A> from interface 192.168.2.20 received
Host 00:30:de:ff:00:5a <PFC200-FF005A> offered 192.168.2.200
DHCPREQUEST for 00:30:de:ff:00:5a <PFC200-FF005A> from interface 192.168.2.20 received
Host 00:30:de:ff:00:5a <PFC200-FF005A> allotted 192.168.2.200 for 10 seconds
```

Ilustracja 36: „Open DHCP, przykład widoku”

W połączeniu z serwerem DNC podłączonym do DHCP możliwe jest uzyskanie dostępu do urządzenia przez nazwę hosta.

Składa się ona z przedrostka „PFCx00-” i ostatnich 6 miejsc adresu MAC (w przykładzie są to: „00:30:DE:FF:00:5A”). Adres MAC urządzenia nadrukowany jest na etykiecie umieszczonej z boku.

Nazwa hosta w prezentowanym przykładzie to „PFC200-FF005A”.

8.3.2 Zmiana adresu IP za pomocą narzędzia konfiguracyjnego „CBM” i programu terminalowego

Za pomocą narzędzia konfiguracyjnego „CBM”, dostępnego na konsoli Linux®, można przydzielać nowe adresy IP m.in. interfejsom ETHERNET X1 i X2. Więcej informacji na temat CBM zamieszczono w rozdziale „Konfiguracja”.

1. Podłączyć PC z zainstalowanym programem terminalowym (obsługującym SSH) do interfejsu ETHERNET X1 sterownika.
2. Uruchomić program terminalowy.
3. Wybrać rodzaj połączenia „SSH” i jako parametr połączenia wpisać adres IP sterownika port 22.
4. Zalogować się do systemu Linux® jako „Superuser”. Nazwę użytkownika i hasło znaleźć można w rozdziale „Użytkownicy hasła” > „Grupa Linux®-User”.
5. Otworzyć narzędzie konfiguracyjne, wpisując „cbm” w wierszu poleceń programu terminalowego (uwzględnić pisownię wielką/małą literą) i potwierdzić klawiszem **[Enter]**.

```
=====
WAGO Console Based Management Tool
=====
Main Menu
-----
0. Quit
1. Information
2. PLC Runtime
3. Networking
4. Firewall
5. Clock
6. Administration
7. Package Server
8. Mass Storage
9. Software Uploads
10. Ports and Services
11. SNMP
12. PROFIBUS DP
-----
Select an entry or Q to quit
=====
```

Ilustracja 37: Menu główne CBM (przykład)

6. W **Main Menu** za pomocą klawiatury (klawisze ze strzałkami lub klawiatura numeryczna) wybrać pozycję **Networking** i nacisnąć **[Enter]**.

```
=====
WAGO Console Based Management Tool
=====
Main Menu
-----
0. Quit
1. Information
2. PLC Runtime
3. Networking
4. Firewall
5. Clock
6. Administration
7. Package Server
8. Mass Storage
9. Software Uploads
10. Ports and Services
11. SNMP
12. PROFIBUS DP
-----
Select an entry or Q to quit
=====
```

Ilustracja 38: CBM – wybór „Networking”

7. W menu **Networking** wybrać pozycję **TCP/IP** i nacisnąć **[Enter]**.

```
=====
WAGO Console Based Management Tool
=====
Networking
-----
0. Back to Main Menu
1. Host-/Domain Name
2. TCP/IP
3. Ethernet
-----
Select an entry or Q to quit
=====
```

Ilustracja 39: CBM – wybór „TCP/IP”

8. W menu **TCP/IP** wybrać pozycję **IP Address** i nacisnąć **[Enter]**.

```
=====
WAGO Console Based Management Tool
=====
TCP/IP
-----
0. Back to Networking Menu
1. IP Address
2. Default Gateway
3. DNS Server
-----
Select an entry or Q to quit
=====
```

Ilustracja 40: CBM – wybór „IP Address”

9. W menu **TCP/IP Configuration** wybrać pozycję **IP Address** i nacisnąć **[Enter]**.

```
=====
WAGO Console Based Management Tool
=====
TCP/IP Configuration of X1
-----
0. Back to TCP/IP Menu
1. Type of IP Address Configuration...Static IP
2. IP Address.....192.168.1.18
3. Subnet Mask.....255.255.255.0
-----
Select an entry or Q to quit
-----
```

Ilustracja 41: CBM – wybór adresu IP

10. W menu **Change IP Address** wpisać nowy adres IP i potwierdzić naciskając **[OK]**. Aby powrócić bez uwzględniania zmian do głównego menu, wybrać **[Abort]**.

```
=====
WAGO Console Based Management Tool
=====
Change IP Address
-----

Enter new IP Address:
+-----+
|192.168.1.17 |
+-----+

< OK >    <Abort>

-----
OK: confirm value, Abort: quit without changes
-----
```

Ilustracja 42: CBM – wpisywanie nowego adresu IP

8.3.3 Zmiana adresu IP przy użyciu „WAGO Ethernet Settings“

Aplikacja Microsoft Windows® „WAGO Ethernet Settings“ jest oprogramowaniem umożliwiającym identyfikację sterownika i konfigurację ustawień sieci.

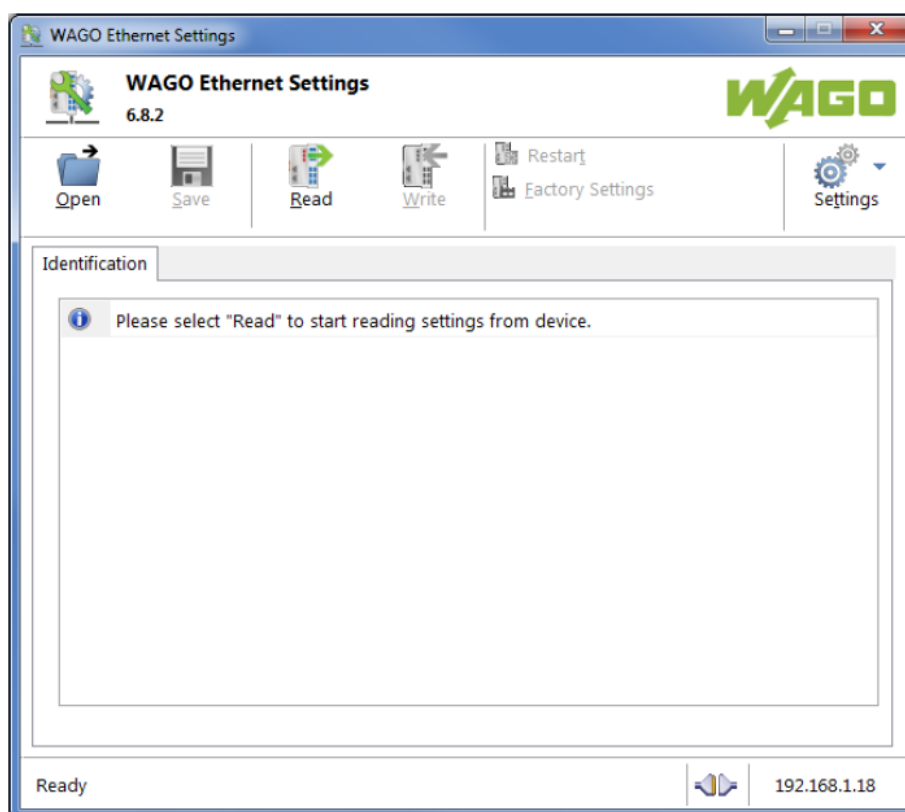
Wskazówka **Zwrócić uwagę na wersję oprogramowania!**



Przy konfiguracji sterownika należy korzystać z wersji „WAGO Ethernet Settings“ nie starszej niż 6.3.1(01)!

Do transmisji danych należy użyć przewodu konfiguracyjnego lub adaptera radiowego WAGO, bądź sieci IP.

1. Wyłączyć napięcie robocze sterownika.
2. Podłączyć przewód konfiguracyjny 750-920 do złącza serwisowego sterownika i do złącza szeregowego PC.
3. Włączyć ponownie napięcie robocze sterownika.
4. Uruchomić program „**WAGO Ethernet Settings**“.



Ilustracja 43: „WAGO Ethernet Settings“ – ekran startowy (przykład)

5. Kliknąć przycisk **[Read]**, aby wczytać i zidentyfikować podłączony sterownik.
6. Wybrać zakładkę „Network“:

Parameter	Edit	Currently used
Address Source	Static Configuration	Static Configuration
IP address	192.168.1.18	192.168.1.18
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0
Preferred DNS-Server	0.0.0.0	0.0.0.0
Alternative DNS-Server	0.0.0.0	0.0.0.0
Time Server	0.0.0.0	0.0.0.0
Hostname		PFC200-400E6F
Domain name	localdomain.lan	localdomain.lan

Interface X1

Interface X2

Run WBM

Interfaces

☐ Switched

☒ Separated

Ilustracja 44: „WAGO Ethernet Settings” – zakładka „Network”

7. W celu nadania stałego adresu w punkcie „Address Source” w kolumnie „Parametr” wybrać wartość „Static Configuration”. Standardowo aktywowany jest BootP.
8. W kolumnie „Parametr” wpisać żądany adres IP oraz adresy podsieci i bramy.
9. Kliknąć przycisk **[Write]**, aby zastosować adres w sterowniku. („WAGO Ethernet Settings” będzie za każdym razem powodował automatyczny restart sterownika. Może to potrwać ok. 30 sekund.)
10. Teraz można zamknąć „WAGO Ethernet Settings”, bądź też, w razie potrzeby, wprowadzić dalsze ustawienia bezpośrednio w systemie zarządzania przez WWW (WBM). W tym celu kliknąć **[Run WBM]** po prawej stronie okna.

8.3.4 Czasowe ustawienie stałego adresu IP

Ta procedura pozwala tymczasowo ustawić adres IP dla interfejsu X1 jako stały adres „192.168.1.17”.

Przy włączonym switchu stały adres stosowany jest także dla interfejsu X2.

Przy wyłączonym switchu pierwotne ustawienia adresu dla interfejsu X2 nie ulegają zmianie.

Nie jest przeprowadzany reset.

Aby ustawić czasowo stały adres IP, należy postępować w następujący sposób:

1. Ustawić przełącznik trybu pracy w pozycji STOP.
2. Nacisnąć przycisk Reset (RST) przez czas dłuższy niż 8 sekund.

Wykonanie jest sygnalizowane miganiem wskaźników LED „SYS” na pomarańczowo.

Aby anulować to ustawienie, należy postępować w następujący sposób:

- Wykonać reset oprogramowania lub
- Wyłączyć i ponownie włączyć sterownik.

8.4 Testowanie połączenia sieciowego

Aby sprawdzić, czy sterownik jest dostępny w sieci pod nadanym adresem IP, należy skorzystać z aplikacji „ping”:

1. Otworzyć okno poleceń.
W polu edycji wybrać **Start > Execute... > Open:** (Windows® XP) lub **Start > Search programs/files** (Windows® 7) i wpisać polecenie „cmd” a następnie potwierdzić przyciskiem **[OK]** lub **[Enter]**.
2. Wpisać polecenie „ping” i adres IP sterownika (np. `ping 192.168.1.17`), a następnie potwierdzić klawiszem **[Enter]**.

Wskazówka



Usunąć wpisy hosta tabeli ARP!

Dobrze jest przed zastosowaniem „ping” usunąć aktualne pozycje tabeli ARP dotyczące hosta za pomocą „arp -d *” (dla Windows® 7 jako administrator). W ten sposób można zagwarantować, że przedawniony wpis hosta nie spowoduje nieudanego „pingu”.

3. PC wysyła zapytanie, na które sterownik odpowiada. Odpowiedź pokazuje się w oknie poleceń. Jeśli pojawi się komunikat o błędzie „Timeout”, oznacza to, że sterownik się nie zgłosił. Należy wtedy sprawdzić ustawienia sieci.

```
C:\WINDOWS\system32\cmd.exe
U:\>ping 192.168.1.17

Ping wird ausgeführt für 192.168.1.17 mit 32 Bytes Daten:

Antwort von 192.168.1.17: Bytes=32 Zeit=1ms TTL=64
Antwort von 192.168.1.17: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.1.17: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.1.17: Bytes=32 Zeit<1ms TTL=64

Ping-Statistik für 192.168.1.17:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 0ms, Maximum = 1ms, Mittelwert = 0ms

U:\>_
```

Ilustracja 45: Przykład testu działania

4. Jeśli test został przeprowadzony pomyślnie, zamknąć okno poleceń.

8.5 Zmiana haseł

Wskazówka Zmiana haseł standardowych



Ustawione fabrycznie, standardowe hasła podane w niniejszej instrukcji obsługi nie stanowią wystarczającego zabezpieczenia! Hasła należy zmieniać stosownie do potrzeb!

W celu zwiększenia bezpieczeństwa hasła powinny zawierać kombinację małych liter (a ... z), dużych liter (A ... Z), cyfr (0 ... 9), spacji i znaków specjalnych: (!"#\$%&'()*+,-./:;<=>?@[\\^_`{|}~). W skład haseł nie powinny wchodzić popularne nazwy, daty urodzenia i inne łatwe do odgadnięcia informacje.

Przed uruchomieniem sterownika należy zmienić hasła standardowe! Hasła standardowe nadawane są dla grup użytkowników „Użytkownicy WBM” i „Użytkownicy Linux®”.

Tabela w rozdziale „Opis funkcji” > ... > „Użytkownicy i hasła” > „Grupa użytkowników WBM” przedstawia standardowe hasła dla użytkowników WBM. Aby zmienić te hasła, należy postępować w następujący sposób:

1. Podłączyć sterownik do PC, korzystając z interfejsów sieciowych (X1, X2).
2. Otworzyć na PC przeglądarkę internetową i wywołać WBM sterownika (patrz rozdział „Uruchamianie” > ... > „Konfiguracja za pomocą systemu zarządzania przez WWW (WBM)”).
3. Zalogować się na sterowniku jako użytkownik „admin” za pomocą standardowego hasła.
4. Zmienić hasło dla wszystkich użytkowników na stronie WBM „Configuration of the users for the WBM”.
5. Wybrać każdego użytkownika, nadać mu nowe hasło i je potwierdzić.

Tabela w rozdziale „Opis funkcji” > ... > „Użytkownicy i hasła” > „Grupa użytkowników Linux®” przedstawia standardowe hasła dla użytkowników Linux®. Aby zmienić te hasła, należy postępować w następujący sposób:

1. Podłączyć sterownik do PC, korzystając z interfejsu sieciowego X1.
2. Otworzyć na PC program terminalowy (patrz rozdział „Uruchamianie” > ... > „Konfiguracja za pomocą Console-Based-Management-Tool (CBM) przez program terminalowy”).
3. Zalogować się na sterowniku jako użytkownik „root” za pomocą standardowego hasła.
4. Zmienić hasło dla wszystkich użytkowników przy użyciu poleceń „passwd root”, „passwd admin” i „passwd user”.

8.6 Wyłączanie / restart

Aby wyłączyć sterownik, należy odłączyć zasilanie.

Aby przeprowadzić restart, należy użyć przycisku RESET, jak opisano w rozdziale „Wyzwalanie funkcji RESET” > „Reset oprogramowania (restart)”. Alternatywnie można wyłączyć i ponownie włączyć sterownik.

Wskazówka



Po zmianach parametrów nie należy przeprowadzać restartu poprzez wyłączanie i ponowne włączanie!

Aby zmiany parametrów zostały zrealizowane, wymagany jest restart sterownika. Zapisanie zmian wymaga czasu.

W celu przeprowadzenia restartu nie należy włączać i wyłączać sterownika, ponieważ w efekcie zbyt wczesnego wyłączenia zmiany mogą zostać utracone.

Restart należy przeprowadzić tylko programowo poprzez funkcję Reboot. Dzięki temu wszystkie procesy zapisu zostaną przeprowadzone poprawnie i w pełni zakończone.

8.7 Wyzwalanie funkcji RESET

Za pomocą przełącznika trybu pracy i przycisku RESET (RST) można realizować różne funkcje resetu.

8.7.1 Gorący reset

Funkcja gorącego resetu jest zależna od aktywowanego systemu runtime (CODESYS V2 lub **e!RUNTIME**).

8.7.1.1 System runtime CODESYS V2

Przy gorącym resecie przywracana jest aplikacja CODESYS V2. Odpowiada on poleceniu „Reset” w środowisku WAGO-I/O-PRO.

W celu przeprowadzenia gorącego resetu należy ustawić przełącznik trybu pracy w pozycji RESET i przytrzymać go co najmniej 2 sekundy, ale nie dłużej niż 7 sekund.

Wykonanie sygnalizowane jest krótkim zgaśnięciem czerwonej LED „RUN” po puszczeniu przełącznika trybu pracy.

8.7.1.2 System runtime **e!RUNTIME**

Przy gorącym resecie przywracane są wszystkie aplikacje **e!RUNTIME**. Wszystkie dane globalne ustawiane są na poziomie ich wartości inicjacyjnych. Odpowiada to poleceniu „Reset warm” w środowisku **e!COCKPIT**.

W celu przeprowadzenia gorącego resetu należy ustawić przełącznik trybu pracy w pozycji RESET i przytrzymać go co najmniej 2 sekundy, ale nie dłużej niż 7 sekund.

Wykonanie sygnalizowane jest krótkim zgaśnięciem czerwonej LED „RUN” po puszczeniu przełącznika trybu pracy.

8.7.2 Zimny reset

Funkcja zimnego resetu jest zależna od aktywowanego systemu runtime (CODESYS V2 lub **e!RUNTIME**).

8.7.2.1 System runtime CODESYS V2

Przy zimnym resecie przywracana jest aplikacja CODESYS V2 i usuwana pamięć ze zmiennymi nieulotnymi. Odpowiada to poleceniu „Reset cold” w środowisku WAGO-I/O-PRO.

W celu przeprowadzenia zimnego resetu należy ustawić przełącznik trybu pracy w pozycji RESET i przytrzymać go dłużej niż 7 sekund.

Wykonanie sygnalizowane jest dłuższym zgaśnięciem czerwonej LED „RUN” po upływie 7 sekund. Następnie można puścić przełącznik trybu pracy.

8.7.2.2 System runtime *e!RUNTIME*

Przy zimnym resecie przywracane są wszystkie aplikacje *e!RUNTIME*. Wszystkie dane globalne i zmienne nieulotne ustawiane są na poziomie ich wartości inicjacyjnych.

Odpowiada to poleceniu „Reset cold“ w środowisku *e!COCKPIT*.

W celu przeprowadzenia zimnego resetu należy ustawić przełącznik trybu pracy w pozycji RESET i przytrzymać go dłużej niż 7 sekund.

Wykonanie sygnalizowane jest dłuższym zgaśnięciem czerwonej LED „RUN“ po upływie 7 sekund. Następnie można puścić przełącznik trybu pracy.

8.7.3 Reset programowy (restart)

Przy resecie programowym sterownik uruchamiany jest ponownie.

W celu przeprowadzenia resetu programowego należy ustawić przełącznik trybu pracy w pozycji RUN lub STOP i przytrzymać przycisk RESET (RST) dłużej niż 1 sekundę, ale nie krócej niż 8 sekund.

Wykonanie sygnalizowane jest krótkim pomarańczowym rozbłyskiem wszystkich wskaźników LED. Po kilku sekundach wskaźniki LED SYS sygnalizują pomyślne zakończenie procesu bootowania sterownika.

8.7.4 Reset fabryczny

UWAGA



Nie wyłączać sterownika!

Przerwanie procedury aktualizacji wstecznej może uszkodzić sterownik. Dlatego podczas procedury Factory Reset nie należy wyłączać sterownika i nie odłączać zasilania!

Wskazówka



Wszystkie parametry i hasła zostaną nadpisane!

Przy Factory Reset wszystkie parametry i hasła sterownika zostaną nadpisane.

Zapisane aplikacje, włącznie z danymi dotyczącymi wizualizacji, zostaną usunięte.

Niezainstalowane funkcje firmware nie zostaną nadpisane.

W razie pytań należy skontaktować się ze wsparciem technicznym WAGO.

Po Factory Reset sterownik uruchamiany jest ponownie.

Aby przeprowadzić Factory Reset sterownika, należy postępować w następujący sposób:

1. Nacisnąć przycisk Reset (RST).
2. Ustawić przełącznik trybu pracy w pozycji RESET.

3. Przytrzymać oba przyciski, aż po ok. 8 sekundach LED „SYS“ zacznie migać na zmianę na czerwono i zielono.
4. Gdy LED „SYS“ miga na zmianę na czerwono i zielono, puścić przełącznik trybu pracy i przycisk Reset.

Wskazówka



Nie przerywać procedury resetu!

Przy zbyt wczesnym puszczeniu przycisku resetu (RST) sterownik uruchomi się ponownie, bez zrealizowania Factory Reset.

8.8 Konfiguracja

Wskazówka



Sprawdzić i zaktualizować wersję firmware!

Rozpoczynając pierwszą konfigurację należy sprawdzić, czy wersja firmware sterownika jest aktualna.

Zainstalowaną wersję firmware można znaleźć w WBM na stronie „Status Information” lub w menu CBM „Information” w punkcie „Controller Details”. Należy przeprowadzić aktualizację wersji firmware. W tym celu postępować zgodnie z opisem w rozdziale „Serwis” > „Zmiany firmware” > „Uaktualnienia firmware”.

W celu konfiguracji sterownika można wybrać następujące możliwości:

- Dostęp przez PC, za pomocą przeglądarki internetowej, do Web-Based-Management (rozdział „Konfiguracja przez Web-Based-Management (WBM)“)
- Dostęp przez PC, za pomocą programu terminalowego do „Console-Based Management Tool” (rozdział „Konfiguracja za pomocą Console-Based Management Tool (CBM)“).
- Dostęp przez program PLC CODESYS za pomocą biblioteki CODESYS V2 „WagoConfigToolLIB.lib” (rozdział „Załącznik” > „WagoConfigToolLIB.lib”) lub biblioteki *e!RUNTIME* „WagoAppConfigTool.lib”
- Dostęp poprzez PC, przy użyciu „WAGO Ethernet Settings” (rozdział „Konfiguracja za pomocą „WAGO Ethernet Settings”“).

CBM służy przeważnie do pierwszej konfiguracji i rozruchu sterownika. Dlatego udostępnia tylko niewielką liczbę parametrów WBM. Nie są wyświetlane na przykład parametry, które nie mogą być w sensowny sposób przedstawione w oknie terminala i które nie są potrzebne do rozruchu. Objasnienia dotyczące tych parametrów można znaleźć od rozdziału „Strona „Informacja”“.

8.8.1 Konfiguracja za pomocą systemu zarządzania przez WWW (WBM)

Strony HTML (zwane dalej w skrócie stronami) w ramach Web-Based-Management (WBM) służą do konfiguracji sterownika. W celu dostępu do WBM przez przeglądarkę internetową należy postępować w sposób następujący:

1. Podłączyć sterownik do sieci ETHERNET przez interfejs ETHERNET X1 i sieć ETHERNET.
2. Na PC otworzyć przeglądarkę internetową.
3. W pasku adresu przeglądarki internetowej wpisać „https://”, a następnie adres IP sterownika, a po nim „/wbm-ng”, np. „https://192.168.1.17/wbm-ng”. Pamiętać, że PC i sterownik muszą znajdować się w tej samej podsieci (patrz rozdział „Ustawianie adresu IP”).
W przypadku nieznajomości adresu IP i braku możliwości jego ustalenia, przełączyć sterownik czasowo na stały domyślny adres IP „192.168.1.17” (tryb „Fix IP Address” patrz rozdział „Uruchamianie” > ... > „Czasowe ustawienie stałego adresu IP”).

Wskazówka



Uwzględnić obciążenie przez program CODESYS

Jeśli sterownik jest obciążony przez program CODESYS, może to spowodować wolniejsze przetwarzanie w WBM. Dlatego niekiedy mogą być zgłaszane błędy wynikające z upływu czasu (time-out). Przed przystąpieniem do obszernych konfiguracji przez WBM uzasadnione jest zatem zatrzymanie aplikacji CODESYS.

- Jeśli połączenie mogło zostać nawiązane, może się pojawić okno logowania.

Ilustracja 46: Wpisywanie uwierzytelnienia (przykład)

4. Wprowadzić nazwę użytkownika i hasło.
5. Kliknąć przycisk **[Login]**.

6. W przypadku logowania się jako gość, kliknąć przycisk **[Guest]**.
 - W zależności od wybranego użytkownika wyświetlają się pasek nawigacji i zakładki WBM.

Jeśli w przeglądarce internetowej zostały dezaktywowane pliki cookies, można nadal korzystać z systemu WBM, o ile pozostanie się na tej stronie. Jeśli jednak strona internetowa zostanie załadowana od nowa (np. za pomocą **[F5]**), należy ponownie się zalogować, gdyż w tym przypadku przeglądarka nie ma możliwości zapisania plików z danej sesji logowania.

8.8.1.1 Zarządzanie użytkownikami WBM

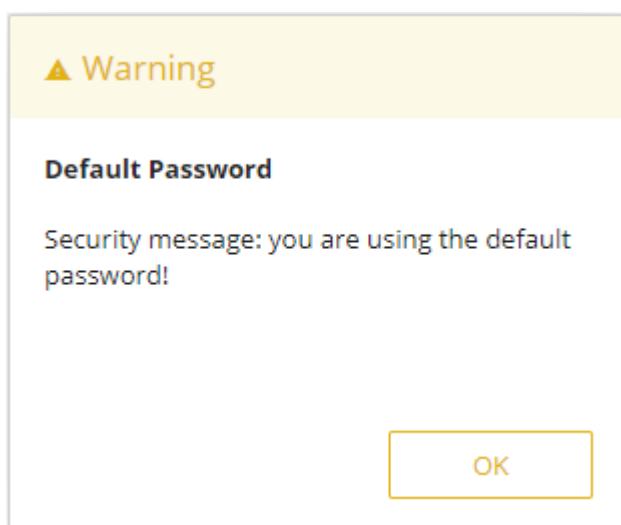
Poprzez zarządzanie użytkownikami można ograniczyć dostęp do funkcji WBM tylko dla wybranych osób.

Wskazówka **Zmiana haseł**



Ustawione fabrycznie, standardowe hasła podane w niniejszej instrukcji obsługi nie stanowią wystarczającego zabezpieczenia! Hasła należy zmieniać stosownie do potrzeb!

Dopóki hasło nie zostanie zmienione, na każdej odwiedzanej po zalogowaniu stronie internetowej pojawi się odpowiedni komunikat ostrzegawczy.



Ilustracja 47: Przypomnienie o konieczności zmiany hasła

Tabela 50: Fabryczne ustawienia użytkownika

Użytkownik	Uprawnienia	Standardowe hasło
admin	pełne (administrator)	wago
user	ograniczone	user
guest	tylko wyświetlanie	---

Wskazówka **Rozszerzone uprawnienia użytkowników WBM**



Użytkownicy WBM „admin” i „user” posiadają uprawnienia wykraczające poza WBM, aby mieć możliwość konfigurowania systemu i instalacji oprogramowania.

Zarządzanie użytkownikami dla aplikacji sterowania ustalane i realizowane jest osobno.

Dla stron WBM dostęp wygląda w następujący sposób:

Tabela 51: Prawa dostępu dla stron WBM

Zakładka / nawigacja	Tytuł strony WBM	Użytkownik
Informacja		
Device Status	Device Status	guest
Vendor Information	Vendor Information	guest
PLC Runtime	PLC Runtime Information	guest
Legal Information		
WAGO Licenses	WAGO Software License Agreement	guest
Open Source Licenses	Open Source Licenses	user
WBM Licenses	WBM Third Party License Information	user
WBM Version	WBM Version Info	guest
Configuration		
PLC Runtime	PLC Runtime Configuration	user
Networking		
TCP/IP Configuration	TCP/IP Configuration	user
Ethernet Configuration	Ethernet Configuration	user
Host/Domain Name	Configuration of Host and Domain Name	user
Routing	Routing	user
Clock	Clock Settings	user
Administration		
Service Interface	Configuration of Service Interface	admin
Create Image	Create bootable Image	admin
Package Server		
Firmware Backup	Firmware Backup	admin
Firmware Restore	Firmware Restore	admin
Active System	Active System	admin
Mass Storage	Mass Storage	admin
Software Uploads	Software Uploads	admin
Ports and Services		
Network Services	Configuration of Network Services	admin
NTP Client	Configuration of NTP Client	admin
PLC Runtime Services	PLC Runtime Services	admin
SSH	SSH Server Settings	admin
TFTP	TFTP Server	admin
DHCP Server	DHCP Server Configuration	admin
DNS	Configuration of DNS Service	user
Cloud Connectivity		

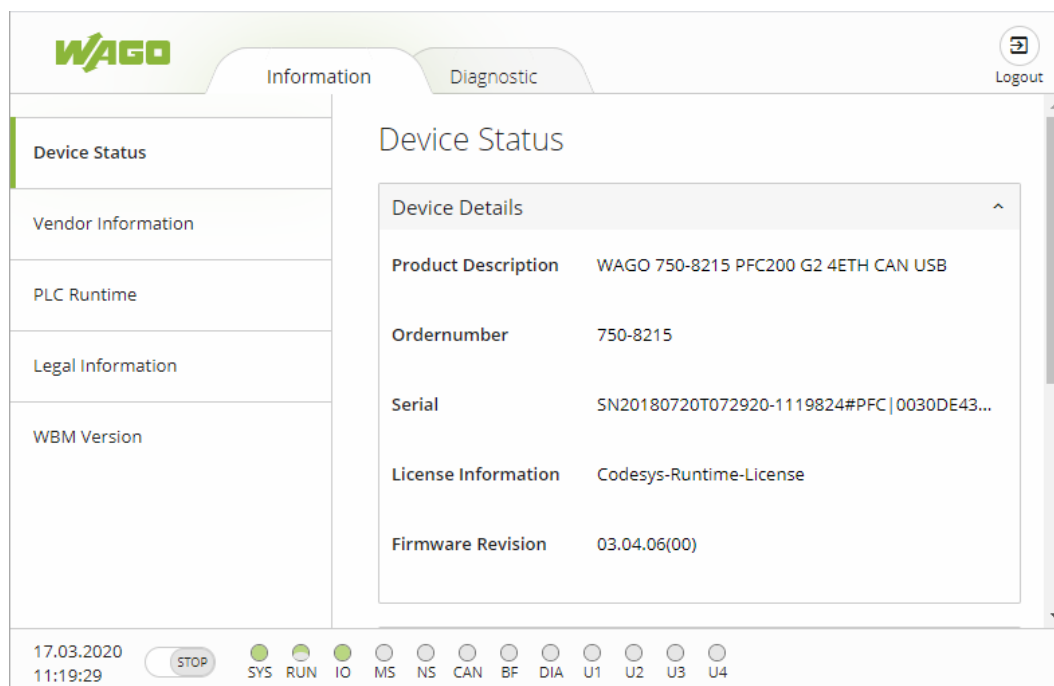
Tabela 51: Prawa dostępu dla stron WBM

Zakładka / nawigacja	Tytuł strony WBM	Użytkownik
Status	Overview	admin
Connection 1	Configuration	admin
Connection 2	Configuration	admin
SNMP		
General Configuration	Configuration of general SNMP parameters	admin
SNMP v1/v2c	Configuration of SNMP v1/v2c parameters	admin
SNMP v3	Configuration of SNMP v3 Users	admin
Users	WBM User Configuration	admin
Fieldbus		
OPC UA		
Status	OPC UA Status	admin
Configuration	OPC UA Configuration	admin
Information Model	OPC UA Information Model	admin
Modbus	Modbus Services Configuration	user
BACnet		
Status	BACnet Status	admin
Configuration	BACnet Configuration	admin
Storage Location	BACnet Storage Location	admin
Files	BACnet Files	admin
Diagnostic	BACnet Diagnostic	admin
Security		
OpenVPN / IPsec	OpenVPN / IPsec Configuration	admin
Firewall		
General Configuration	General Firewall Configuration	admin
Interface Configuration	Interface Configuration	admin
MAC Address Filter	Configuration of MAC Address Filter	admin
User Filter	Configuration of User Filter	admin
Certificates	Certificates	admin
TLS	Security Settings	admin
Integrity	Advanced Intrusion Detection Environment (AIDE)	admin
Diagnostic	Diagnostic Information	guest

8.8.1.2 Ogólne informacje o stronie

W pasku przeglądarki internetowej wyświetla się adres IP danego urządzenia.

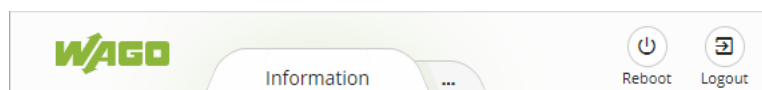
Strony WMB wyświetlane są dopiero po zalogowaniu. Aby się zalogować, należy wpisać w oknie logowania nazwę użytkownika i hasło, a następnie kliknąć przycisk **[Login]**.



Ilustracja 48: Okno przeglądarki WBM (przykład)

W wierszu nagłówka okna przeglądarki wyświetlane są zakładki różnych obszarów WBM i przyciski **[Reboot]** oraz **[Logout]**. Przycisk **[Reboot]** widoczny jest tylko wtedy, gdy zalogowany jest administrator.

Gdy na wybranej szerokości okna nie mieszczą się wszystkie zakładki, w miejscu niewyświetlonej zakładki widoczna jest zakładka z symbolem (...). Dzięki temu poprzez listę rozwijalną można wybrać zakładki, które nie są wyświetlane.

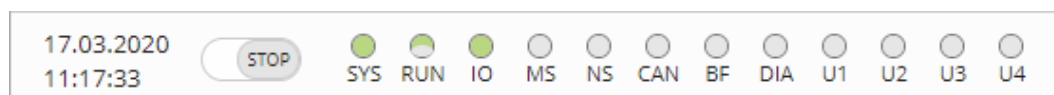


Ilustracja 49: Wiersz nagłówka WBM z niewyświetlanymi zakładkami (przykład)

Po lewej stronie okna przeglądarki wyświetlane jest drzewo nawigacji. Zawartość drzewa nawigacji zależy od wybranej zakładki.

Poprzez drzewo nawigacji można wejść na poszczególne strony oraz podstrony (jeśli takie istnieją).

Na pasku statusu wyświetlany jest aktualny stan urządzenia.



Ilustracja 50: Wiersz statusu WBM (przykład)

- Data i godzina – lokalny czas i lokalna data na urządzeniu
- Stan przełącznika trybu pracy
- Stany LED urządzenia:
LED mają odpowiednie opis (np. SYS, RUN, ...), a ich stany są przedstawione w sposób graficzny.
Możliwe są następujące stany LED:
 - kolor szary: LED jest wyłączona.
 - kolor na całej powierzchni: LED jest włączona i ma odpowiedni kolor.
 - kolor na połowie powierzchni: LED miga w odpowiednim kolorze. Druga połówka powierzchni jest wtedy szara lub może również mieć jakiś kolor. Ten ostatni przypadek oznacza, że LED miga w różnych kolorach.

Po najechaniu kursorem na LED otwiera się tooltip, zawierający dalsze informacje. Wyświetlony tekst zawiera komunikat, który wprowadził LED w aktualny stan. Podana jest też godzina komunikatu.

Stany wyświetlone w WBM nie odpowiadają w każdym momencie aktualnym stanom urządzenia. Transmisja danych wymaga określonego czasu, a odpytywanie następuje w określonych interwałach. Czas między odpytywaniami wynosi 30 sekund.

Wskazówka



Po zmianach parametrów nie należy przeprowadzać restartu poprzez wyłączanie i ponowne włączanie!

Aby zmiany parametrów zostały zrealizowane, wymagany jest restart sterownika. Zapisanie zmian wymaga czasu.

W celu przeprowadzenia restartu nie należy włączać i wyłączać sterownika, ponieważ w efekcie zbyt wczesnego wyłączenia zmiany mogą zostać utracone.

Restart należy przeprowadzić tylko programowo poprzez funkcję Reboot. Dzięki temu wszystkie procesy zapisu zostaną przeprowadzone poprawnie i w pełni zakończone.

Opis stron WBM i odpowiednich parametrów można znaleźć w punkcie „Dialogi konfiguracyjne” > „Web-Based-Management (WBM)”.

8.8.2 Konfiguracja za pomocą Console-Based-Management-Tool (CBM) przez program terminalowy

Console-Based-Management-Tool (CBM) służy zasadniczo do pierwszej konfiguracji i rozruchu sterownika przez program terminalowy. Dlatego udostępnia tylko niewielką liczbę parametrów sterownika. Nie są wyświetlane na przykład parametry, które nie mogą być w sensowny sposób przedstawione w oknie terminala i które nie są potrzebne do rozruchu.

1. Podłączyć PC z zainstalowanym programem terminalowym (obsługującym SSH) do interfejsu ETHERNET X1 sterownika.
2. Uruchomić program terminalowy.
3. Wybrać rodzaj połączenia „SSH” i jako parametr połączenia wpisać adres IP sterownika port 22.
4. Zalogować się do systemu Linux® jako „Superuser”. Nazwę użytkownika i hasło znaleźć można w rozdziale „Użytkownicy i hasła” > „Grupa Linux®-User”.
5. Otworzyć narzędzie konfiguracyjne, wpisując „cbm” w wierszu poleceń programu terminalowego (uwzględnić pisownię wielką/małą literą) i potwierdzić klawiszem **[Enter]**.

```
=====
WAGO Console Based Management Tool
=====
```

```
Main Menu
```

```
-----
0. Quit
1. Information
2. PLC Runtime
3. Networking
4. Firewall
5. Clock
6. Administration
7. Package Server
8. Mass Storage
9. Software Uploads
10. Ports and Services
11. SNMP
12. PROFIBUS DP
-----
```

```
Select an entry or Q to quit
-----
```

Ilustracja 51: Menu główne CBM (przykład)

8.8.2.1 Struktura menu CBM

Tabela 52: Struktura menu CBM

Hierarchia menu
0. Quit
1. Information
0. Back to Main Menu
1. Controller Details
2. Network Details
2. PLC Runtime
0. Back to Main Menu
1. Information
2. General Configuration
3. WebVisu
3. Networking
0. Back to Main Menu
1. Host-/Domain Name
2. TCP/IP
0. Back to Networking Menu
1. IP Address
2. Default Gateway
3. DNS Server
3. Ethernet
0. Back to Networking Menu
1. Switch Configuration
2. Ethernet Ports
0. Back to Ethernet Menu
1. Interface X1
2. Interface X2
4. Firewall
0. Back to Main Menu
1. General Configuration
2. MAC Address Filter
3. User Filter
5. Clock
0. Back to Main Menu
1. Date on device (local)
2. Time on device (local)
3. Time on device (UTC)
4. Clock Display Mode
5. Timezone
6. TZ-String
6. Administration
0. Back to Main Menu

Tabela 52: Struktura menu CBM

Hierarchia menu	
1. Users	
2. Create Image	
3. Reboot Controller	
7. Package Server	
0. Back to Main Menu	
1. Firmware Backup	
2. Firmware Restore	
3. System Partition	
8. Mass Storage	
0. Back to Main Menu	
1. Internal Flash (active partition)	
9. Software Uploads	
0. Back to Main Menu	
1. Update Script	
10. Ports and Services	
0. Back to Main Menu	
1. Telnet	
2. FTP	
3. FTPS	
4. HTTP	
5. HTTPS	
6. NTP	
7. SSH	
8. TFTP	
9. DHCPD	
10. DNS	
11. IOCHECK PORT	
12. Modbus TCP	
13. Modbus UDP	
14. PLC Runtime Services	
11. SNMP	
0. Back to Main Menu	
1. General SNMP Configuration	
2. SNMP v1/v2c Manager Configuration	
3. SNMP v1/v2c Trap Receiver Configuration	
4. SNMP v3 Configuration	
5. SNMP firewalling	
6. Secure SNMP firewalling	

Wskazówka



Po zmianach parametrów nie należy przeprowadzać restartu poprzez wyłączenie i ponowne włączenie!

Aby zmiany parametrów zostały zrealizowane, wymagany jest restart sterownika. Zapisanie zmian wymaga czasu.

W celu przeprowadzenia restartu nie należy włączać i wyłączać sterownika, ponieważ w efekcie zbyt wczesnego wyłączenia zmiany mogą zostać utracone.

Restart należy przeprowadzić tylko programowo poprzez funkcję Reboot. Dzięki temu wszystkie procesy zapisu zostaną przeprowadzone poprawnie i w pełni zakończone.

Opis menu CBM i odpowiednich parametrów można znaleźć w punkcie „Dialogi konfiguracyjne” > „Console-Based-Management (CBM)”.

8.8.3 Konfiguracja za pomocą „WAGO Ethernet Settings“

Za pomocą programu „WAGO Ethernet Settings“ można poprzez sterownik odczytywać informacje systemowe, konfigurować ustawienia sieci i aktywować/dezaktywować serwer WWW.

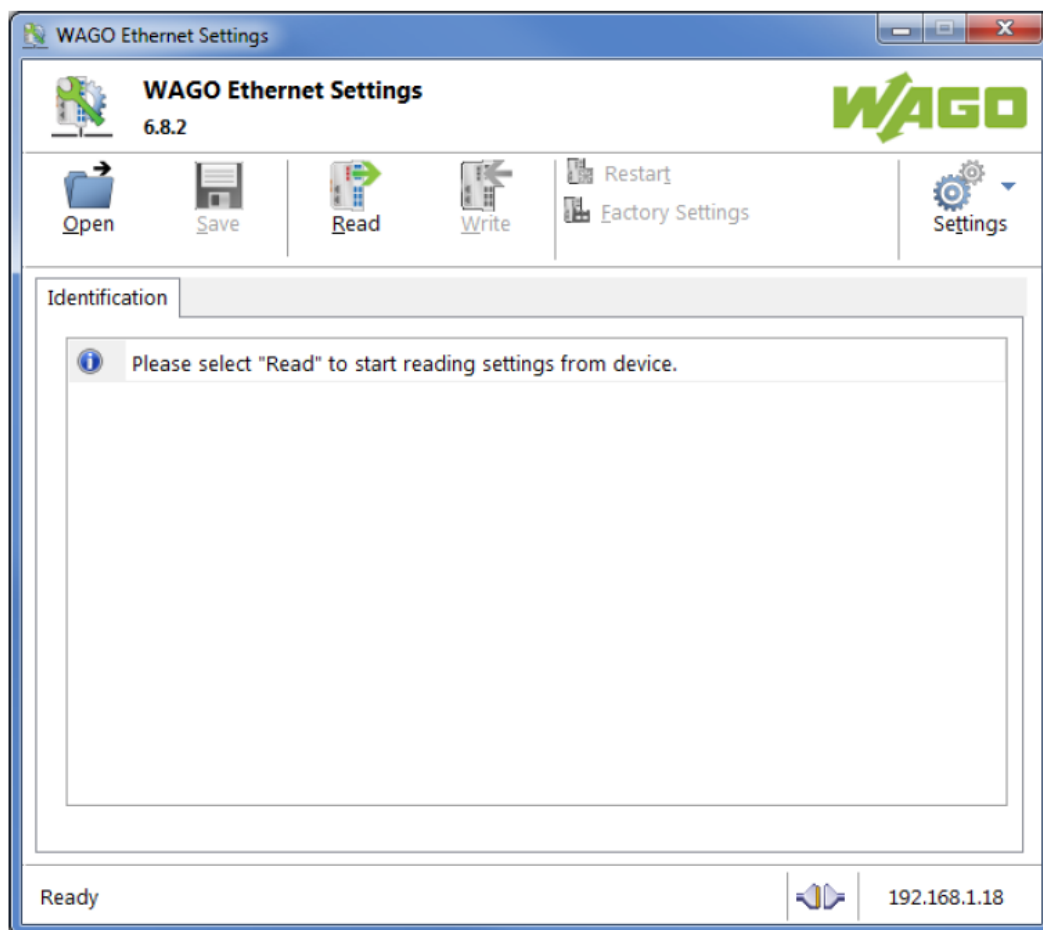
Wskazówka **Zwrócić uwagę na wersję oprogramowania!**



Przy konfiguracji sterownika należy korzystać z wersji „WAGO Ethernet Settings“ nie starszej niż 6.3.1(01)!

Po uruchomieniu „WAGO Ethernet Settings“ należy wybrać odpowiedni interfejs.

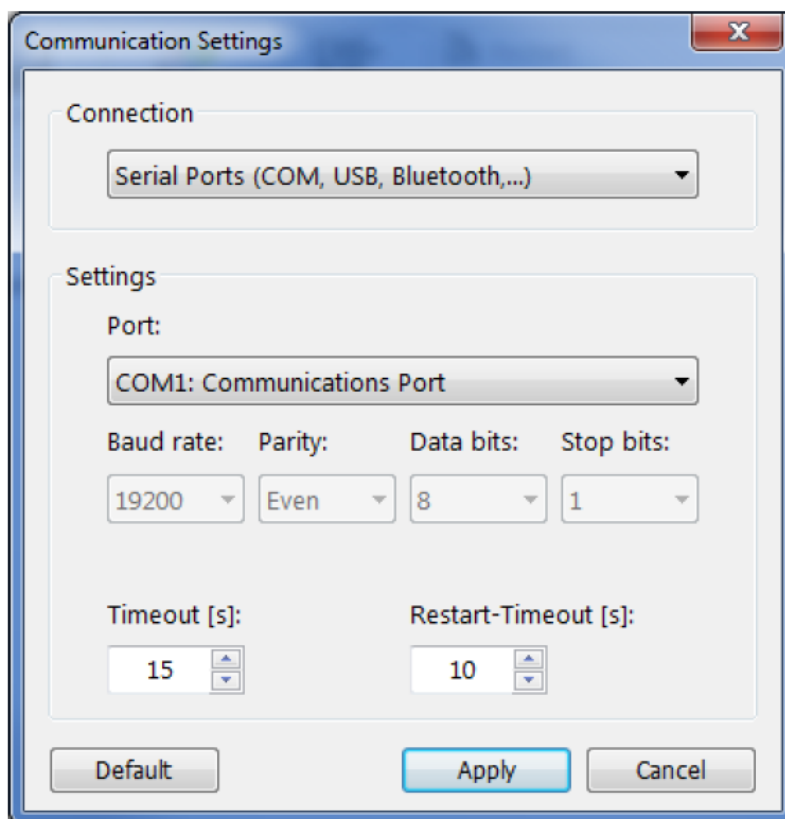
Możliwe jest połączenie przez złącze serwisowe przy użyciu przewodu konfiguracyjnego 750-920, adaptera Bluetooth® 750-921 bądź też przewodu konfiguracyjnego 750-923 lub 750-923/000-001 lub przez interfejs ETHERNET.



Ilustracja 52: „WAGO Ethernet Settings“ – ekran startowy (przykład)

Należy kliknąć „Settings“ a potem „Communication“.

W nowo otwartym oknie „Communication settings“ konfiguruje się ustawienia w zależności od potrzeb.



Ilustracja 53: „WAGO Ethernet Settings” – konfiguracja połączeń komunikacyjnych

Po skonfigurowaniu „WAGO Ethernet Settings” i kliknięciu **[Apply]** automatycznie zostanie nawiązane połączenie ze sterownikiem.

Jeśli „WAGO Ethernet Settings” był już uruchomiony z prawidłowymi parametrami, można nawiązać połączenie ze sterownikiem klikając **[Read]**.

8.8.3.1 Zakładka Identification

W tym miejscu zawarte są podstawowe informacje o podłączonym urządzeniu.

Oprócz niektórych stałych wartości jak nr katalogowy, adres MAC i wersja firmware widoczne są także aktualnie zastosowany adres IP i typ konfiguracji.

Identification	Network	PLC	Status
Item Number	750-8206		
Description	WAGO 750-8206 PFC200 CS 2ETH RS CAN DPS		
FW Version	02.06.20(09)		
HW Version	01		
FWL Version	2014.11.0-pXc-02.01.01 IDX=02		
Serial Number	SN20141204T134141-0025639#PFCJ0030DE400E6F		
MAC address X1	0030DE400E6F		
MAC address X2	0030DE400E6F		
IP address X1	192.168.1.18 (Static Configuration)		
IP address X2	0.0.0.0 (No configuration!)		
Runtime system	e!RUNTIME		

Ilustracja 54: „WAGO Ethernet Settings” – zakładka Identification (przykład)

8.8.3.2 Zakładka Network

Ta zakładka wykorzystywana jest do konfigurowania ustawień sieci.

W kolumnie „Edit” można zmieniać wartości, a w kolumnie „Currently used” widoczne są aktualnie zastosowane parametry.

Parameter	Edit	Currently used
Address Source	Static Configuration	Static Configuration
IP address	192.168.1.18	192.168.1.18
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0
Preferred DNS-Server	0.0.0.0	0.0.0.0
Alternative DNS-Server	0.0.0.0	0.0.0.0
Time Server	0.0.0.0	0.0.0.0
Hostname		PFC200-400E6F
Domain name	localdomain.lan	localdomain.lan

Interface X1
Interface X2
Run WBM

Interfaces
☐ Switched
☒ Separated

Ilustracja 55: „WAGO Ethernet Settings” – zakładka Network

Adres Source

Tutaj można wybrać, w jaki sposób sterownik ma uzyskać adres IP: statycznie, przez DHCP lub przez BootP.

IP address, subnet mask, gateway

W przypadku konfiguracji statycznej tutaj wpisuje się parametry sieci.

Wskazówka



Ograniczone ustawienia dla bram domyślnych!

Za pomocą „WAGO Ethernet Settings” można ustawić tylko bramę domyślną 1.

Bramę domyślną 2 można ustawić wyłącznie w WBM!

Preferred DNS Server, alternative DNS Server

Tutaj w razie potrzeby wprowadza się adres IP dostępnego serwera DNS, który może być wykorzystany w identyfikowaniu nazw w sieci.

Time server

Tutaj wpisuje się adres IP serwera czasowego, gdy sterownik ma ustawić czas systemowy przez NTP.

Hostname

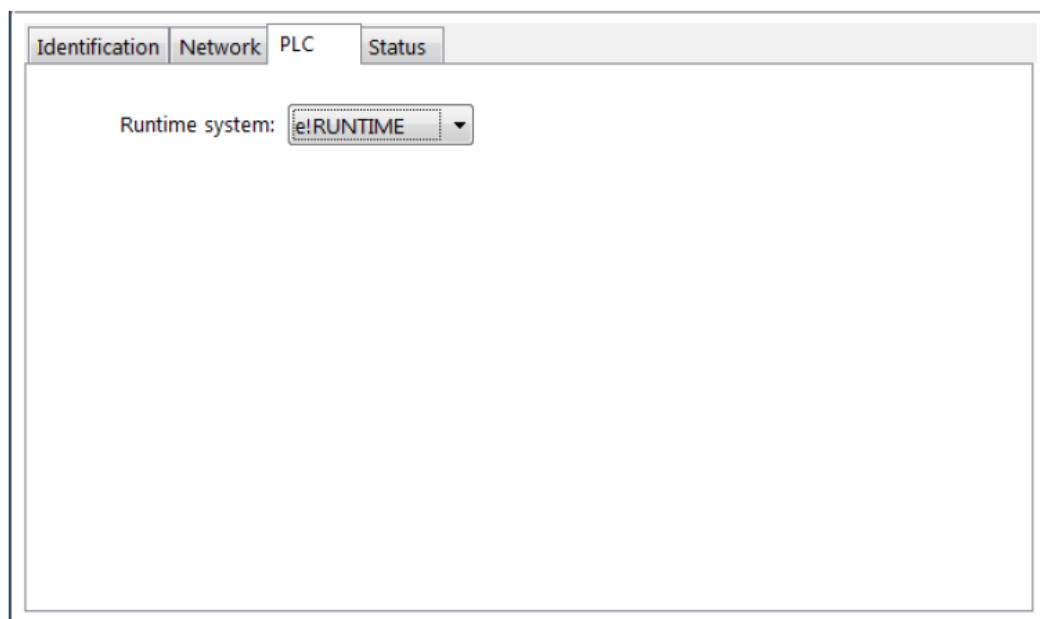
W tym miejscu wyświetlana jest nazwa hosta sterownika. W ustawieniach fabrycznych składa się ona z ciągu „PFCx00-” i ostatnich 3 bajtów adresu MAC.

Ta standardowa wartość jest stosowana zawsze wtedy, gdy wybrana samodzielnie nazwa usuwana jest w kolumnie „Edit“.

Domain name

Tu wyświetlana jest aktualna nazwa domeny. Przy konfiguracji dynamicznej (np. DHCP) ustawienie to może zostać automatycznie nadpisane.

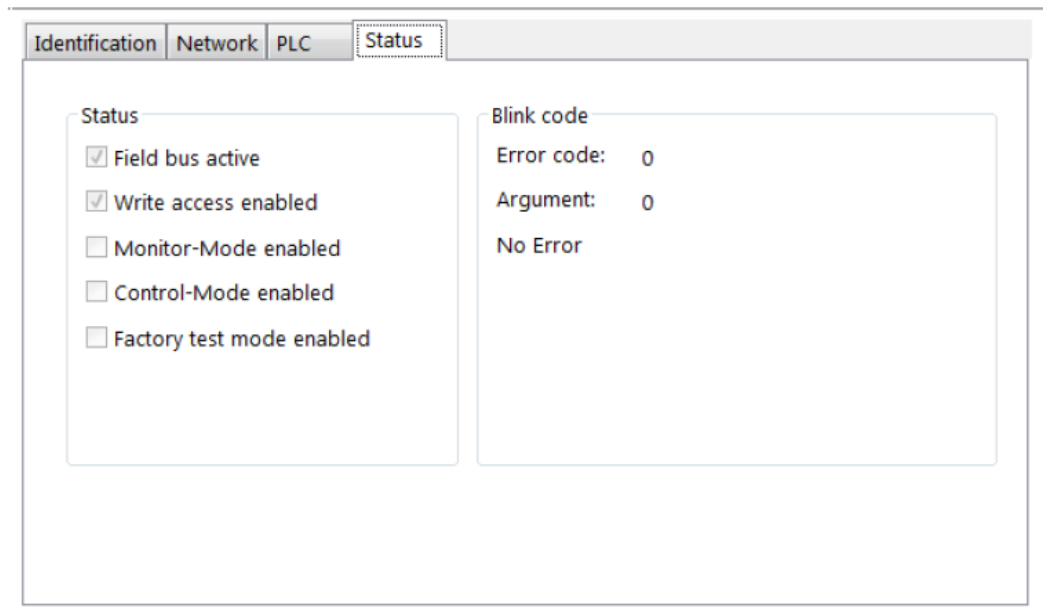
8.8.3.3 Zakładka PLC



Ilustracja 56: „WAGO Ethernet Settings” – zakładka PLC

Tutaj można wybrać system runtime.

8.8.3.4 Zakładka Status



Ilustracja 57: „WAGO Ethernet Settings” – zakładka Status

Tutaj wyświetlane są ogólne informacje o statusie sterownika.

9 Środowisko systemowe CODESYS 2.3

9.1 Instalacja środowiska programistycznego CODESYS 2.3

Instalacja CODESYS obejmuje dodatkowo filtry targetu WAGO. Zawierają one wszystkie informacje specyficzne dla urządzeń WAGO z serii 750/758.

Aby zainstalować środowisko programistyczne CODESYS 2.3 na PC, należy postępować zgodnie z poniższą instrukcją.

1. Włożyć CD-ROM „WAGO-I/O-PRO CAA” do napędu komputera.
2. Postępować zgodnie ze wskazówkami dotyczącymi instalacji, wyświetlanymi na ekranie. Po pomyślnej instalacji na ekranie pojawi się symbol CODESYS.

9.2 Pierwszy program z CODESYS 2.3

Ten rozdział opisuje przykładowe istotne kroki, wymagane do utworzenia projektu CODESYS. Może on służyć jako instrukcja szybkiego startu i nie uwzględnia pełnego zakresu funkcji CODESYS 2.3.

Informacja



Więcej informacji

Szczegółowy opis pełnej funkcjonalności można znaleźć w podręczniku „Manual for PLC Programming using CODESYS 2.3” na CD „WAGO-I/O-PRO CAA” (759-911).

9.2.1 Otwieranie środowiska programistycznego CODESYS

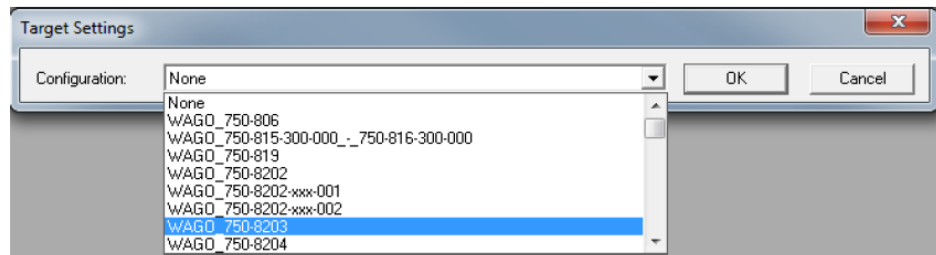
CODESYS otwiera się podwójnym kliknięciem symbolu CODESYS, który jest widoczny na ekranie lub poprzez menu startowe systemu operacyjnego.

W tym celu należy kliknąć przycisk „Start” i wybrać **Programs** >

WAGO Software > **CODESYS** > **CODESYS V2.3**.

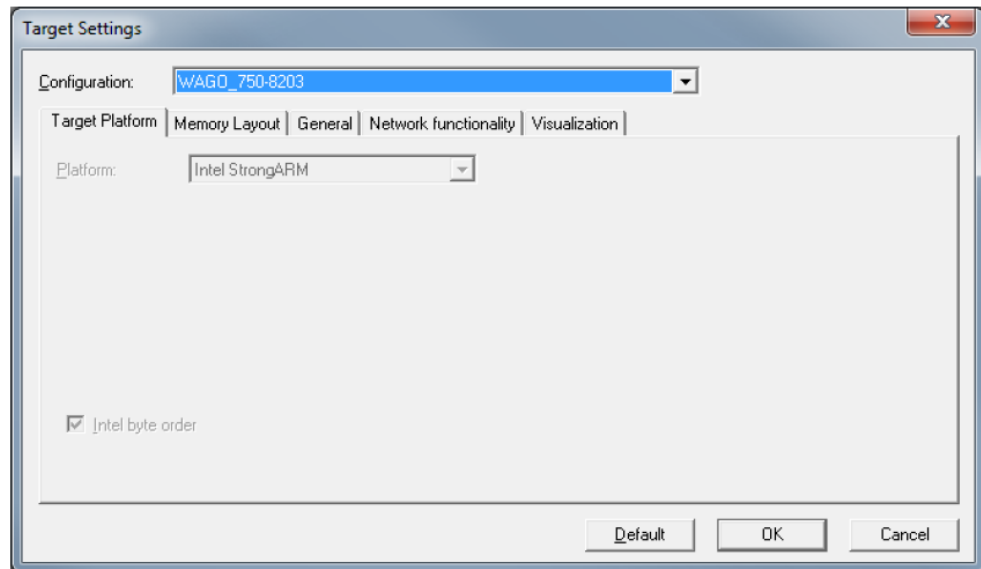
9.2.2 Zakładanie projektu i wybór systemu docelowego

1. Na pasku menu kliknąć **File** i wybrać **New**. Otworzy się okno „Target Settings”. Wyświetlą się wszystkie dostępne systemy docelowe, które można programować za pomocą CODESYS 2.3.
2. Otworzyć pole wyboru okna „Ustawienia systemu docelowego” i wybrać zastosowany sterownik sieciowy. W tym przykładzie jest nim PFC200 CS 2ETH CAN „WAGO_750-8203”.
3. Kliknąć przycisk **[OK]**. Otworzy się okno konfiguracyjne „Target Settings”.



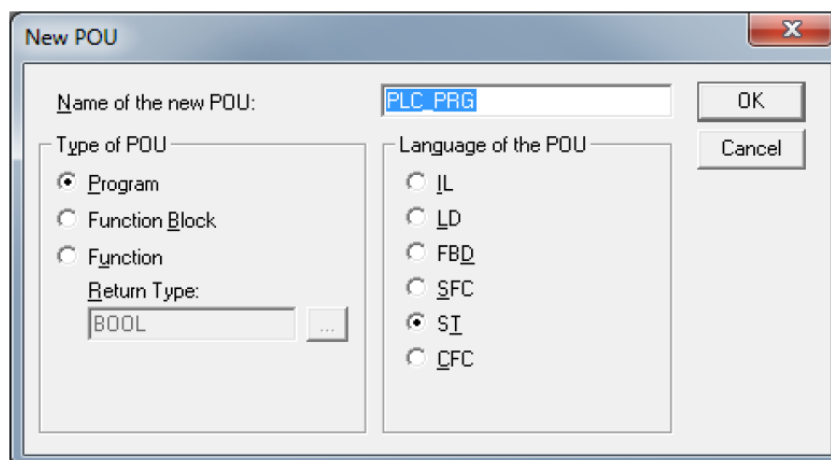
Ilustracja 58: Ustawienia systemu docelowego (1)

4. Aby zastosować standardową konfigurację dla sterownika sieciowego, należy kliknąć **[OK]**. Otworzy się okno „New POU”.

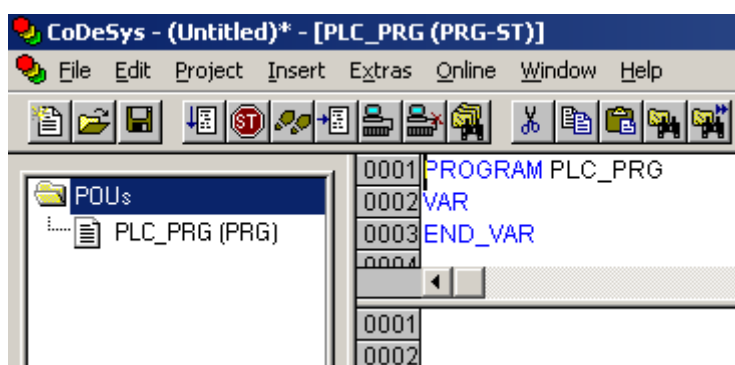


Ilustracja 59: Ustawienia systemu docelowego (2)

5. W oknie „New POU” utworzyć nowy blok funkcyjny. W tym przykładzie utworzony zostaje nowy blok „PLC_PRG” w języku programowania „ST”.
6. Aby utworzyć projekt, kliknąć **[OK]**. Otworzy się interfejs programowania.



Ilustracja 60: Tworzenie nowego bloku funkcyjnego



Ilustracja 61: Interfejs programowania z blokiem funkcyjnym PLC_PRG

9.2.3 Konfiguracja sterownika

Wskazówka

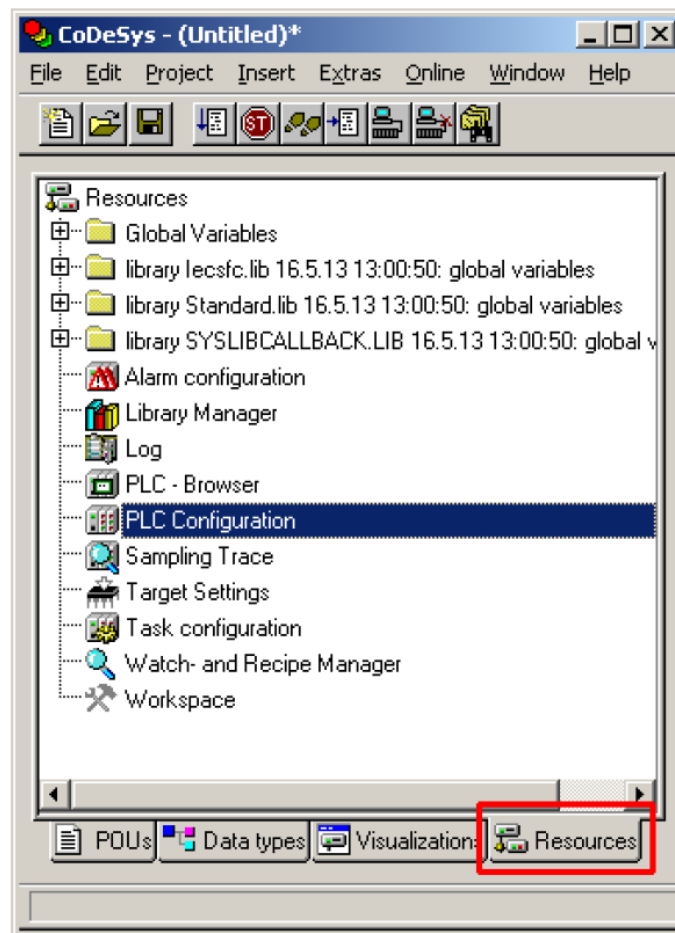


Sposób postępowania przy konfiguracji sterownika

Przedstawiony w tym rozdziale sposób postępowania opisuje konfigurację sterownika dla modułów I/O podłączonych do sterownika. Informacje o konfiguracji sterownika dla podłączonych sieci obiektowych zawarto w rozdziale dotyczącym danej sieci.

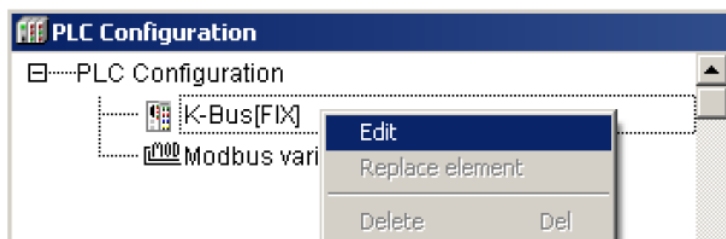
Konfiguracja sterownika służy do skonfigurowania sterownika z podłączonymi do niego modułami I/O i deklarowaniu zmiennych, aby zapewnić dostęp do wejść i wyjść modułów I/O. W tym celu postępować w następujący sposób:

1. Kliknąć zakładkę „Resources”.



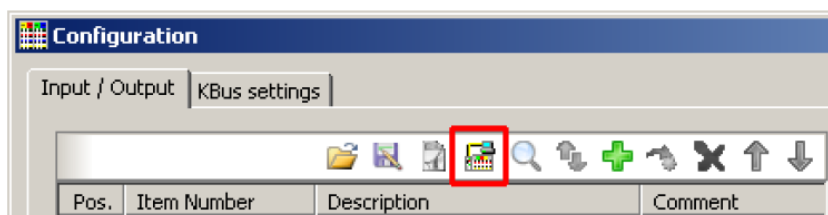
Ilustracja 62: Zakładka „Resources“

2. W oknie po lewej kliknąć dwukrotnie „PLC Configuration“. Otworzy się konfiguracja sterownika.
3. Prawym klawiszem myszy kliknąć punkt „K-Bus[Fix]“ i wybrać „Edit“ w menu kontekstowym. Otworzy się okno dialogowe „Configuration“.



Ilustracja 63: PLC Configuration – Edit

4. Aby zastosować topologię modułów I/O podłączonych do sterownika do wyboru są 3 możliwości: najprostsza to zeskanowanie topologii przez WAGO-I/O-CHECK.
W tym celu kliknąć przycisk „Start WAGO-I/O-CHECK and scan“.



Ilustracja 64: Przycisk „Start WAGO-I/O-CHECK and scan“

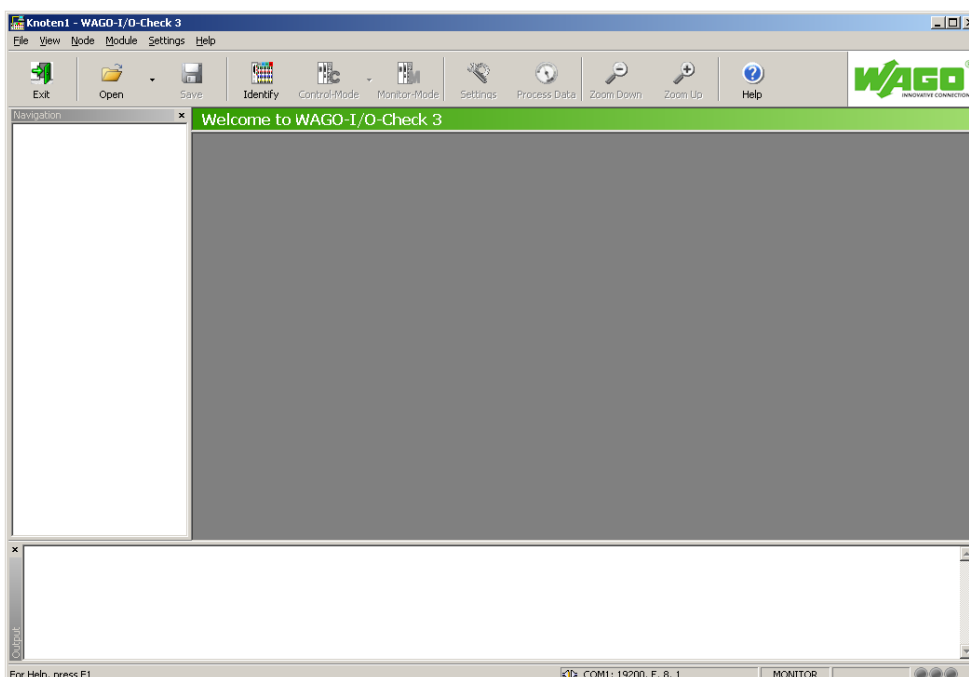
Wskazówka



Pamiętać o zainstalowaniu WAGO-I/O-CHECK!

Aby mieć dostęp do tej funkcjonalności, należy zainstalować aktualną wersję WAGO-I/O-CHECK i ustawić adres IP w oknie „Online > Communication parameters“, gdyż w przeciwnym razie komunikacja nie będzie możliwa.

5. Uruchomi się WAGO-I/O-CHECK.

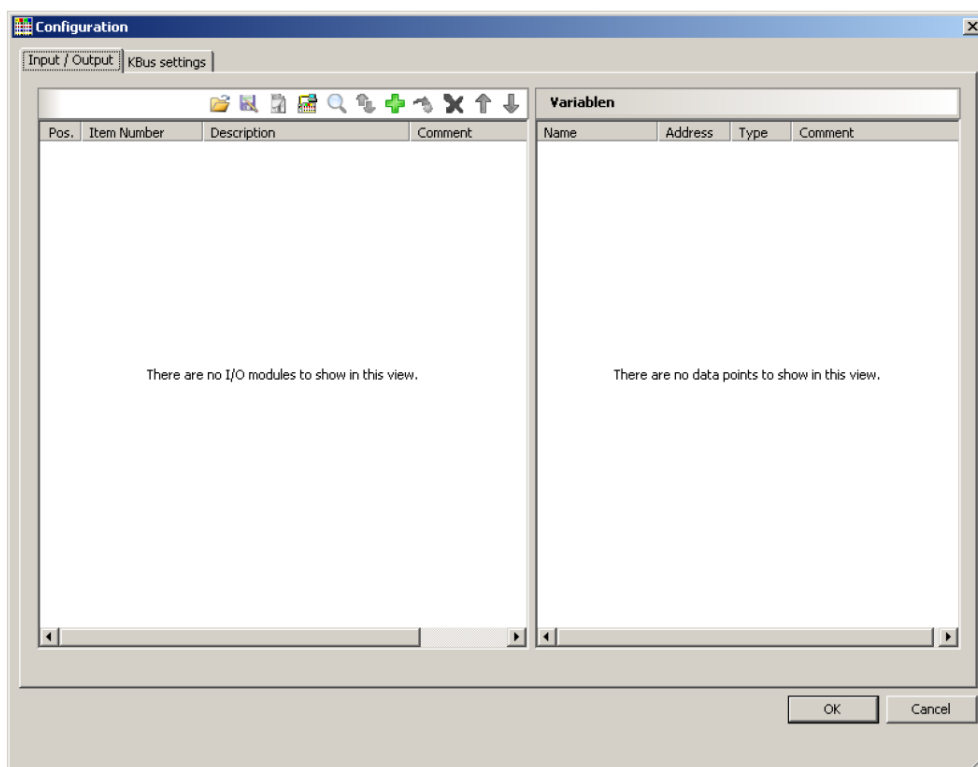


Ilustracja 65: WAGO-I/O-CHECK – ekran startowy

6. Aby utworzyć połączenie ze sterownikiem i wczytać konfigurację modułów I/O, kliknąć **[Identify]**.
7. Po pomyślnej identyfikacji kliknąć **[Save]** i zamknąć WAGO-I/O-CHECK.
8. W efekcie w oknie konfiguracji wprowadzone zostały wykryte moduły I/O.

Wskazówka**Pasywne moduły I/O**

Należy pamiętać, że pasywne moduły I/O, jak np. moduł zasilający (750-602/xxx-xxx) lub moduł końcowy (750-600/xxx-xxx) nie są widoczne w konfiguratorze I/O.



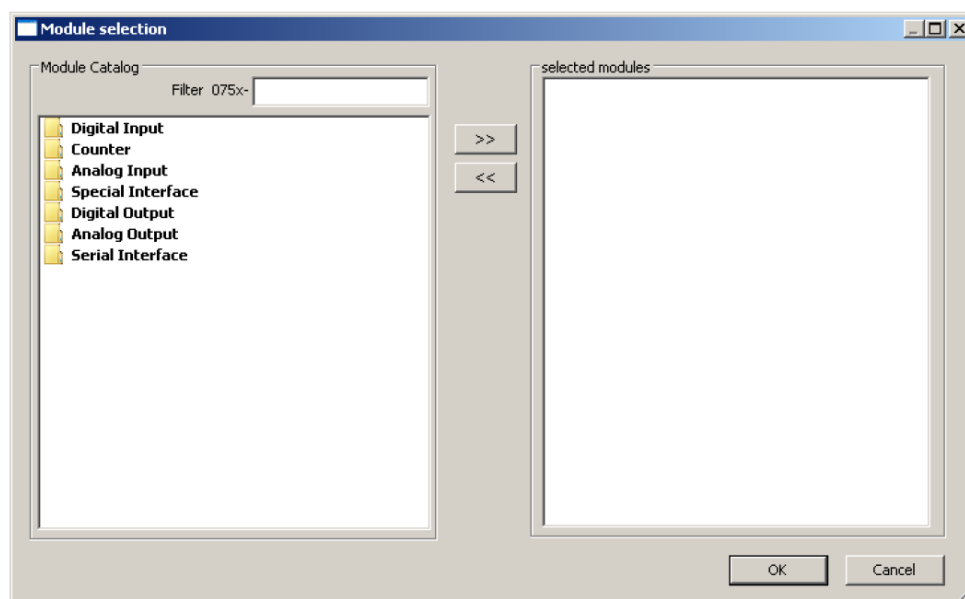
Ilustracja 66: Pusty konfigurator I/O

9. Aby przeprowadzić ręczną konfigurację lub modyfikację, można użyć przycisku **[Add]**, który pozwala dodać nowe moduły I/O.



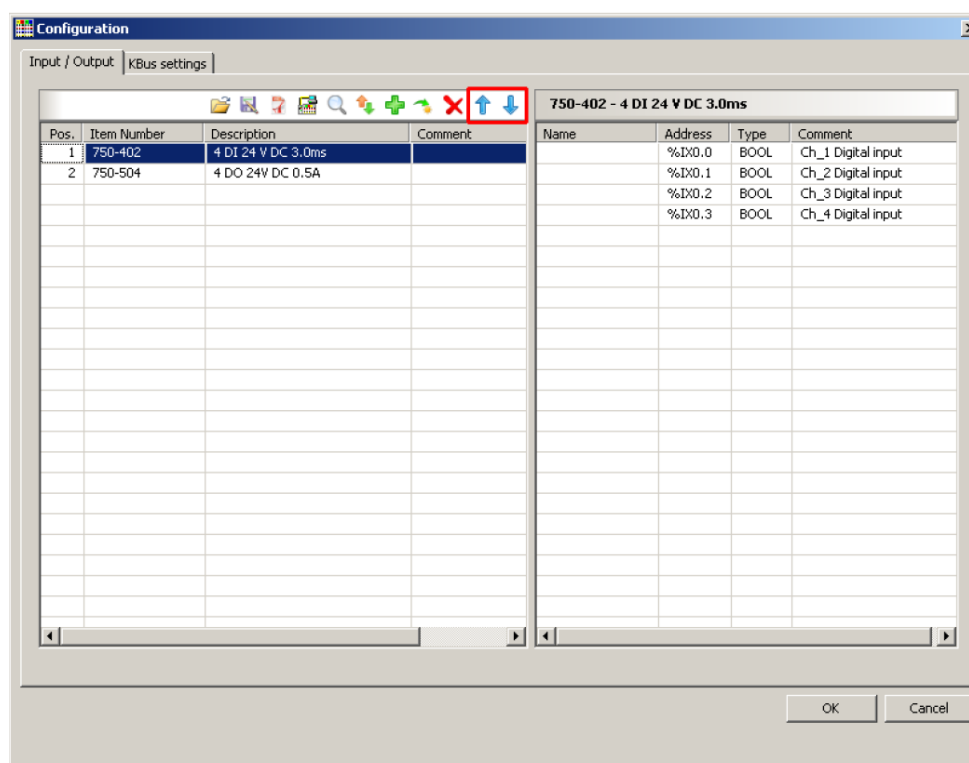
Ilustracja 67: Przycisk „Add I/O Modules”

10. W nowo wyświetlonym oknie „Module Selection” można wybrać żądane moduły.



Ilustracja 68: Okno „Module Selection“

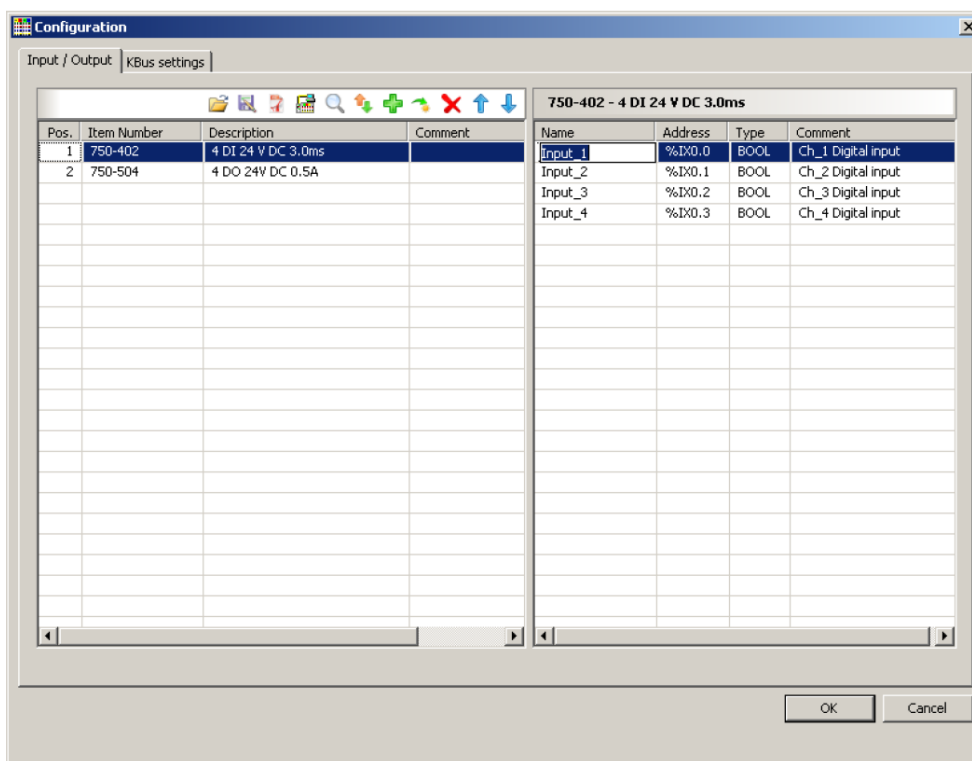
11. Pozycję modułu I/O można zmienić, zaznaczając moduł i przesuwając strzałkami widocznymi w prawym rogu okna w górę lub w dół.



Ilustracja 69: Konfigurator I/O z wyświetlonymi modułami I/O

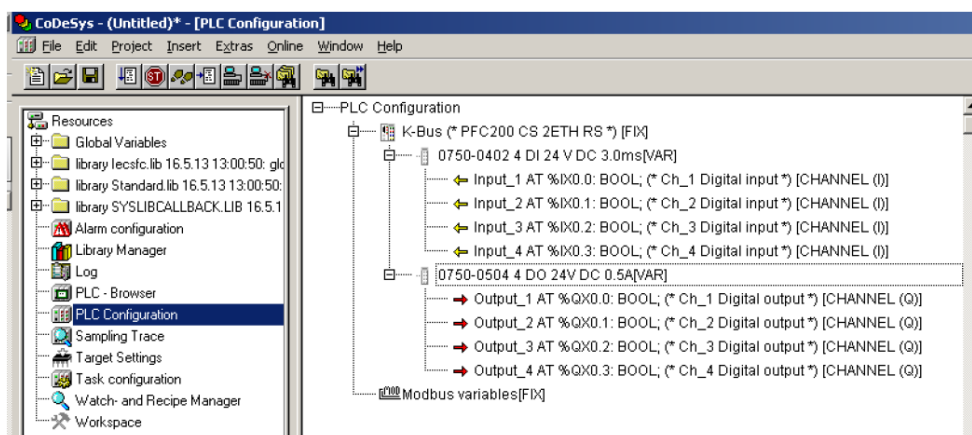
12. Wybrać opcję **[Import configuration from file]** aby dodać konfigurację zaimportowaną wcześniej za pomocą WAGO-I/O-CHECK.
13. W celu zakończenia konfiguracji I/O kliknąć **[OK]**.

14. Po prawej stronie okna konfiguracji wyświetlane są wejścia i wyjścia wybranego modułu I/O.
W kolumnie „Name” można zadeklarować własną zmienną, np. „Output_1”, „Output_2”, „Input_1”, „Input_2”.



Ilustracja 70: Deklaracja zmiennych

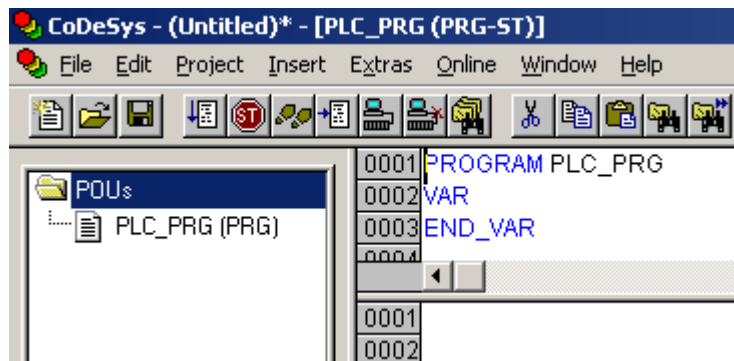
15. W konfiguracji sterownika pod „K-Bus[FIX]” widoczne są podłączone moduły I/O z przypisanymi stałymi adresami oraz ustawione wcześniej nazwy zmiennych.



Ilustracja 71: Konfiguracja sterownika: moduły I/O z przydzielonymi adresami

9.2.4 Edycja bloku funkcyjnego

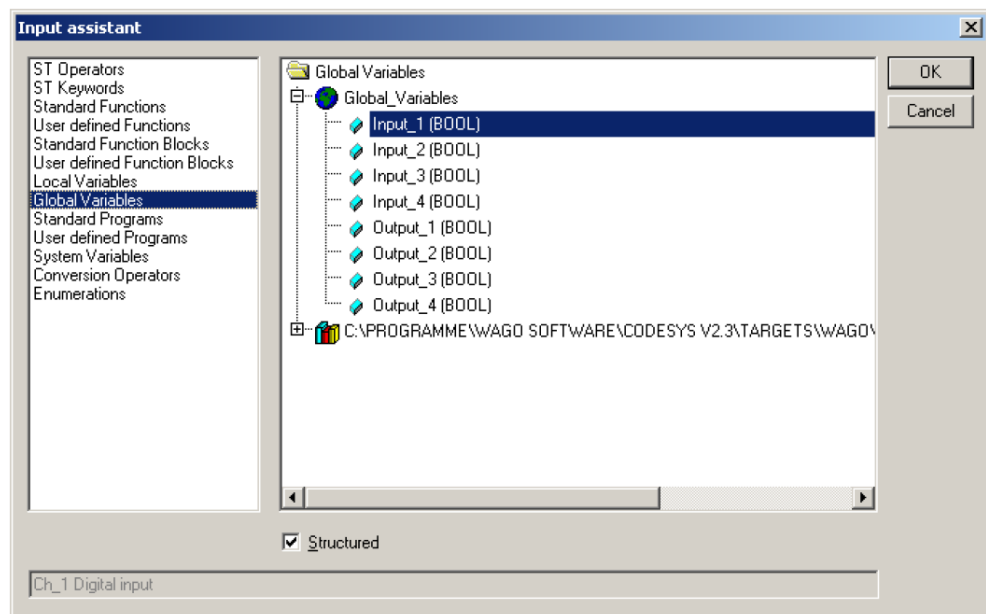
W celu edycji bloku funkcyjnego PLC_PRG należy otworzyć zakładkę „Function block” i kliknąć dwukrotnie PLC_PRG.



Ilustracja 72: Function block

Poniższy przykład objaśnia zasady edycji bloku funkcyjnego. Należy przydzielić wejście do wyjścia:

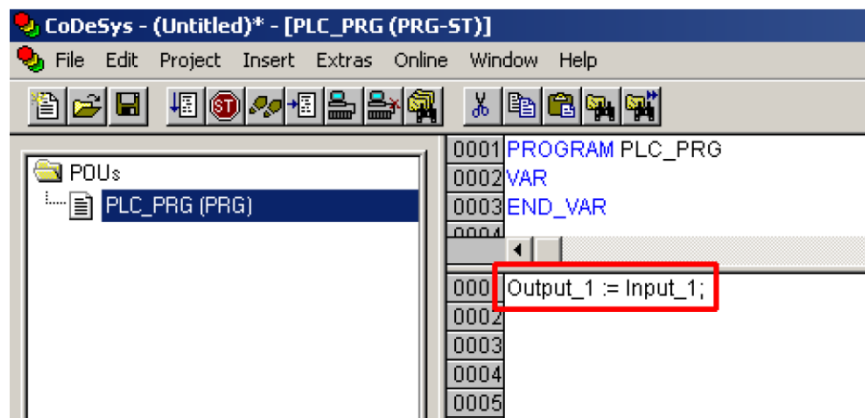
1. Nacisnąć **[F2]**, aby otworzyć okno asystenta lub kliknąć prawym przyciskiem myszy i wybrać z menu kontekstowego funkcję „Input assistant”.



Ilustracja 73: Asystent deklaracji zmiennych (Input assistant)

2. W katalogu „Global variables” wybrać zadeklarowaną zmienną „Output_1” i kliknąć **[OK]**.
3. Za zmienną wprowadzić znak przypisania „:=”.

4. Powtórzyć krok 2 dla zmiennej „Input_1”.



Ilustracja 74: Przykład przypisywania zmiennej

5. W celu kompilacji na pasku menu kliknąć **Project > Compile all**.

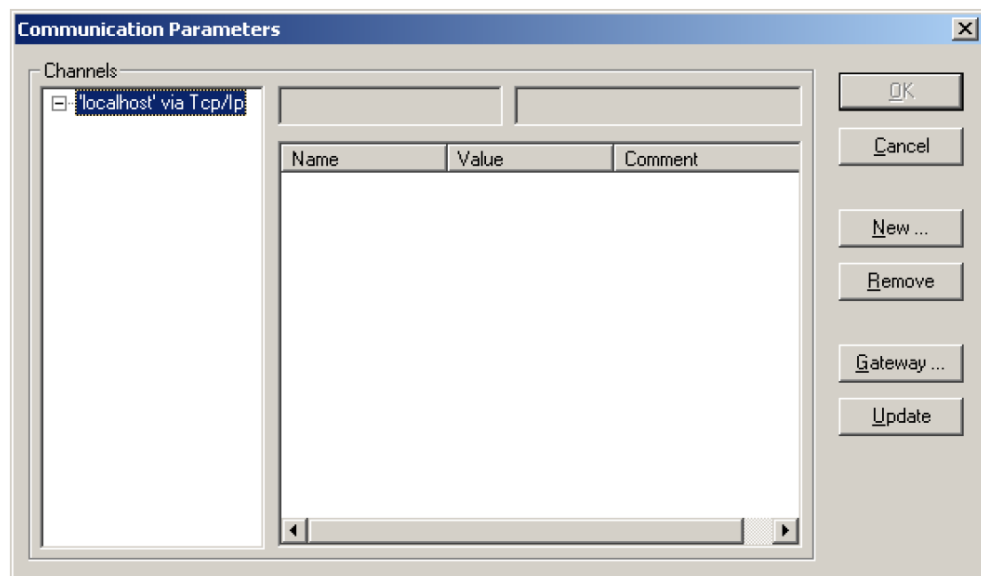
9.2.5 Ładowanie programu PLC do sterownika

Wymagania:

- Symulacja jest dezaktywowana (**Online > Simulation**).
- PC jest połączony ze sterownikiem przez sieć ETHERNET. Informacje na ten temat zawarto w rozdziale „Opis urządzenia” > ...> „Złącze sieciowe ETHERNET – X1, X2”.

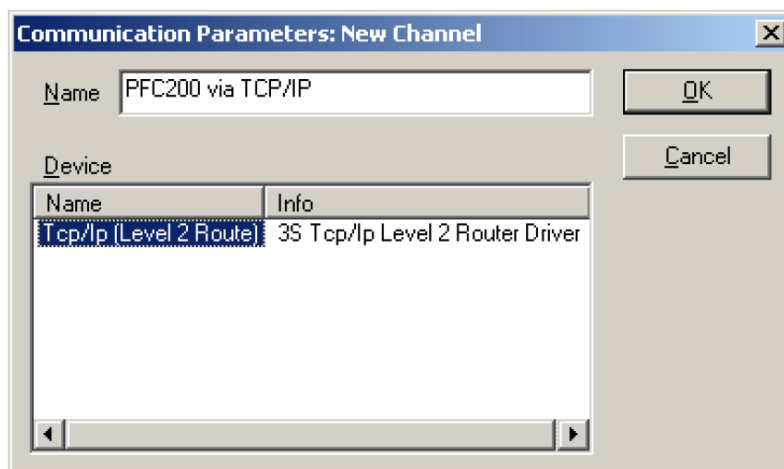
Wykonać poniższe czynności:

1. Na pasku menu kliknąć **Online** i wybrać **Communication Parameters** Otworzy się okno „Communication Parameters”.
2. W celu wybrania połączenia komunikacyjnego w oknie „Communication Parameters” kliknąć [**New ...**]. Otworzy się okno do konfiguracji połączeń.



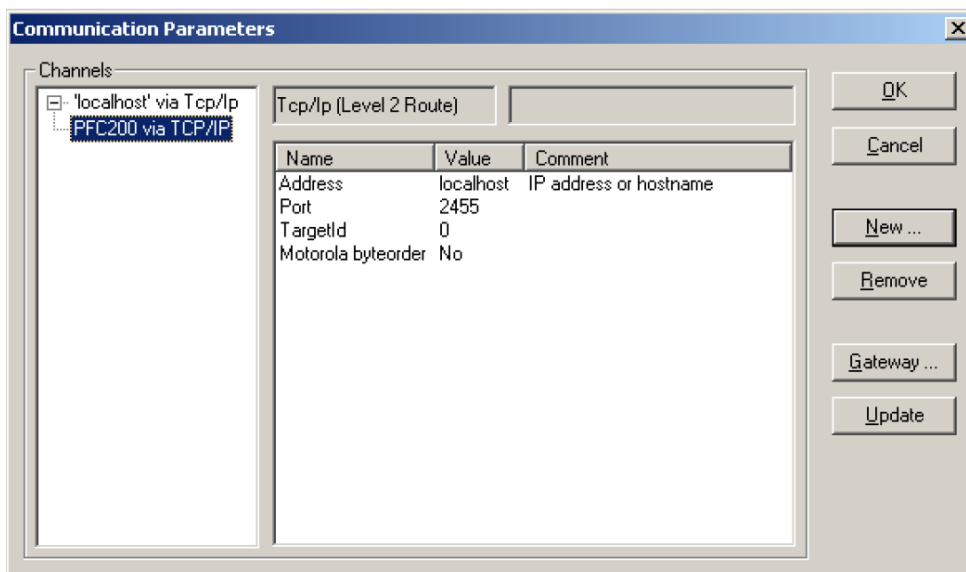
Ilustracja 75: Nawiązywanie połączenia komunikacyjnego – krok 1

3. W polu „Name” wpisać dowolną nazwę sterownika sieciowego i kliknąć „Tcp/Ip (Level 2 Route)”. Następnie potwierdzić za pomocą [OK].



Ilustracja 76: Nawiązywanie połączenia komunikacyjnego – krok 2

4. W oknie „Communication Parameters” w punkcie „Address” wpisać **adres IP sterownika sieciowego** i nacisnąć klawisz logowania na klawiaturze PC. Aby zamknąć okno, kliknąć [OK].
W celu wyboru sterownika, który został już utworzony, należy wybrać go w oknie po lewej, a następnie kliknąć [OK].



Ilustracja 77: Nawiązywanie połączenia komunikacyjnego – krok 3

5. Aby przesłać program PLC, kliknąć **Online** na pasku menu i wybrać **Login**.
6. Upewnić się, że przełącznik Run/Stop na sterowniku znajduje się w pozycji „Run”.
7. Uruchomić program PLC, klikając **Online > Start** na pasku menu.

9.2.6 Tworzenie projektu bootowalnego

Aby po restarcie sterownika program PLC mógł być automatycznie zainicjowany, należy utworzyć projekt bootowalny. Wybrać na pasku menu **Online > Create boot project**. Aby uruchomić tę funkcję, trzeba być zalogowanym w CODESYS.

Wskazówka Automatyczne ładowanie projektu bootowalnego



Projekt bootowalny można również automatycznie załadować przy uruchamianiu sterownika. Po kliknięciu zakładki „Resources” wystarczy otworzyć „Target Settings”. Następnie wybrać zakładkę „General” i „Load boot project automaticall”.

Jeśli projekt bootowalny (DEFAULT.PRG. DEFAULT.CHK) znajduje się już w katalogu /home/codesys, a przełącznik „Run/Stop” sterownika jest ustawiony na „Run”, sterownik rozpocznie automatycznie przetwarzanie programu PLC. Jeśli przełącznik jest ustawiony na „Stop”, program PLC nie uruchomi się.

Jeśli program PLC jest już uruchomiony w sterowniku, zadanie PLC rozpoczyna się od odczytania danych sieciowych (tylko w przypadku sterowników ze złączem sieci obiektowej), danych zintegrowanych wejść i wyjść oraz modułów I/O. Dane wyjściowe zmienione w programie PLC zostają zaktualizowane po przetworzeniu zadania PLC. Zmiana trybu pracy („Stop/Run”) następuje na końcu zadania PFC. Czas trwania cyklu obejmuje czas od rozpoczęcia programu PLC do kolejnego rozpoczęcia. Jeżeli w trakcie programu PLC realizowana jest większa pętla, to czas wykonywania zadania wydłuża się odpowiednio o . W tym czasie wejścia i wyjścia nie są aktualizowane. Te aktualizacje mają miejsce na końcu zadania PLC.

9.3 Sposób zapisywania adresów logicznych

Zgodnie z IEC 61131-3 dostęp do indywidualnych elementów pamięci jest możliwy tylko przy zastosowaniu następujących znaków:

Tabela 53: Sposób zapisywania adresów logicznych

Pozycja	Znak	Nazwa	Uwagi
1	%	Poprzedza adres absolutny	-
2	I	Input	
	Q	Output	
	M	Znaczniki	
3	X	Pojedynczy bit	Reprezentacja w obrazie procesu
	B	Bajt (8 bitów)	
	W	Słowo (16 bitów)	
	D	Podwójne słowo (32 bity)	
4		Adres	

Poniżej dwa przykłady:

Adres jako słowo %QW27 (28. słowo)

Adres jako bit %IX1.9 (10. bit w słowie 2)

Znaki w adresie absolutnym powinny być wpisane bez spacji. Pierwszy bit słowa ma adres 0.

9.4 Tworzenie zadań

W konfiguracji zadań należy wpisać charakterystykę czasową i priorytet poszczególnych zadań.

Wskazówka

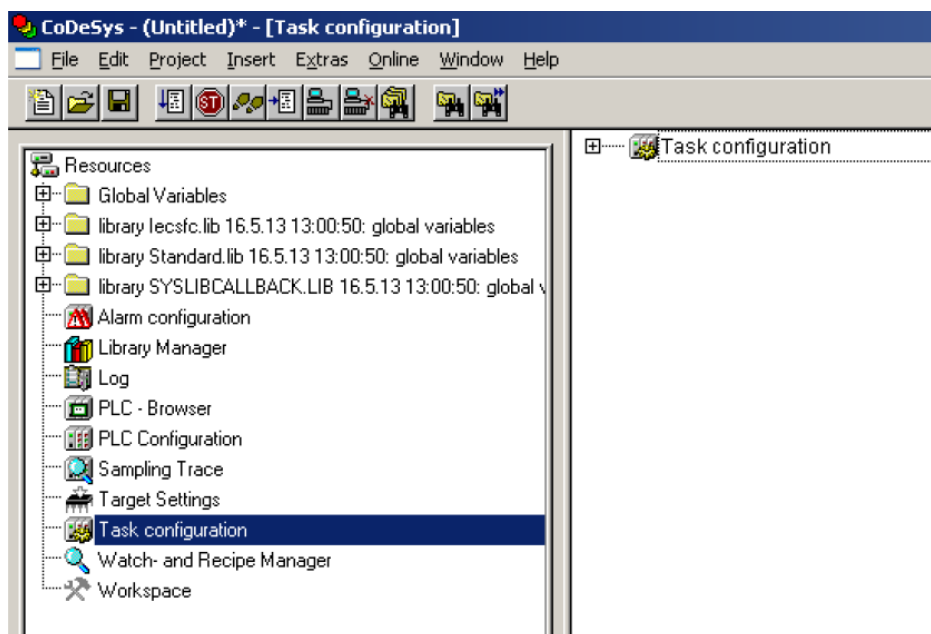
Watchdog



W programie aplikacyjnym bez konfiguracji zadań nie ma funkcji watchdog, monitorującej czas trwania cyklu programu (PLC_PRG).

Zadanie tworzy się w następujący sposób:

1. Otworzyć okno do konfiguracji zadań, klikając dwukrotnie węzeł „Task configuration” w zakładce „Resources”.



Ilustracja 78: Task configuration

2. Aby utworzyć zadanie, należy kliknąć prawym klawiszem myszy „Task configuration” i w menu kontekstowym wybrać „Attach task”.

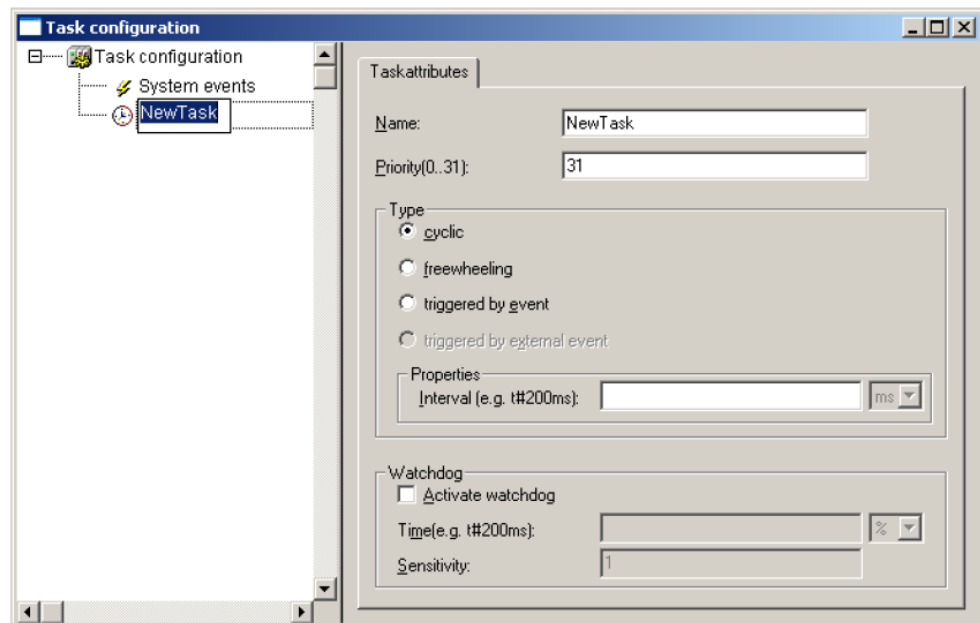
3. Aby przydzielić do zadania nową nazwę (np. PLC_Prog), należy kliknąć „New Task“. Następnie wybrać typ zadania. W tym przypadku przydzielono typ „cyclic“.

Wskazówka



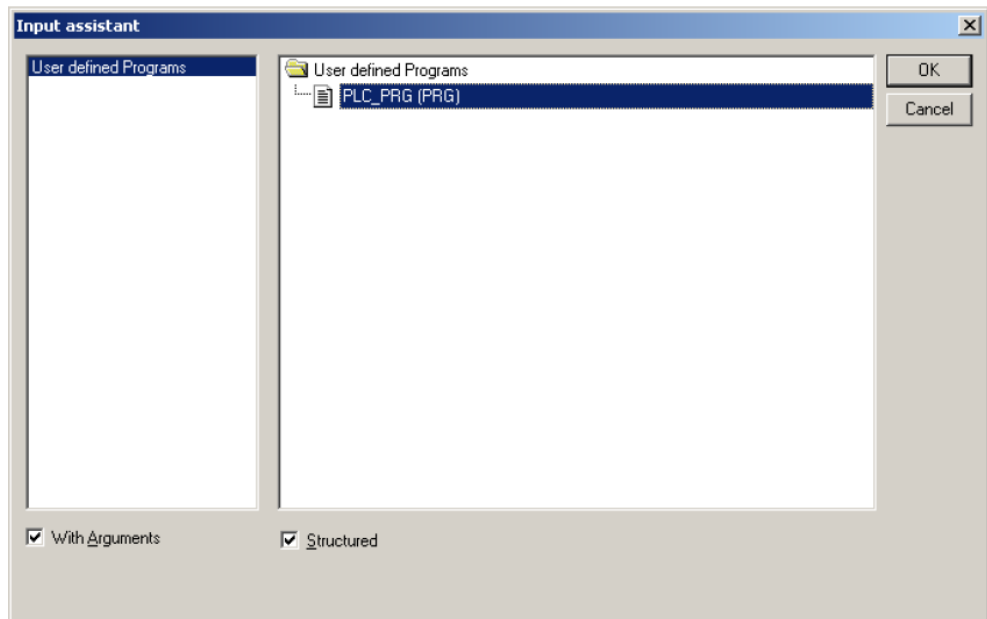
Uwzględnić czas trwania cyklu!

Minimalny czas trwania cyklu dla zadań zależnych od I/O wynosi 2 milisekundy!



Ilustracja 79: Zmiana nazwy zadania 1

4. Dodać utworzony wcześniej blok funkcyjny PLC_PRG (patrz rozdział „Edycja bloku funkcyjnego“). W tym celu należy kliknąć prawym przyciskiem myszy symbol zegara i wybrać w menu kontekstowym „Attach program call-up“. Następnie kliknąć przycisk [...] oraz [OK].

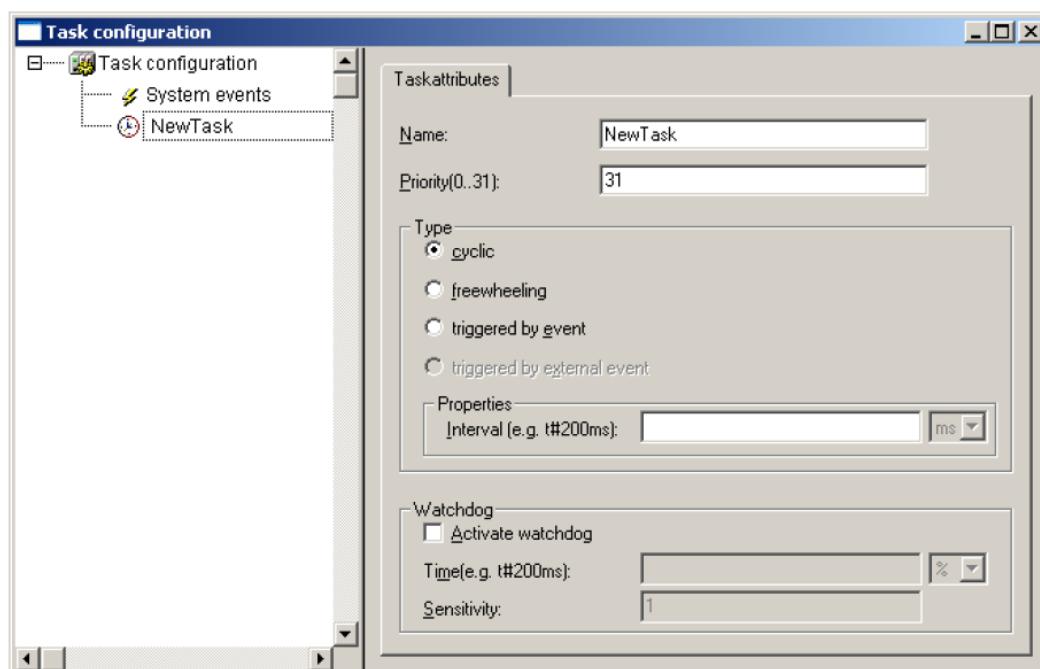


Ilustracja 80: Wywołanie dołączenia bloku funkcyjnego

5. Skompilować program, klikając **Project > Rebuild all** na pasku menu.

9.4.1 Zadania cykliczne

Dla każdego zadania można nadać priorytet, aby określić kolejność wykonywania zadań.



Ilustracja 81: Zadanie cykliczne

Wskazówka Kolejność wykonywania zadań



Priorytety przedstawione poniżej nie określają kolejności wykonywania zadań. Zadania są rozpoczynane w dowolnej kolejności.

Priorytet 0 ... 5:

Zadania o najwyższych priorytetach 0 ... 5 powinny dotyczyć ważnych operacji obliczeniowych i synchronicznych dostępu do obrazu procesu modułów I/O. Zadania te przetwarzane są zgodnie z numerem priorytetu i odpowiadają priorytetom LinuxRT -79 ... -74.

Priorytet 6 ... 20:

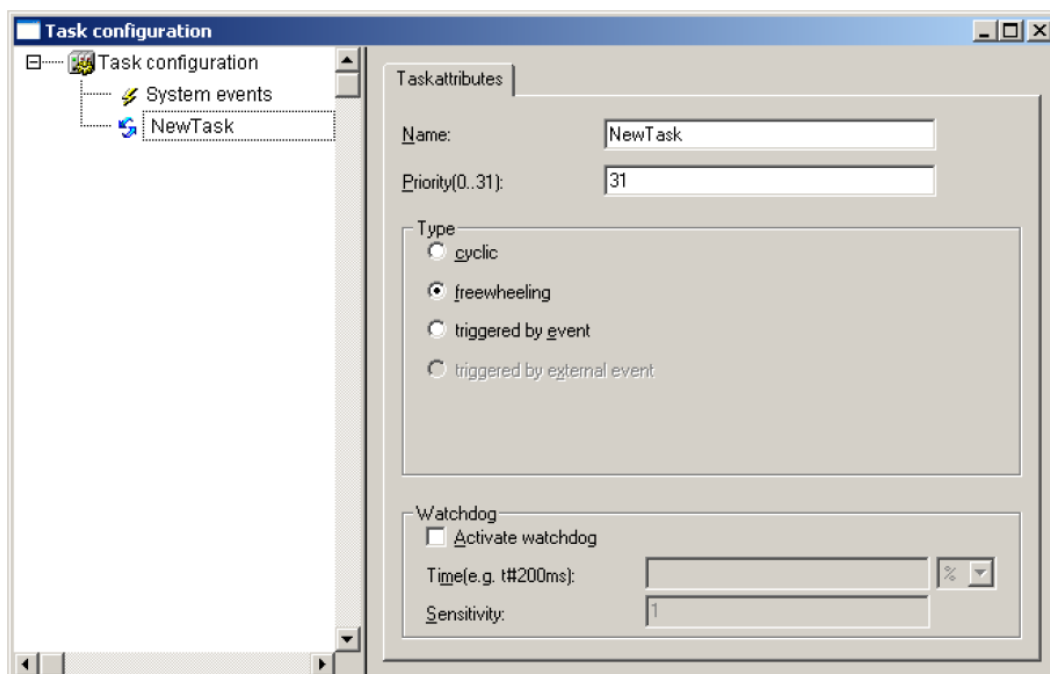
Zadania o średnich priorytetach 6 ... 20 powinny dotyczyć dostępu w czasie rzeczywistym, np. do sieci Ethernet i systemu plików lub danych sieci obiektowej i interfejsu RS-232 (jeśli istnieje). Zadania te przetwarzane są zgodnie z numerem priorytetu i odpowiadają priorytetom LinuxRT -40 ... -26.

Priorytet 21 ... 31:

Zadania o najniższych priorytetach 21 ... 31 powinny dotyczyć np. operacji obliczeniowych wymagających dłuższego okresu czasu lub niewymagających czasu rzeczywistego dostępu do sieci ETHERNET i systemu plików lub danych sieci obiektowej i interfejsu RS-232 (jeśli występuje). Między zadaniami priorytetów 21 ... 31 nie ma różnicowania kolejności wykonywania ze względu na numer priorytetu. W systemie operacyjnym otrzymują one taki sam czas przetwarzania (metoda „Completely Fair Scheduler“).

9.4.2 Zadania dowolne

Zadania dowolne nie są przetwarzane cyklicznie. Moment ich przetwarzania zależy jedynie od obciążenia systemu. Dlatego w przypadku zadań dowolnych pole „Priorytet (0 ... 31)” nie ma funkcji. Traktowane są one jak zadania o priorytecie 21 ... 31.



Ilustracja 82: Zadanie dowolne

Wskazówka



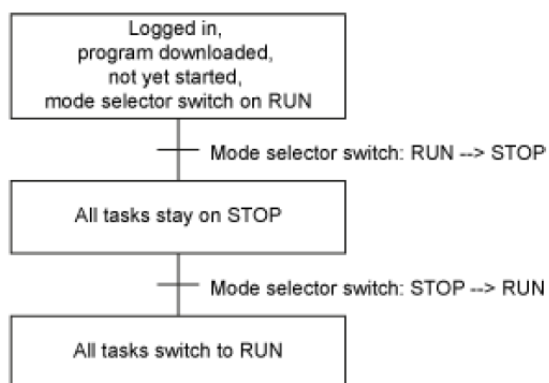
PLC-PRG jako zadanie dowolne bez konfiguracji zadania

Jeśli zadanie nie zostało skonfigurowane, program PLC_PRG wykonywany jest z najniższym priorytetem cyklicznie co 10 ms. Czas przebiegu zadania dowolnego nie jest monitorowany przez funkcję CODESYS watchdog.

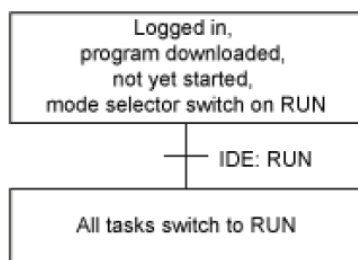
9.4.3 Debugowanie programu IEC

Jeśli program IEC jest sprawdzany za pomocą punktów wstrzymania (breakpoints), to rola przełącznika trybu pracy jest następująca:

Dopóki w punkcie wstrzymania nie będzie zadania, RUN i STOP z interfejsu użytkownika (IDE) i z przełącznika trybu pracy (BAS) oddziałują na wszystkie zadania (przypadek 1 i 2).

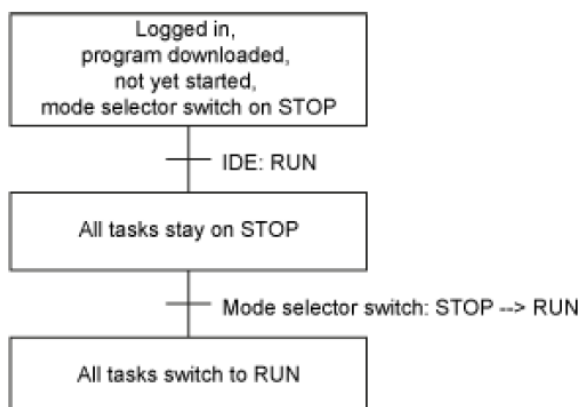


Ilustracja 83: Debugowanie (przypadek 1)

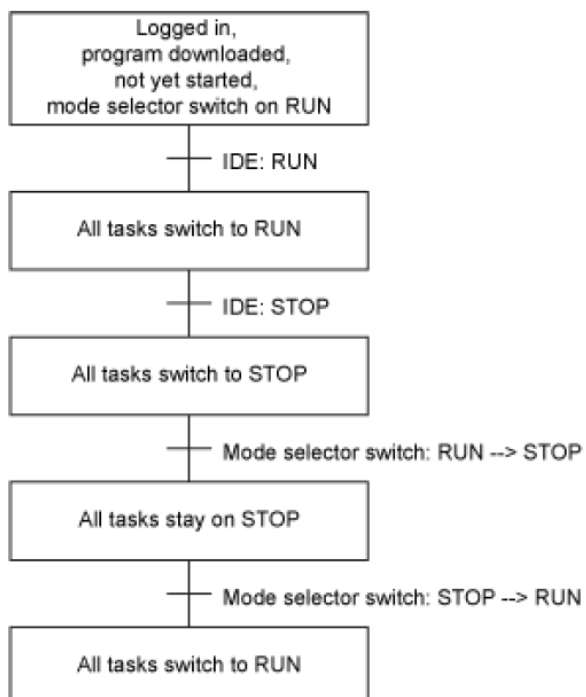


Ilustracja 84: Debugowanie (przypadek 2)

Przy równoczesnym wykorzystaniu przełącznika trybu pracy i funkcji STOP w interfejsie użytkownika pierwszeństwo mają wskazania przełącznika (przełącznik 3 i przełącznik 4).



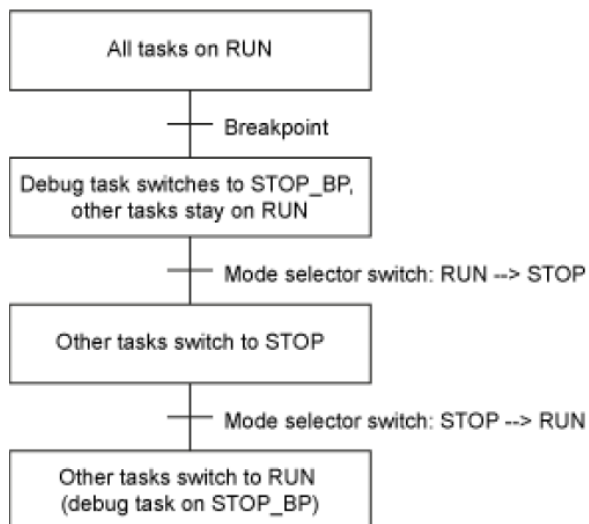
Ilustracja 85: Debugowanie (przypadek 3)



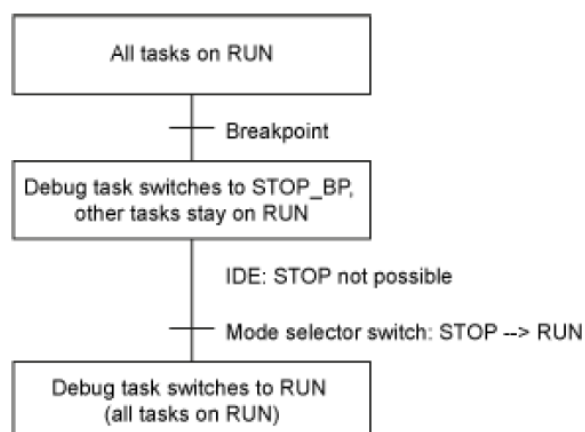
Ilustracja 86: Debugowanie (przypadek 4)

Jeśli w punkcie wstrzymania znajduje się zadanie, przełącznik trybu pracy może sterować wszystkimi innymi zadaniami.

Wyjątek: Jeśli przełącznik trybu pracy jest ustawiony na STOP, zadanie debugowania nie jest kontynuowane.



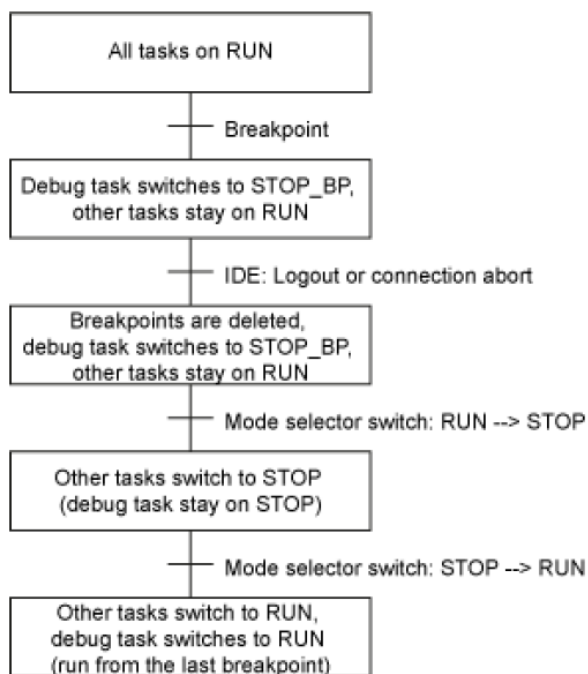
Ilustracja 87: Debugowanie (przypadek 5)



Ilustracja 88: Debugowanie (przypadek 6)

Jeśli w punkcie wstrzymania obecne jest zadania, a połączenie do IDE zostanie przerwane (np. przez wylogowanie), wówczas wszystkie punkty wstrzymania są usuwane.

Zadanie debugowania pozostaje na aktualnej pozycji do momentu ponownego przestawienia przełącznika trybu pracy z STOP na RUN. W tym przypadku zadanie jest kontynuowane z aktualnej pozycji (przypadek 7).

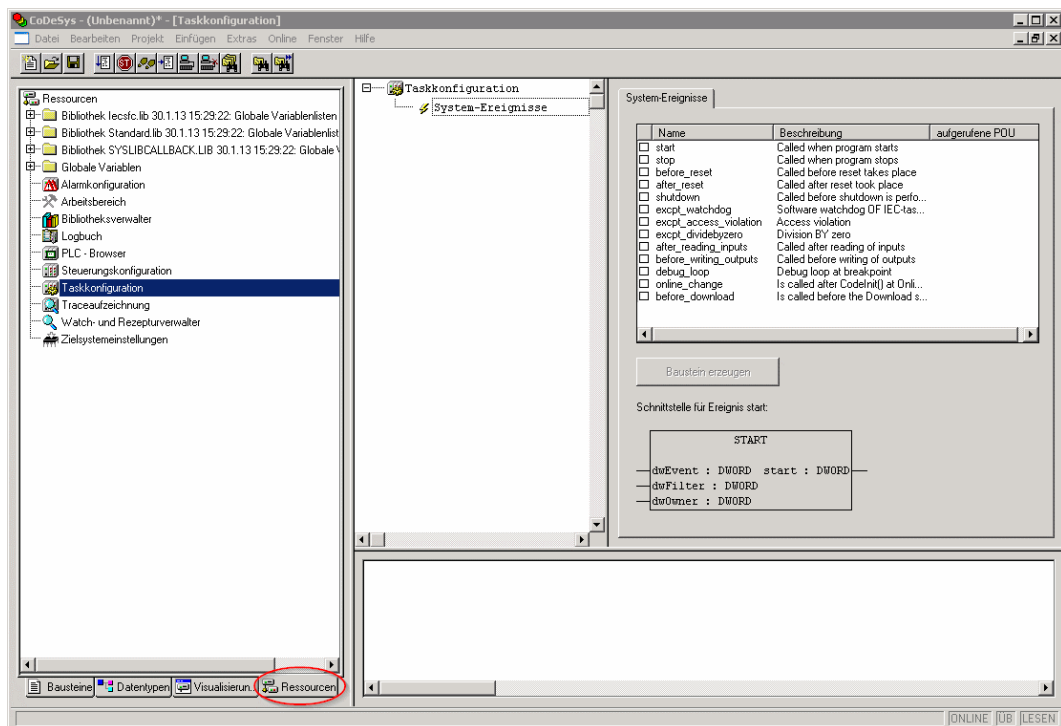


Ilustracja 89: Debugowanie (przypadek 7)

9.5 Zdarzenia systemowe

Przy konfiguracji zadań w CODESYS oprócz zadań cyklicznych można użyć także EventTasks. Te zadania wywoływane są w urządzeniu przy określonych zdarzeniach.

Aby aktywować Events i wprowadzić program, który ma być wywołany, należy w środowisku programistycznym CODESYS otworzyć w zakładce „Resources” okno „Task configuration”.



Ilustracja 90: CODESYS – System Events

Wskazówka



Nie stosować punktów debugowania w przetwarzaniu zdarzeń!

Punkty debugowania w obsłudze zdarzeń mogą spowodować trudne do przewidzenia błędy i z tego względu nie powinny być stosowane!

Można aktywować następujące zdarzenia:

Tabela 54: Events

Nazwa	Opis
start	Zdarzenie zostaje wywołane bezpośrednio po uruchomieniu programu aplikacyjnego.
stop	Zdarzenie zostaje wywołane bezpośrednio po zatrzymaniu programu aplikacyjnego.
before_reset	Zdarzenie zostaje wywołane bezpośrednio przed resetem programu aplikacyjnego.
after_reset	Zdarzenie zostaje wywołane bezpośrednio po resecie programu aplikacyjnego.
shutdown	Zdarzenie zostaje wywołane bezpośrednio przed zamknięciem systemu.
excpt_watchdog	Zdarzenie jest wywoływane, jeśli zostanie rozpoznany watchdog zadania.
excpt_access_violation	Zdarzenie zostaje wywołane, gdy rozpoznany zostanie błąd dostępu do zapisu w nieuprawnionym obszarze pamięci. (błędny Pointer, niewłaściwy index Array, niewłaściwy deskryptor pliku)
excpt_dividebyzero	Zdarzenie zostaje wywołane, gdy rozpoznane zostanie dzielenie przez zero
after_reading_inputs	To zdarzenie jest wyzwalane niezależnie od programu aplikacyjnego po odczytaniu wszystkich wejść.
before_writing_outputs	To zdarzenie jest wyzwalane niezależnie od programu aplikacyjnego przed zapisaniem wszystkich wyjść.
debug_loop	To zdarzenie jest wyzwalane przy każdym wywołaniu zadania, jeśli w tym zadaniu został osiągnięty punkt przerwania (braekpoint) i w rezultacie przetwarzanie tego zadania zostało zablokowane.
online_change	To zdarzenie zostaje wywołane po zainicjowaniu programu przy Online-Change.
before_download	To zdarzenie zostaje wywołane zawsze przed pobraniem danych z IDE do urządzenia.

Wskazówka



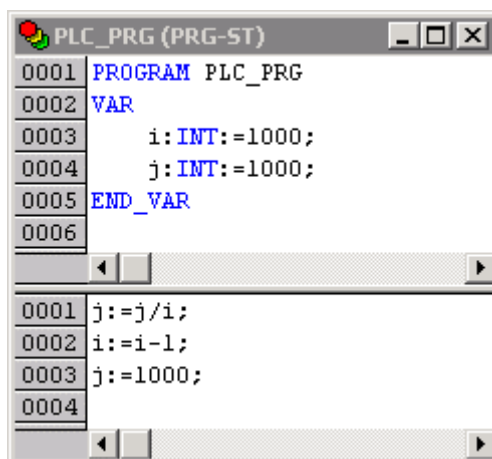
Przy niezdefiniowanej obsłudze zdarzeń aplikacja przechodzi w stan Stop!

Jeśli w systemie występują zdarzenia oznaczone jako „excpt” bez zdefiniowanej obsługi zdarzeń, aplikacja przechodzi w stan „Stop”.

9.5.1 Tworzenia obsługi zdarzeń

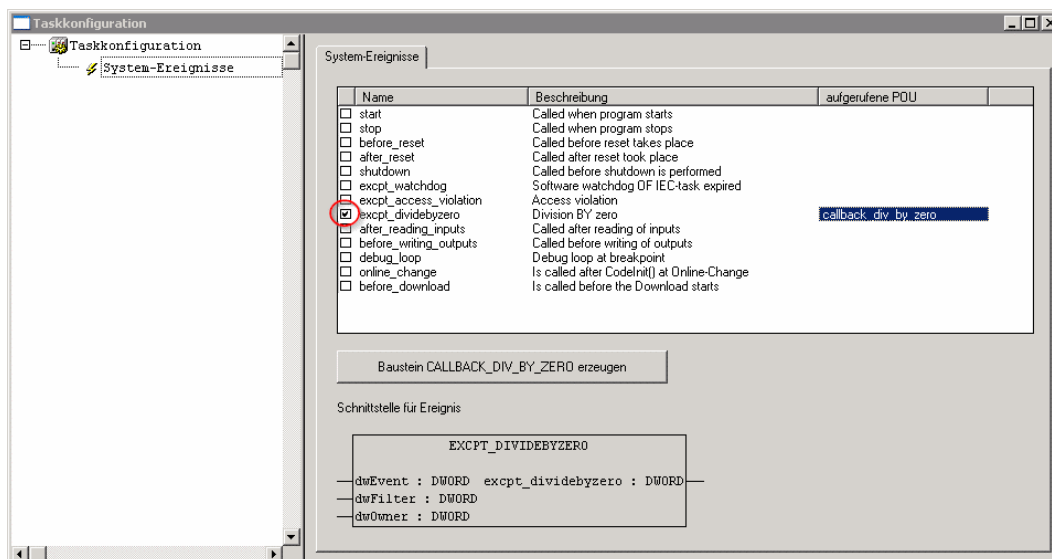
Poniższy przykład ilustruje sposób tworzenia i zastosowania zdarzeń.
W przykładzie zastosowano zdarzenie „excpt_dividebyzero”.

Najpierw w module PLC_PRG tworzony jest program, który wywołuje dzielenie przez 0.



Ilustracja 91: CODESYS – program wywołujący dzielenie przez „0”

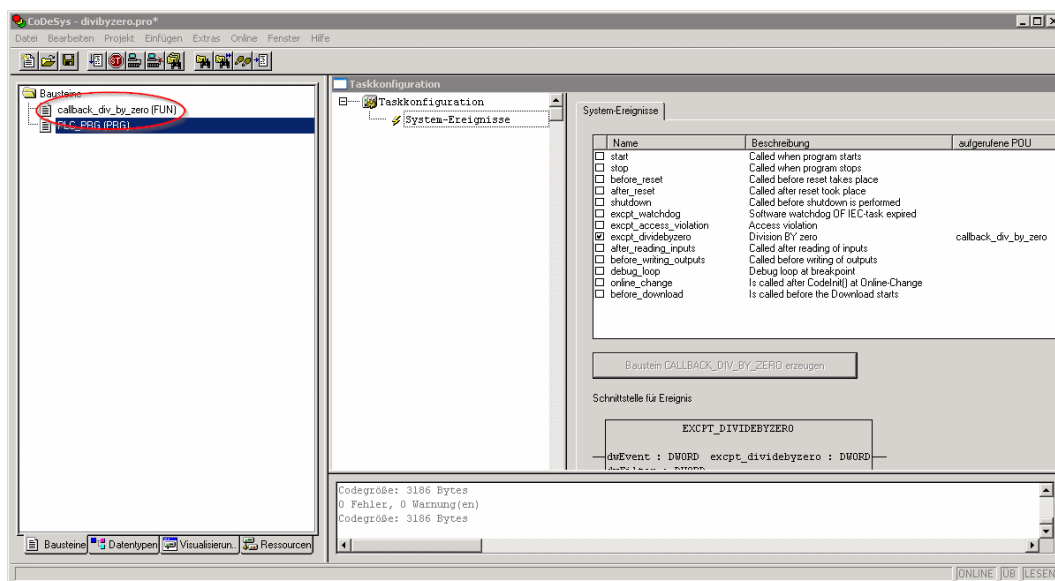
W konfiguratorze zadań aktywowane jest zdarzenie systemowe „excpt_dividebyzero” a w kolumnie „Called POU” zostaje wprowadzona nazwa zdarzenia do wygenerowania.



Ilustracja 92: CODESYS – tworzenie i aktywowanie zdarzeń

Aby wygenerować zdarzenie, należy kliknąć **[Generate CALLBACK_DIV_BY_ZERO function block]**.

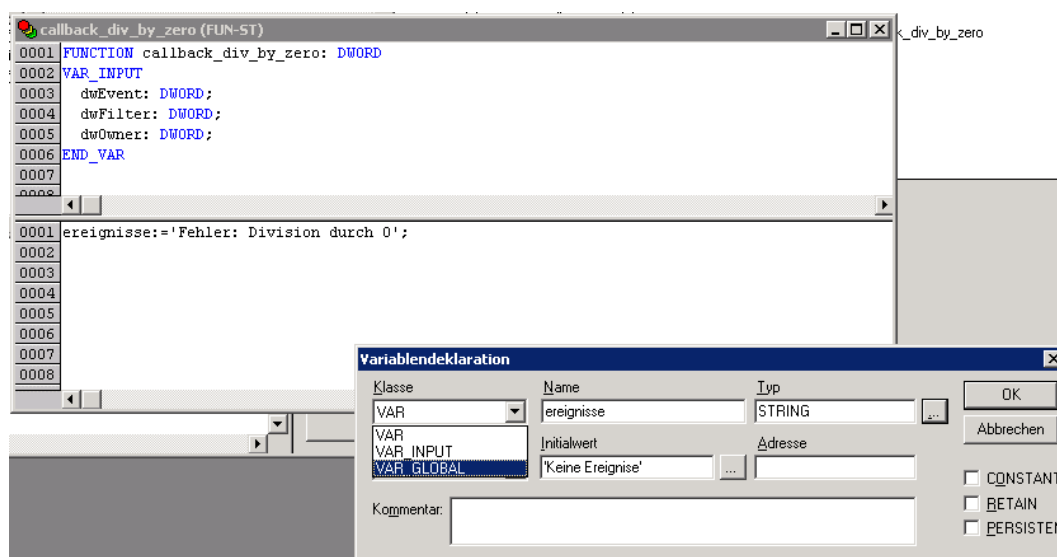
W efekcie tego w zakładce „Function blocks” pojawia się nowa funkcja o wybranej nazwie.



Ilustracja 93: CODESYS – wygenerowany nowy moduł

W nowej funkcji zaprogramowana jest obsługa tego zdarzenia.

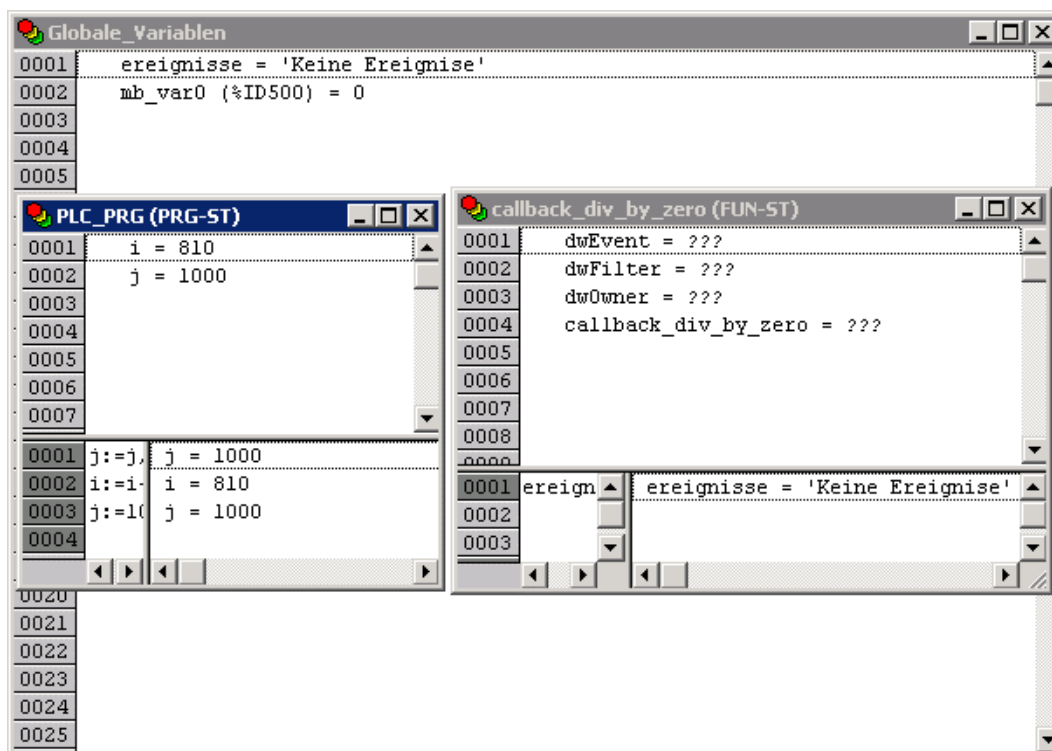
W tym przykładzie zdarzenie udokumentowane jest w zmiennej globalnej.



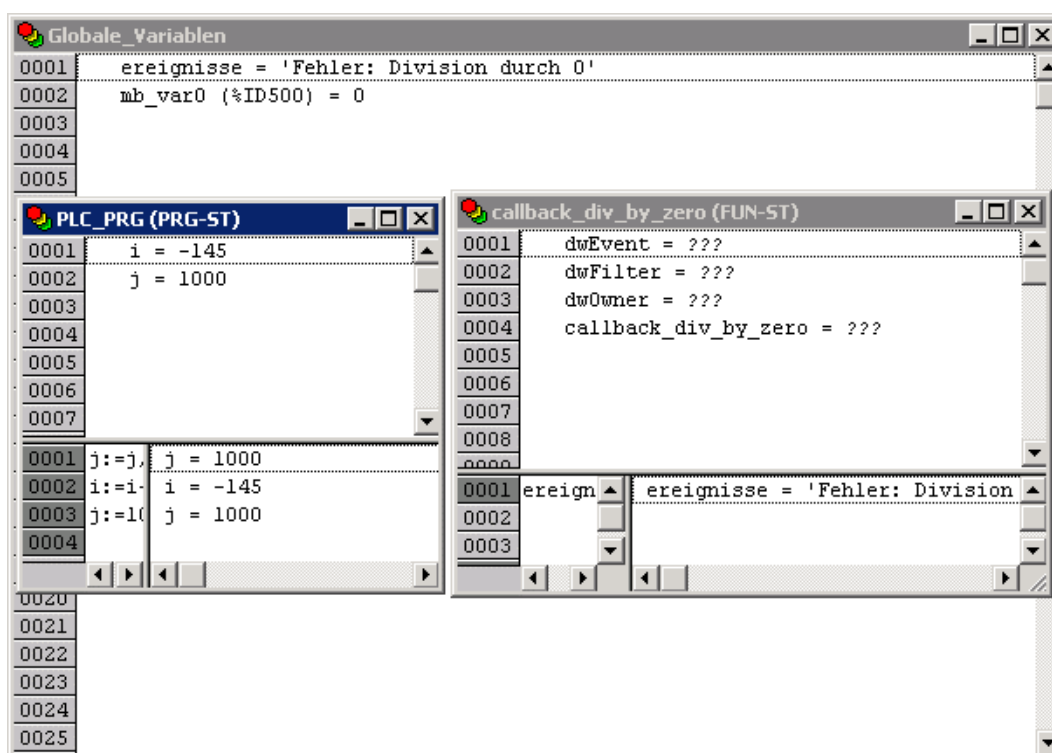
Ilustracja 94: CODESYS – zapisanie zdarzenia w zmiennych globalnych

Teraz można skompilować nowo utworzony projekt i załadować go do sterownika.

Po uruchomieniu wartość zmiennej „Events” zmieni się dopiero wtedy, gdy licznik „i” osiągnie 0 i zostanie wykonane dzielenie przez 0.



Ilustracja 95: CODESYS – zawartość zmiennych przed dzieleniem przez „0”

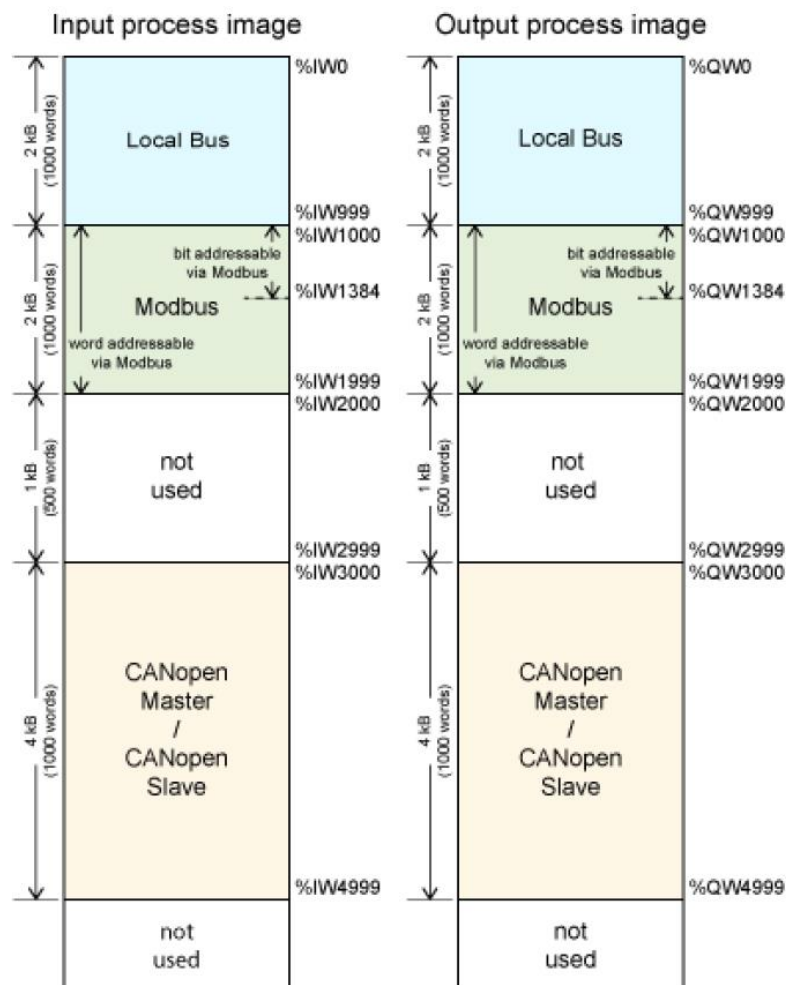


Ilustracja 96: CODESYS – zawartość zmiennych po dzieleniu przez „0”

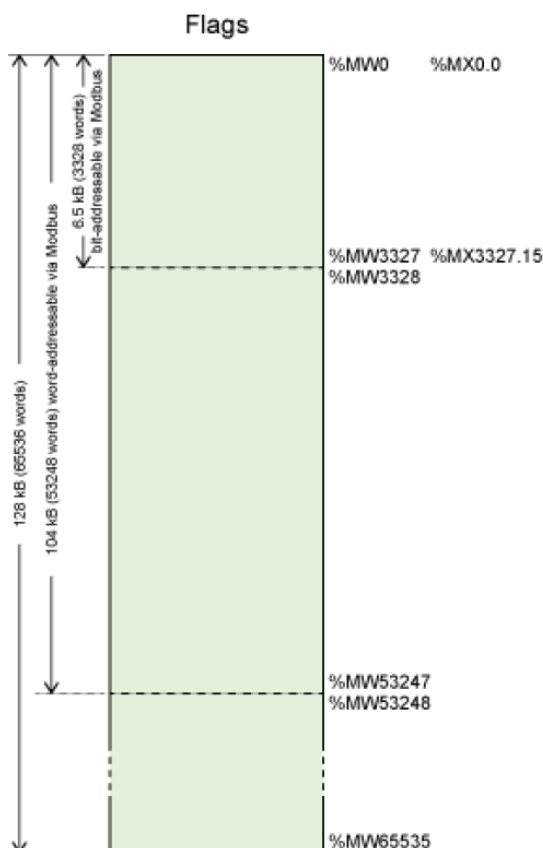
9.6 Obrazy procesu

Obraz procesu jest zakresem pamięci, w którym gromadzone są dane procesowe w zdefiniowanej kolejności. Składa się z modułów I/O podłączonych do magistrali

systemowej, zmiennych PFC, zakresu znaczników i urządzeń slave podłączonych do sieci obiektowej.



Ilustracja 97: Obraz procesu



Ilustracja 98: Zakres znaczników

9.6.1 Obraz procesu dla modułów I/O podłączonych do sterownika

Po uruchomieniu sterownik automatycznie rozpoznaje wszystkie podłączone moduły I/O.

W obrazie procesu najpierw zapisywane są analogowe dane wejściowe i wyjściowe w postaci słowa. Po nich następują bity dwustanowych danych wejściowych i wyjściowych złożone do postaci słowa.

Wielkość i budowa obrazu procesu dla poszczególnych modułów I/O została opisana w załączniku.

Wskazówka



Reprezentacja modułów I/O w obrazie procesu

Reprezentacja modułu I/O w obrazie procesu może leżeć w zakresie od 0 do 48 bajtów.

Wskazówka



Budowa danych procesowych modułów I/O

Należy sprawdzić dane procesowe modułów I/O w przypadku dodawania ich lub usuwania ze sterownika: zmiana topologii modułów I/O powoduje przesunięcia w obrazie procesu, ponieważ zmieniają się też adresy danych procesowych.

9.6.2 Obraz procesu dla urządzeń slave podłączonych do sieci obiektowej

Wielkość i budowa obrazu procesu dla podłączonych urządzeń slave została opisana w rozdziale dotyczącym konkretnej sieci obiektowej.

Wskazówka



Brak bezpośredniego dostępu z sieci obiektowej do obrazu procesu modułów I/O!

Potrzebne dane z obrazu procesu magistrali systemowej muszą być wyraźnie zmapowane w programie sterującym na dane w obrazie procesu sieci obiektowej i na odwrót! Bezpośredni dostęp nie jest możliwy!

9.7 Dostęp do obrazów procesu danych wejściowych i wyjściowych przez CODESYS 2.3

Poniższe tabele przedstawiają możliwości, dzięki którym można uzyskać dostęp do zakresów adresów obrazu procesu dla wejść i wyjść podłączonych do magistrali systemowej.

Tabela 55: Dostęp do obrazów procesu danych wejściowych i wyjściowych – magistrala systemowa

Obszar zapisu	Opis	Dostęp przez PLC	Zakres adresów logicznych
Obraz procesu wejść – magistrala systemowa	Obraz lokalnego modułu wejść (magistrala systemowa, moduły I/O 1 do 64*) w RAM.	Odczyt	Słowo %IW0 do %IW999
			Bajt %IB0 do %IB1999
Obraz procesu wyjść – magistrala systemowa	Obraz lokalnego modułu wyjść (magistrala systemowa, moduły I/O 1 do 64*) w RAM.	Odczyt/zapis	Słowo %QW0 do %QW999
			Bajt %QB0 do %QB1999

* Przy użyciu modułu przedłużacza magistrali systemowej WAGO można podłączyć nawet 250 modułów I/O.

Tabela 56: Dostęp do obrazów procesu danych wejściowych i wyjściowych – Modbus

Obszar zapisu	Opis	Dostęp przez PLC	Zakres adresów logicznych
Obraz procesu wejść Modbus	Zmienne wejściowe Modbus, adresowanie w postaci słowa przez Modbus	Odczyt	Słowo %IW1000 do %IW1999
			Bajt %IB2000 do %IB3999
Obraz procesu wyjść Modbus	Zmienne wyjściowe Modbus, adresowanie w postaci słowa przez Modbus	Odczyt/zapis	Bit %QX1000.0 ... %QX1000.15 do %QX1384.0 ... %QX1384.15
			Słowo %QW1000 do %QW1999
Obraz procesu wejść Modbus	Zmienne wejściowe Modbus, adresowanie bitowe przez Modbus	Odczyt	Bit %IX1000.0 ... %IX1000.15 do %IX1384.0 ... %IX1384.15
			Słowo %QW1000 do %QW1999
Obraz procesu wyjść Modbus	Zmienne wyjściowe Modbus, adresowanie bitowe przez Modbus	Odczyt/zapis	Bit %QX1000.0 ... %QX1000.15 do %QX1384.0 ... %QX1384.15
			Słowo %QW1000 do %QW1999

Tabela 57: Dostęp do obrazów procesu danych wejściowych i wyjściowych – CANopen

Obszar zapisu	Opis	Dostęp przez PLC	Zakres adresów logicznych
Obraz procesu wejść CANopen	Zmienne wejściowe CANopen master lub CANopen slave	Odczyt	Słowo %IW3000 do %IW4999
			Bajt %IB6000 do %IB9999
Obraz procesu wyjść CANopen	Zmienne wyjściowe CANopen master lub CANopen slave	Odczyt/zapis	Słowo %QW3000 do %QW4999
			Bajt %QB6000 do %QB9999

Tabela 58: Dostęp do obrazów procesu danych wejściowych i wyjściowych – znaczniki

Obszar zapisu	Opis	Dostęp przez PLC	Zakres adresów logicznych
Zmienne znaczników	Łącznie 128 kB pamięci nieulotnej (65536 słów).	Odczyt/zapis	%MW0 do %MW65535
	104 kB adresowanie w postaci słowa przez Modbus (53248 słów)	Odczyt/zapis	Słowo (Modbus) %MW0 do %MW53247
	6,5 kB adresowanie bitowe przez Modbus (3328 słów).	Odczyt/zapis	Bit (Modbus) %MX0.0 ... %MX0.15 do %MX3327.0 ... %MX3327.15
Zmienne nieulotne	Symboliczne adresowana pamięć nieulotna w NVRAM: 128 kB	Odczyt/zapis	-

* Przy użyciu modułu przedłużacza magistrali systemowej WAGO można podłączyć nawet 250 modułów I/O.

Całkowita wielkość pamięci dla zmiennych znaczników i nieulotnych wynosi maksymalnie 128 kB (131060 bajtów). Wielkości obu zakresów mogą być w razie potrzeby dostosowywane, dopóki całkowita wielkość nie zostanie przekroczona. Przy zastosowaniu adresowania bitowego należy pamiętać, że adres bazowy ma postać słowa. Bity adresowane są od 0 do 15.

9.8 Przykład adresowania

Poniższy przykład adresowania ilustruje dostęp do obrazu procesu:

Tabela 59: Przyporządkowanie modułów I/O na potrzeby przykładu adresowania

Sterownik	750-400	750-554	750-402	750-504	750-454	750-650	750-468	750-600
	1	2	3	4	5	6	7	8

Tabela 60: Przyporządkowanie modułów I/O na potrzeby przykładu adresowania

Moduł I/O		Dane wejściowe		Dane wyjściowe		Opis
Typ	C					
750-400	1		%IX8.0			2DI, 24 V, 3 ms: 1. Moduł wejść dwustanowych z reprezentacją w obrazie procesu w postaci 2 bitów. Ponieważ moduły wejść analogowych zajmują już pierwszych 8 słów obrazu procesu wejść, te 2 bity zajmują najniższe bity 8. słowa.
	2		%IX8.1			
750-554	1			%QW0		2AO, 4 – 20 mA: 1. Moduł wyjść analogowych z reprezentacją w obrazie procesu w postaci 2 słów. W obrazie procesu wyjść zajmują one pierwsze 2 słowa.
	2			%QW1		
750-402	1		%IX8.2			4DI, 24 V: 2. Moduł wejść dwustanowych z reprezentacją w obrazie procesu w postaci 4 bitów. Dołączane są one do 2 bitów modułu 750-400 i umieszczone w 8. słowie obrazu procesu.
	2		%IX8.3			
	3		%IX8.4			
	4		%IX8.5			
750-504	1				%QX4.0	4DO, 24 V: 1. Moduł wyjść dwustanowych z reprezentacją w obrazie procesu w postaci 4 bitów. Ponieważ moduły wyjść analogowych zajmują już pierwsze 4 słowa obrazu procesu wyjść, te 4 bity zajmują najniższe bity 4. słowa.
	2				%QX4.1	
	3				%QX4.2	
	4				%QX4.3	
750-454	1	%IW0				2AI, 4 – 20 mA: 1. Moduł wejść analogowych z reprezentacją w obrazie procesu w postaci 2 słów. W obrazie procesu wejść zajmują one pierwsze 2 słowa.
	2	%IW1				
750-650	1	%IW2				RS232, C 9600/8/N/1: Moduł interfejsu szeregowego jest modułem wejść i wyjść analogowych, który przedstawiany jest w postaci 2 słów zarówno w obrazie procesu wejść jak i wyjść.
		%IW3				
				%QW2		
				%QW3		
750-468	1	%IW4				4AI, 0 – 10 V S.E: 2. Moduł wejść analogowych z reprezentacją w obrazie procesu w postaci 4 słów. Ponieważ moduły wejść i wyjść analogowych 750-454 i 750-650 zajmują już pierwsze 4 słowa obrazu procesu wejść, te 4 słowa tych
	2	%IW5				
	3	%IW6				

Tabela 60: Przyporządkowanie modułów I/O na potrzeby przykładu adresowania

Moduł I/O		Dane wejściowe		Dane wyjściowe		Opis
Typ	C*					
	4	%IW7				modułów I/O są dodawane za innymi.
750-600						Moduł końcowy Pasywny moduł końcowy 750-600 nie transmituje żadnych danych.

☐ Moduł wejść i wyjść analogowych
☐ Moduł wejść i wyjść dwustanowych

*C: Numer wejścia/wyjścia

9.9 Synchronizacja magistrali systemowej

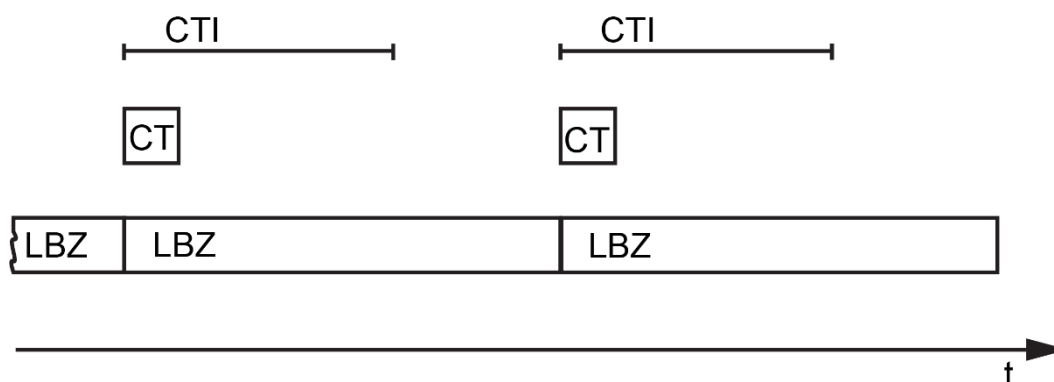
Cykle magistrali systemowej i zadań CODESYS są w sposób optymalny automatycznie synchronizowane: zależnie od liczby zamontowanych modułów I/O i najszybszego ustawionego cyklu zadań CODESYS sterownika. Przy synchronizacji mogą występować opisane niżej przypadki.

Pod pojęciem zadania CODESYS rozumiane są w tym rozdziale tylko zadania wewnątrz środowiska CODESYS, które zawierają dostęp do magistrali systemowej. Zadania bez dostępu do magistrali systemowej nie są synchronizowane. Więcej informacji na ten temat zawiera rozdział „Tworzenie zadań”.

9.9.1 Przypadek 1: Interwał zadania CODESYS mniejszy od cyklu magistrali systemowej

Wykonanie zadań CODESYS synchronizowane jest z czasem cyklu magistrali systemowej.

Zadanie CODESYS przetwarzane jest równocześnie z cyklem magistrali systemowej. Interwał zadania CODESYS zostaje przedłużony do czasu trwania cyklu magistrali systemowej. Jest to konieczne, aby w momencie rozpoczęcia zadania CODESYS wykorzystane były nowe dane wejściowe magistrali systemowej i po zakończeniu każdego zadania CODESYS na modułach I/O zostały ustawione wartości wyjściowe.



Ilustracja 99: Synchronizacja magistrali systemowej (przypadek 1)

CTI: Interwał zadania CODESYS (CODESYS Task Intervall)
CT: Zadanie CODESYS (CODESYS Task), mające dostęp do modułów I/O magistrali systemowej
LBZ: Cykl magistrali systemowej (Local Bus Cycle)

Przykład:

Interwał zadania CODESYS (CTI): 100 μ s

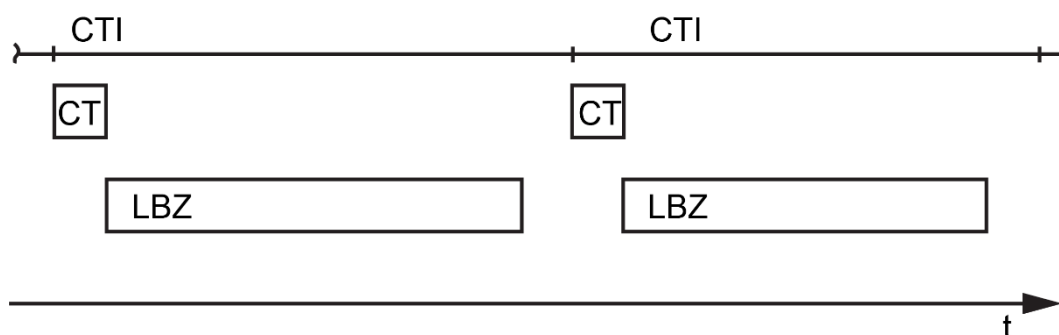
Cykl magistrali systemowej (LBZ): 2000 μ s

Efekt: Dopasowanie interwału zadania CODESYS do cyklu magistrali systemowej: 2000 μ s.

9.9.2 Przypadek 2: Interwał zadania CODESYS mniejszy od podwójnego cyklu magistrali systemowej

Wykonanie cyklu magistrali systemowej synchronizowane jest z ustawionym interwałem zadań CODESYS.

Na końcu zadania CODESYS rozpoczyna się cykl magistrali systemowej, który przetwarzany jest synchronicznie do najszybszego zadania CODESYS. W ten sposób zapewnione zostaje, że w momencie rozpoczęcia zadania CODESYS udostępnione zostają aktualne dane wejściowe magistrali systemowej, a wartości wyjściowe każdego zadania CODESYS zostają ustawione na modułach I/O.



Ilustracja 100: Synchronizacja magistrali systemowej (przypadek 2)

CTI: Interwał zadania CODESYS (CODESYS Task Intervall)

CT: Zadanie CODESYS (CODESYS Task), mające dostęp do modułów I/O magistrali systemowej

LBZ: Cykl magistrali systemowej (Local Bus Cycle)

Przykład:

Interwał zadania CODESYS (CTI): 2500 μ s

Cykl magistrali systemowej (LBZ): 2000 μ s

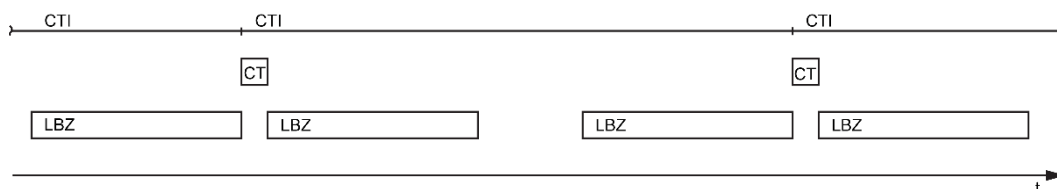
Efekt: Wykonanie cyklu magistrali systemowej co 2500 μ s.

9.9.3 Przypadek 3: Interwał zadania CODESYS większy od podwójnego cyklu magistrali systemowej

Dane I/O magistrali systemowej aktualizowane są jednym razem przed zadaniem CODESYS, a innym razem po zadaniu CODESYS.

Przed przetworzeniem zadania CODESYS wykonywany jest cykl magistrali systemowej, który udostępnia aktualne dane wejściowe dla zadania CODESYS. Po wykonaniu zadania CODESYS rozpoczynany jest kolejny cykl magistrali systemowej, który udostępnia aktualne dane wyjściowe na modułach I/O.

W ten sposób zapewnione zostaje, że w momencie rozpoczęcia zadania CODESYS udostępnione zostają aktualne dane wejściowe magistrali systemowej, a wartości wyjściowe każdego zadania CODESYS zostają szybko ustawione na modułach I/O. Równocześnie przy przetwarzaniu cykli magistrali systemowej unika się nadmiernie długiego czasu obliczeniowego CPU.



Ilustracja 101: Synchronizacja magistrali systemowej (przypadek 3)

CTI: Interwał zadania CODESYS (CODESYS Task Intervall)

CT: Zadanie CODESYS (CODESYS Task), mające dostęp do modułów I/O magistrali systemowej

LBZ: Cykl magistrali systemowej (Local Bus Cycle)

Przykład:

Interwał zadania CODESYS (CTI): 5000 μ s

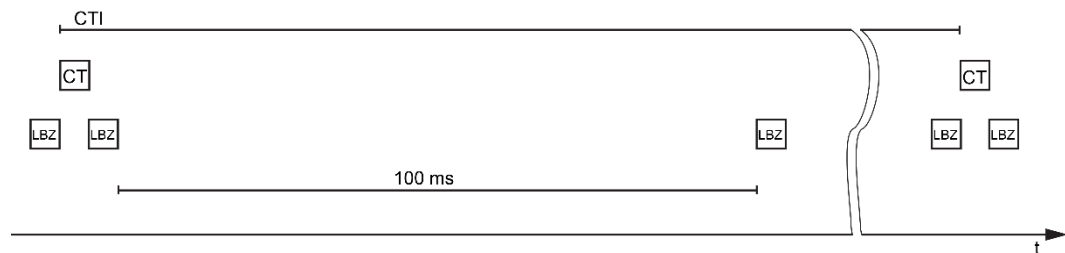
Cykl magistrali systemowej (LBZ): 2000 μ s

Efekt: Wykonanie cyklu magistrali systemowej 2000 μ s raz przed zadaniem CODESYS i raz bezpośrednio po zadaniu CODESYS.

9.9.4 Przypadek 4: Interwał zadania CODESYS większy niż 10 ms

Synchronizacja odbywa się tak samo jak w przypadku 3, jednak po 100 ms moduły wyjść byłyby resetowane do stanu domyślnego bez wykonania cyklu magistrali systemowej. Aby temu zapobiec, należy zapewnić, że cykl magistrali systemowej jest zawsze wykonywany po co najmniej 10 ms.

Dane I/O magistrali systemowej aktualizowane są jednym razem przed zadaniem CODESYS, a innym razem po zadaniu CODESYS i dodatkowo co 10 ms wykonywany jest kolejny cykl magistrali systemowej.



Ilustracja 102: Synchronizacja magistrali systemowej (przypadek 4)

CTI: Interwał zadania CODESYS (CODESYS Task Intervall)
CT: Zadanie CODESYS (CODESYS Task), mające dostęp do modułów I/O magistrali systemowej
LBZ: Cykl magistrali systemowej (Local Bus Cycle)

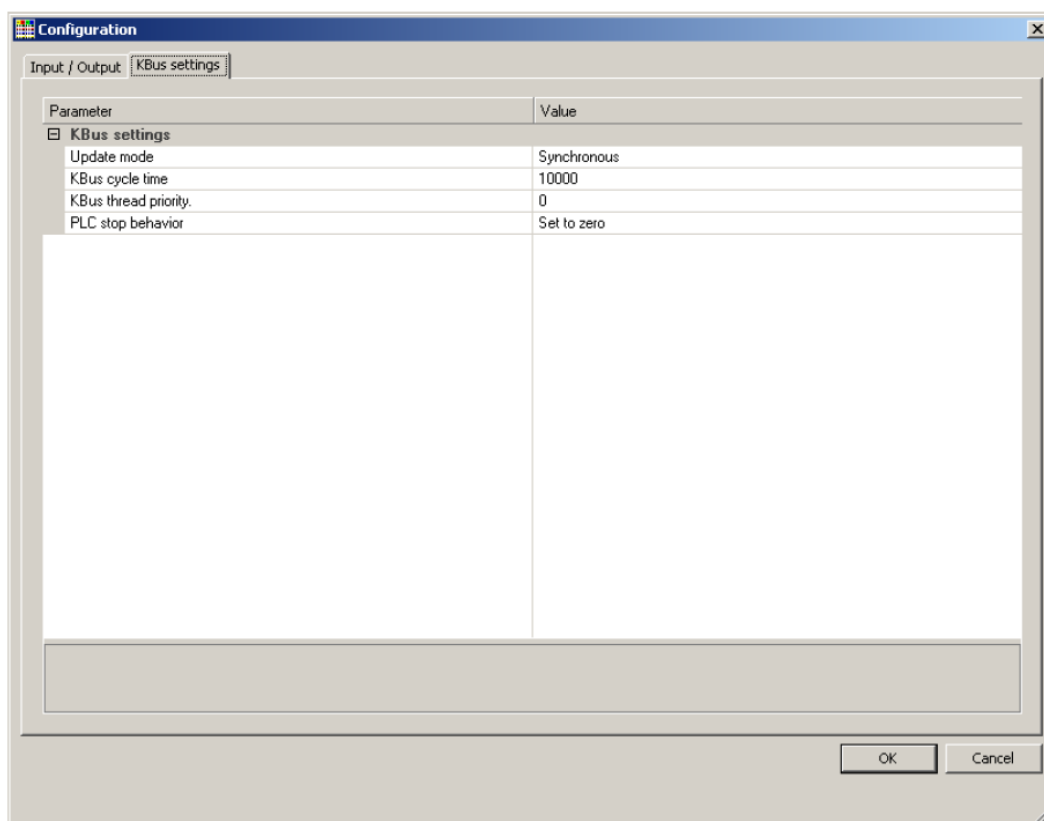
Przykład:

Interwał zadania CODESYS (CTI): 150000 μ s

Cykl magistrali systemowej (LBZ): 2000 μ s

Efekt: Wykonanie cyklu magistrali systemowej 2000 μ s raz przed zadaniem CODESYS, raz bezpośrednio po zadaniu i 10 ms po ostatnim cyklu magistrali systemowej

9.9.5 Konfiguracja magistrali systemowej



Ilustracja 103: Ustawienia magistrali systemowej

Tabela 61: Ustawienia magistrali systemowej

Parametr	Znaczenie	
Update mode	Za pomocą tego trybu konfiguruje się aktualizację danych procesowych magistrali systemowej.	
	Asynchroniczny	W trybie asynchronicznym dane procesowe aktualizowane są cyklicznie w ustawionych interwałach czasowych.
	Synchroniczny *	W trybie synchronicznym aktualizacja danych procesowych synchronizowana jest z najszybszym zadaniem CODESYS, które ma dostęp do magistrali systemowej.
KBus cycle time	Czas trwania cyklu określa interwał aktualizacji magistrali systemowej. To ustawienie aktywne jest tylko w asynchronicznym trybie pracy.	
	1000 µs	Minimalna wartość wynosi 1 milisekundę.
	10000 µs*	Standardowa wartość wynosi 10 milisekund.
	50000 µs	Maksymalna wartość wynosi 50 milisekund.
KBus thread priority	Podaje priorytet aktualizacji wątku KBus. To ustawienie aktywne jest tylko w asynchronicznym trybie pracy. Priorytet ten odpowiada priorytetowi cyklicznych zadań CODESYS (patrz rozdział „Zadania cykliczne”). To ustawienie aktywne jest tylko w asynchronicznym trybie pracy.	
	0*	Najwyższy priorytet
	15	Najniższy priorytet
PLC stop behavior	Określa reakcję wyjść magistrali systemowej przy zatrzymaniu aplikacji PLC.	
	Zatrzymanie ostatniej wartości	Stan wyjść zostaje utrzymany.
	Ustawienie na zero*	Wyjścia ustawiane są na zero.

* ustawienie standardowe

9.9.5.1 Oddziaływanie trybu Update na zadania CODESYS

9.9.5.1.1 Asynchroniczny tryb Update

W asynchronicznym trybie Update nie ma bezpośredniego oddziaływania na zadania CODESYS.

Wskazówka



Zanik magistrali systemowej przy konflikcie priorytetów!

W asynchronicznym trybie Update istnieje niebezpieczeństwo, że magistrala systemowa zaniknie, gdyż Thread pracuje na tych samych priorytetach co zadania IEC. Aby temu zapobiec, priorytet Thread magistrali systemowej musi być wyższy od zadań IEC.

9.9.5.1.2 Synchroniczny tryb Update

W synchronicznym trybie Update przebieg zadań CODESYS może być determinowany przez magistralę systemową. Minimalny osiągalny interwał zadania jest zależny od czasu trwania cyklu magistrali systemowej, przy czym czas trwania cyklu magistrali systemowej zależy od podłączonych modułów I/O. Zasadniczo: im krótsza magistrala systemowa, tym krótszy czas cyklu, a dwustanowe moduły I/O są szybsze niż moduły analogowe lub systemowe.

W przypadku błędu magistrali systemowej zadania CODESYS zostają zablokowane na tak długo, aż błąd zostanie usunięty, tzn. cykl magistrali systemowej będzie kontynuowany.

Wskazówka



Nie można wywołać statusu magistrali systemowej przy błędzie magistrali systemowej!

Jeśli wystąpił błąd magistrali systemowej, w synchronicznym trybie Update nie funkcjonuje wywołanie statusu magistrali systemowej za pomocą `KBUS_ERROR_INFORMATION (mod_com.lib)`.

9.10 Ustawienia pamięci w CODESYS

Poniższa lista przedstawia podział pamięci w PFC200:

- Pamięć programu: 16 MB (maks.)
- Pamięć danych: 64 MB
- Dane wejściowe: 64 kB
- Dane wyjściowe: 64 kB
- Znaczniki: 24 kB
- Retain: 104 kB
- Ograniczenie modułu: $12 * 4096 \text{ B} = 48 \text{ kB}$

9.10.1 Pamięć programu

Pamięci programu (także pamięci kodu) nie można skonfigurować i jest ona ograniczona do maksymalnie 16 MB. Faktycznie wykorzystywana wielkość pamięci zależy od aplikacji.

The image shows a 'Target Settings' dialog box with a 'Configuration' dropdown and tabs for 'Target Platform', 'Memory Layout', 'General', 'Network functionality', and 'Visualization'. The 'Memory Layout' tab is active, displaying a table with columns 'Base' and 'Size'. The 'Code' row is highlighted with a red rectangle. Below the table, there are fields for 'Total size of data memory' and 'Maximum number of POU's'. At the bottom are 'Default', 'OK', and 'Cancel' buttons.

Base	Size
Code :	16#1000000
Global :	16#4000000 per segment
Memory :	16#2000
Input :	16#10000
Output :	16#10000
Retain:	16#1E000

Total size of data memory: 16#400C000

Maximum number of POU's: 4096

Ilustracja 104: Pamięć programu (przykład)

9.10.2 Pamięć danych i ograniczenie modułu

Pamięć danych ustawiona jest fabrycznie na 64 MB.

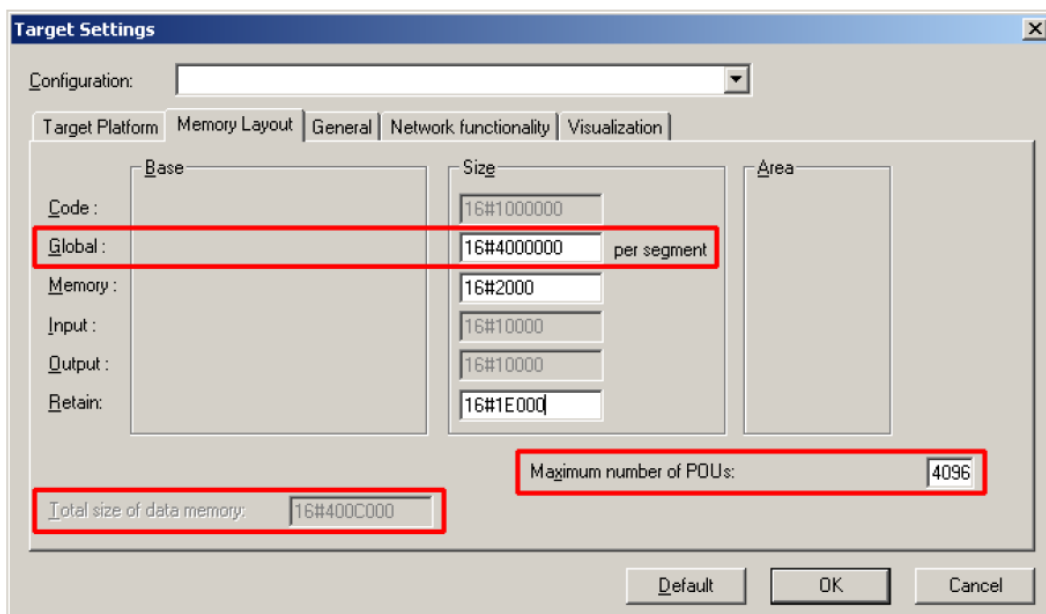
Ta wartość jest już udostępniona w systemie po pomyślnym pobraniu programu i może być w pełni wykorzystana.

Wraz z pamięcią danych przeznaczoną dla aplikacji potrzebna jest pamięć dla poszczególnych bloków funkcyjnych.

Wielkość zakresu pamięci obliczana jest z ograniczenia modułu * 12 (a więc w ustawieniu standardowym $4096 * 12$).

Suma globalnej pamięci danych i pamięci ograniczenia modułu określa rzeczywistą wielkość pamięci roboczej zarezerwowanej dla danych w systemie.

Wartość ta nie powinna przekraczać wartości podanej w polu „Total size of data memory“.

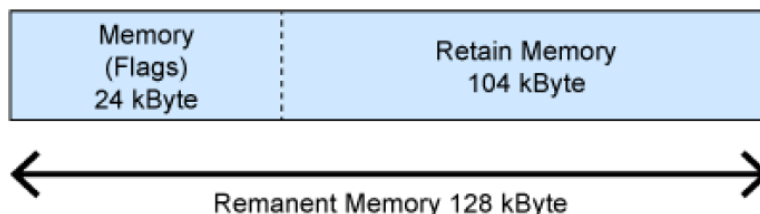


Ilustracja 105: Pamięć danych i ograniczenie modułu (przykład)

9.10.3 Pamięć RAM nieulotna

Dla aplikacji IEC -61131 dostępna pamięć nieulotna wynosi 128 kB.

Część nieulotna podzielona jest na zakres znaczników (Memory) i zakres Retain.



Ilustracja 106: Pamięć RAM nieulotna (przykład)

Podział zmiennych znaczników i Retain można kształtować indywidualnie.

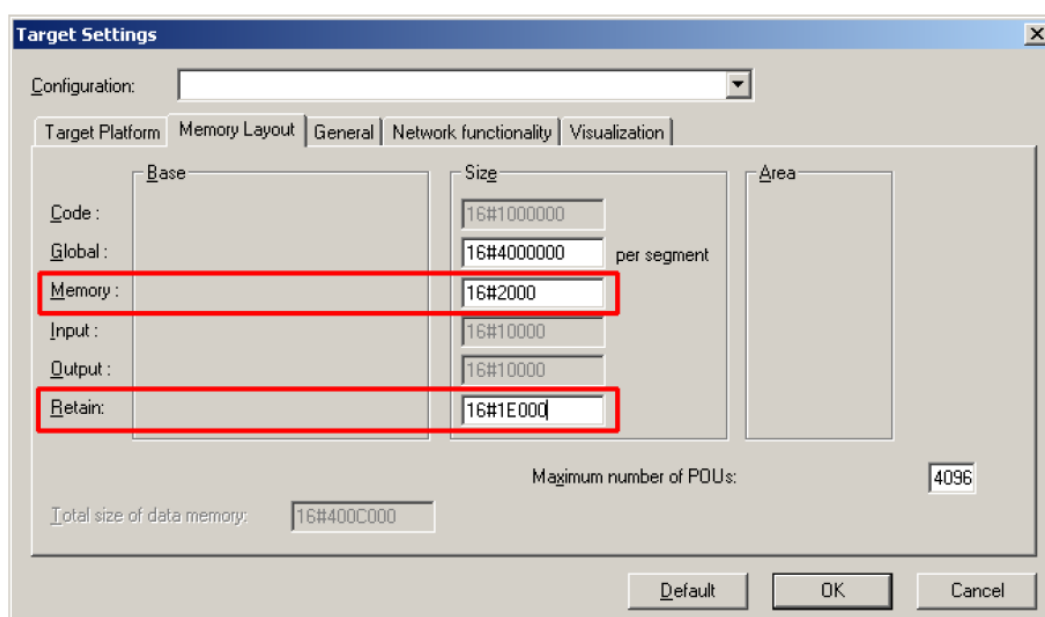
Wskazówka



Uwzględnić ograniczenia!

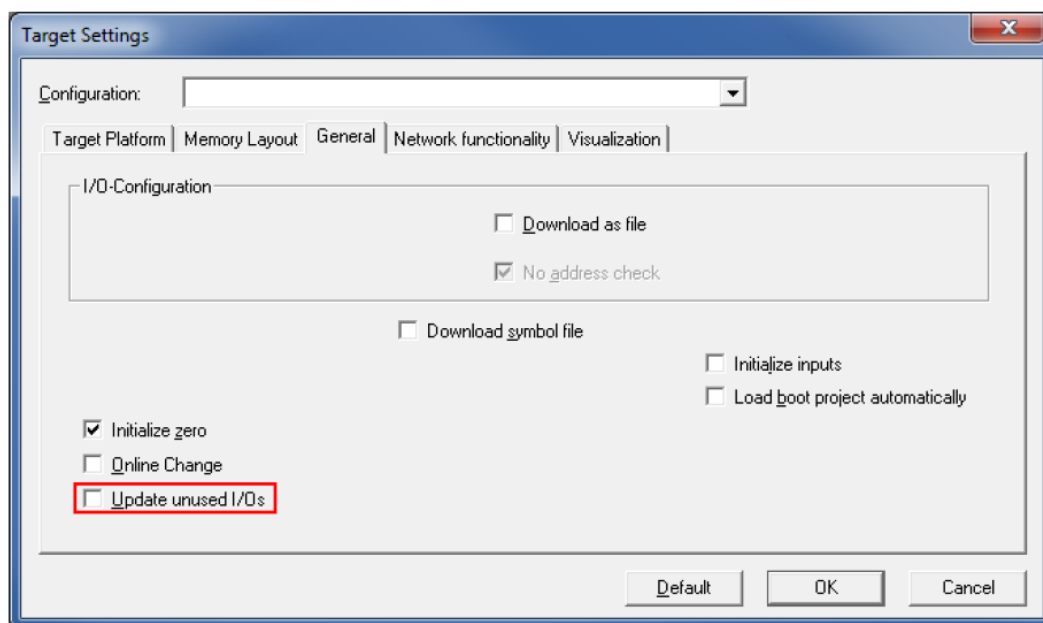
Suma Memory + Retain nie może przekraczać maksymalnej wartości 128 kB (0x20000)!

Maksymalnie można założyć 10000 zmiennych Retain.



Ilustracja 107: Pamięć znaczników i Retain (przykład)

9.11 Ogólne ustawienia systemu docelowego



Ilustracja 108: Ogólne ustawienia systemu docelowego

W zakładce „General” nie trzeba zmieniać ustawień.

Pole wyboru „Update unused I/Os” można zaznaczyć tylko w momencie rozruchu. Aktywacja powoduje większe obciążenie CPU i ma znaczący wpływ na przetwarzanie zadań.

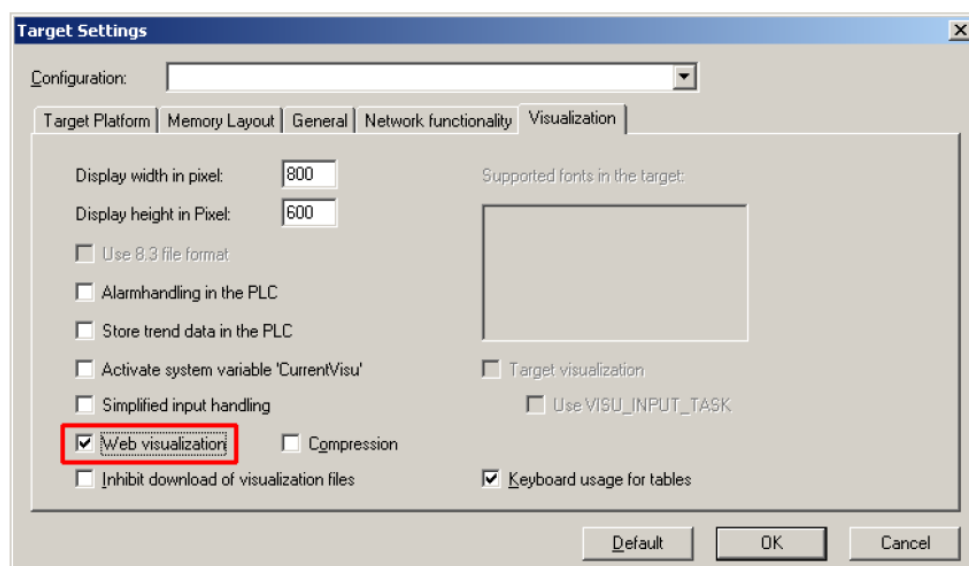
9.12 Wizualizacja CODESYS

Wizualizacja internetowa CODESYS bazuje na technologii Java. Wszystkie programy Java wymagają środowiska Java (JRE), które musi być zainstalowane na PC, pełniącym funkcję hosta, wraz z przeglądarką internetową. Applet umieszczony jest w systemie plików serwera WWW i udostępniony przez stronę wejściową HTML dla przeglądarki internetowej.

Wszystkie warianty wizualizacji (HMI i internetowa) tworzy się za pomocą graficznego edytora CODESYS. Warianty wizualizacji wybiera się w oknie „Target Settings”. Na bazie tych informacji tworzony jest dla każdej z tych stron plik opisowy w formacie XML. Pliki te można znaleźć w ścieżce instalacyjnej CODESYS w podkatalogu „visu”. Tam umieszczona jest także strona startowa HTML „webvisu.htm” i archiwum Java „webvisu.jar”, w którym zapisany jest skompresowany applet (webvisu.class).

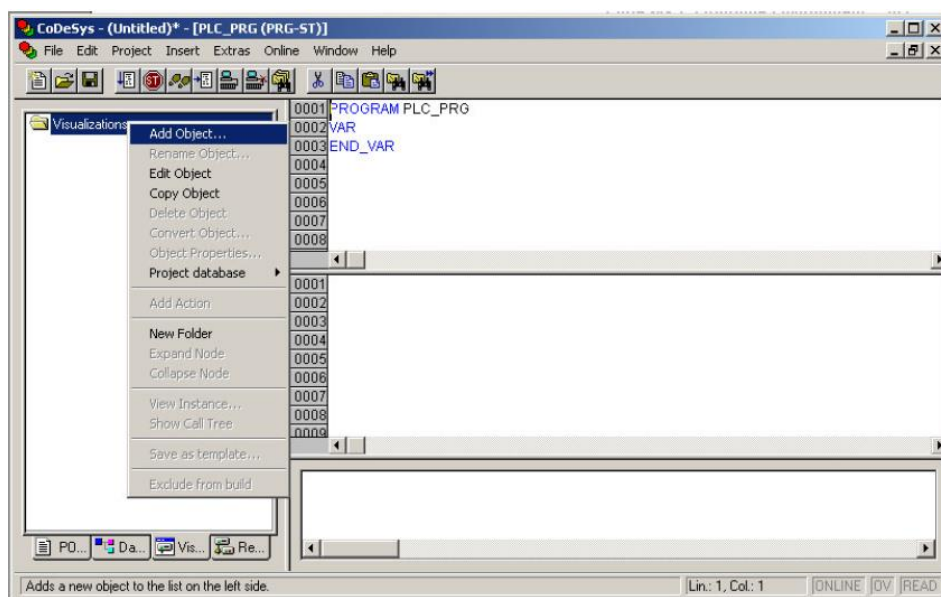
Po utworzeniu wizualizacji trzeba wykonać jeszcze następujące kroki:

1. Kliknąć zakładkę „Resources” i otworzyć „Target Settings”. Tu określa się, czy wizualizacja ma być wyświetlana jako „Web visualization” przez przeglądarkę internetową.



Ilustracja 109: Wybór wariantu wizualizacji w ustawieniach systemu docelowego

2. Utworzyć stronę startową dla wizualizacji. W tym celu należy w folderze „Visualization“ kliknąć prawym przyciskiem myszy katalog „Visualization“. Następnie w menu kontekstowym wybrać funkcję **Add Object ...**. Otworzy się okno dialogowe „New visualization“.



Ilustracja 110: Tworzenie strony startowej wizualizacji PLC_VISU

3. W oknie dialogowym „New visualization“ wpisać nazwę wizualizacji **PLC_VISU**. Podczas uruchamiania systemu wyświetli ona jako strona startowa.
4. W WBM na stronie „Ports and Services – CODESYS Services“ w grupie „CODESYS Webserver“ aktywować serwer WWW CODESYS.
5. W WBM na stronie „Ports and Services – Network Services“ w grupie „HTTP“ aktywować usługę http.

Po przesłaniu programu PLC do sterownika (**Online > Login**) i uruchomieniu (**Online > Start**), wpisać w pasku adresu przeglądarki jeden z następujących wierszy:

- „https://<IP address of the controller>/webvisu“, metoda zalecana (zamiast https można zastosować http),
- „https://<IP address of the controller>“, gdy domyślny serwer WWW został w WBM ustawiony na „WebVisu“ (zamiast https można zastosować http),
- „http://<IP address of the controller>:8080/webvisu.htm“.

Wizualizację sieciową można także wyświetlić w WBM (patrz rozdział „Strona ,CODESYS – WebVisu“).

Wskazówka



Więcej informacji

Więcej informacji (FAQ) na temat wizualizacji sieciowej CODESYS zawarto w rozdziale „Często zadawane pytania na temat wizualizacji internetowej CODESYS” oraz w pomocy online CODESYS 2.3.

9.12.1 Ograniczenia wizualizacji CODESYS

Sterownik obsługuje zintegrowany z CODESYS wariant wizualizacji „WebVisu”. W zależności od wariantu istnieją określone ograniczenia technologiczne.

Wizualizacja internetowa w sterowniku ma w porównaniu z „HMI” pewne ograniczenia. O ile „HMI” ma dostęp do niemal nieograniczonych zasobów komputera, to wizualizacja internetowa musi uwzględnić następujące limity:

Dopasowanie do systemu plików

Łączny rozmiar programu PLC, plików wizualizacji, map bitowych, logów, plików konfiguracyjnych itp. musi pasować do systemu plików.

Pamięć danych procesowych

Wizualizacja internetowa używa osobnego protokołu do wymiany danych procesowych między appletem a sterownikiem.

Sterownik przesyła dane procesowe w kodzie ASCII. Znakiem rozdzielającym wartości w obrazie procesu jest („|”). Tym samym potrzebna ilość miejsca na zmienne danych procesowych zależy nie tylko od typu danych, lecz również od samej wartości w obrazie procesu. Zatem zmienna typu „WORD” zajmuje między jednym bajtem dla wartości od 0 do 9 a pięcioma bajtami dla wartości powyżej 10000. Wybrany format (ASCII + |) pozwala jedynie na oszacowanie ilości miejsca potrzebnego na dane procesowe w buforze tych danych. W razie przekroczenia liczby danych procesowych w kodzie ASCII wizualizacja sieciowa nie będzie pracowała prawidłowo.

Moc obliczeniowa / czas procesora

Sterownik bazuje na systemie operacyjnym czasu rzeczywistego.

Procesy o wysokim priorytecie, np. program PLC, przerywają lub wyłączają procesy o niskim priorytecie, jak np. program PLC. Serwer WWW, dostępny dla wizualizacji sieciowej, należy do takiego niskiego priorytetu.

Wskazówka



Czas procesora

Przy konfiguracji zadań należy zwracać uwagę, aby dla wszystkich procesów dostępna była odpowiednia ilość czasu procesora.

Obciążenie sieci

CPU sterownika jest odpowiedzialny zarówno za wykonywanie programu PLC, jak i obsługę komunikacji sieciowej. Komunikacja za pośrednictwem ETHERNET wymaga, aby przetwarzany był każdy otrzymany telegram, niezależnie od tego, czy jest przeznaczony dla sterownika, czy też nie.

Znaczącą redukcję obciążenia sieci można osiągnąć przez zastosowanie switcha zamiast huba.

Sterownik nie ma jednak zabezpieczenia przed telegramami broadcast. Można je jedynie stłumić tylko przy wysyłaniu lub przez zastosowanie konfigurowalnych switchów z opcją limitowania telegramów broadcast. Monitor sieciowy, na przykład „wireshark” (www.wireshark.com) pozwala na sprawdzenie aktualnego obciążenia sieci.

9.12.2 Usuwanie zakłóceń wizualizacji internetowej CODESYS

W przypadku występowania problemów w zastosowaniu wizualizacji internetowej CODESYS należy najpierw spróbować znaleźć rozwiązanie w poniższej tabeli. Jeśli problemu nie uda się usunąć, należy skontaktować się z wsparciem technicznym WAGO.

Tabela 62: Błędy i ich rozwiązanie

Błąd	Środek zaradczy
Internet Explorer zgłasza „APPLET NOT INITIATED“	Zamknąć wszystkie okna przeglądarki Internet Explorer i uruchomić ją ponownie. Jeśli błąd się powtórzy, oznacza to brakujący lub uszkodzony plik. Sprawdzić przez FTP, czy archiwum Java „webvisu.jar“ znajduje się w katalogu „/PLC“ sterownika. Oryginalny plik można znaleźć w ścieżce instalacyjnej CODESYS (zazwyczaj na C:\Programme\WAGO Software\CODESYS V2.3\Visu\webvisu.jar). Zastąpić uszkodzony plik przez FTP lub zastosować w CODESYS download wszystkich plików przez Purge All > Compile All > Log in.
Wizualizacja internetowa nie jest wyświetlana.	Czy zainstalowany jest JRE? Sprawdzić ustawienia firewall, np. czy jest udostępniony port 8080.
Wizualizacja internetowa zawiesza się. Wizualizacja internetowa po pewnym czasie zatrzymuje się.	W konfiguracji zadania zostały wybrane za małe interwały wywołania. Przez to serwer WWW sterownika, który ma niski priorytet, nie ma wystarczającego czasu obliczeniowego. Jeśli nie wprowadzono konfiguracji zadania, program PLC_PRG wykonywany jest (domyślnie) w trybie free running o priorytecie 1. W tej sytuacji serwer WWW ma za mało czasu obliczeniowego. Przy zastosowaniu wizualizacji sieciowej zawsze należy dokonać konfiguracji zadania. Interwał wywołania nie powinien przekraczać trzykrotnego średniego czasu wywołania. Przy ustalaniu czasu wywołania należy pamiętać, że program PLC osiągnął stan „ustalony“.
Nie można załadować wizualizacji sieciowej do sterownika.	Prawdopodobnie nie wszystkie pliki pasują do systemu plików sterownika. Usunąć niepotrzebne pliki (np. przez FTP).
Mapa bitowa nie jest wyświetlana.	Jeśli nazwa pliku graficznego zawiera znaki specjalne, serwer WWW nie potrafi zinterpretować tych plików.
Konsola Java zgłasza: „Class not found“	JRE nie znajduje w archiwum Java „WebVisu.jar“ ingresji dla klasy „webvisu.class“. Prawdopodobnie archiwum Java jest niekompletne. Usuń „WebVisu.jar“ z bufora Java i/lub dezaktywuj bufor. W tym przypadku sterownik zażąda ponownie archiwum (applet). Jeśli problem pojawi się ponownie, załadować jeszcze raz projekt do sterownika.
Wizualizacja sieciowa jest wyświetlana statycznie, wszystkie wartości procesowe wyświetlają „0“.	Przyczyną może być niepomysłna komunikacja danych procesowych. Jeśli wizualizacja sieciowa jest obsługiwana przez serwer Proxy, obok właściwego HTTP-Proxy do wymiany danych potrzebny jest dodatkowo SOCKS-Proxy.

9.12.3 Często zadawane pytania na temat wizualizacji internetowej CODESYS

Jak można zoptymalizować applet dla specjalnych rozdzielczości ekranu?

Aby zoptymalizować urządzenia wyświetlające wizualizację internetową ze stałą rozdzielczością, zaleca się następujące działania:

W „Target Settings” w zakładce „Visualization” należy wpisać wysokość i szerokość widoku w pikselach. Przy tworzeniu wizualizacji ten obszar będzie potem zaznaczony kolorem szarym. Rzeczywista wielkość widoku w wizualizacji sieciowej definiowana jest przez atrybuty „Height” i „Width” tagu HTML-APPLET w pliku „webvisu.htm”. Również ten parametr należy dostosować do zadanej rozdzielczości.

Którą wersję środowiska Java zastosować?

Zalecane jest stosowanie Java2 Standard Edition w wersji 1.5.0 (J2SE1.5.0_06) lub nowszej. Jest ona dostępna na www.oracle.com.

Sprawdzona jest także wersja Microsofts MSJVM3810. Dla PDA dostępne są także systemy runtime innych producentów (JamaicaVM, CrEme, ...). Należy pamiętać, że te rozwiązania mogą w przypadku wizualizacji odbiegać wydajnością (np. w zakresie stabilności) od programów wymienionych wyżej.

Czy należy stosować pamięć podręczną środowiska Java?

Na to pytanie nie ma jednoznacznej odpowiedzi. W trakcie standardowej instalacji pamięć podręczna (cache) zostaje zainstalowana. Jeśli pamięć jest aktywna, JRE zapisuje w niej applety i archiwum Java. Znacznie skraca się czas drugiego wywołania wizualizacji, ponieważ applet wielkości ok. 250 kB nie musi być od nowa ładowany przez sieć, lecz znajduje się już w pamięci podręcznej. Jest to szczególnie istotne przy połączeniach sieciowych o niewielkiej przepustowości.

Wskazówka:

Na skutek zakłóceń w komunikacji sieciowej może się zdarzyć, że archiwum Java nie zostanie w całości przesłane do pamięci. W takim przypadku należy opróżnić ręcznie pamięć podręczną lub ją dezaktywować.

Dlaczego element wizualizacji „TREND” może działać tylko w trybie „Online”?

Dla projektów wizualizacji należy wybrać następujące ustawienia: zakładka **Resources > Target Settings**.

Zaznaczyć opcje „Web visualization” i „Trend data recording within control”. W przeciwnym razie dane trendów zostaną zapisane na twardym dysku komputera z zainstalowanym środowiskiem CODESYS. Wymaga to stałego połączenia między sterownikiem i bramą CODESYS. Przerwanie tego połączenia może doprowadzić do trudnych do przewidzenia reakcji sterownika.

W oknie dialogowym TREND można wybierać między trybem pracy „Online” i „History”. Na potrzeby projektów wizualizacji sterownik obsługuje tylko tryb „Online”, ponieważ nie ma możliwości skonfigurowania maksymalnej wielkości (Quota) plików trendu (*.trd). Niekontrolowany przyrost plików trendu może doprowadzić do trudnych do przewidzenia reakcji sterownika.

Najlepszą opcją jest na ogół zastosowanie elementu wizualizacji „HISTOGRAM”, ponieważ daje to pełną kontrolę momentu i liczby pomiarów, a tym samym dostępnej pamięci.

O czym należy pamiętać przy zastosowaniu elementu wizualizacji „ALARM TABLE”?

Status tych komponentów wizualizacji opisuje się najwygodniej za pomocą „Add-On”, co umożliwia dodanie danej opcji bezpłatnie i bez jakichkolwiek gwarancji.

Dla projektów wizualizacji należy wybrać następujące ustawienia: zakładka **Resources > Target Settings**.

Zaznaczyć opcje „Web visualization” i „Alarm handling within control”. W przeciwnym razie dane o alarmach przetwarzane będą na komputerze z zainstalowanym środowiskiem CODESYS. Wymaga to stałego połączenia między sterownikiem i bramą CODESYS. Przerwanie tego połączenia może doprowadzić do trudnych do przewidzenia reakcji sterownika.

10 Środowisko systemowe *e!RUNTIME*

10.1 Wskazówki ogólne

Informacja**Dodatkowa informacja**

Informacje dotyczące instalacji i uruchomienia *e!COCKPIT* można znaleźć w załączonym podręczniku.

Informacje na temat programowania znajdują się w dokumentacji do CODESYS 3.

10.2 Priorytety CODESYS V3

Jako uzupełnienie do dokumentacji CODESYS V3 poniżej przedstawiono listę priorytetów zaimplementowanych w sterowniku.

Tabela 63: Priorytety CODESYS V3

Scheduler	Zadanie	Priorytet Linux®	Priorytet IEC	Uwaga
Preemptives Scheduling - Zakres czasu rzeczywistego	Magistrala systemowa lub obiektowa – HIGH	-95 ... -86		Magistrala systemowa (-88)
	Monitorowanie przełącznika trybu pracy	-85		Zadanie rejestruje zmiany przełącznika trybu pracy i zmienia stan aplikacji PLC. (start, stop, zimny/gorący reset)
	Watchdog CODESYS	-83		Wykonywanie funkcjonalności watchdoga
	Zadania IEC cykliczne i sterowania zdarzeniami	-55 ... -53	1 ... 3	Dla zadań czasu rzeczywistego, których wykonanie nie może być determinowane przez zewnętrzne interfejsy (np. sieć obiektowa).
	Magistrala systemowa lub obiektowa – MID	-52 ... -43		CAN (-52 ... -51) PROFIBUS (-49 ... -45) Modbus slave/master (-43)
	Zadania IEC cykliczne i sterowania zdarzeniami	-42 ... -32	4 ... 14	Dla zadań czasu rzeczywistego, których wykonanie nie może mieć wpływu na komunikację sieciową.
	Magistrala systemowa lub obiektowa – LOW	-13 ... -4		
Fair Scheduling - Bez zakresu czasu rzeczywistego	Komunikacja CODESYS	Back-ground (20)		Komunikacja ze środowiskiem programistycznym CODESYS
	Zadania IEC cykliczne, dowolne i sterowania zdarzeniami		15	M.in. standardowe priorytety i zadania wizualizacji

10.3 Zakresy pamięci w *e!RUNTIME*

Zakresy pamięci sterownika mają *e!RUNTIME* następujące wielkości:

- Pamięć programowa: 32 MB
- Pamięć danych: 128 MB
- Dane wejściowe: 64 kB
- Dane wyjściowe: 64 kB
- Znaczniki: 24 kB
- Retain: 104 kB
- Ograniczenie modułu: $12 * 4096 \text{ B} = 48 \text{ kB}$

10.3.1 Pamięć programu i danych

Pamięć programu (także kodu) ma wielkość maksymalnie 32 MB.

Pamięć danych ma wielkość 128 MB.

Oba zakresy są od siebie odseparowane i w zależności od wielkości programu zostają udostępnione w systemie wraz z jego pobraniem. Ewentualne przekroczenie ograniczenia wartości sygnalizowane jest jako błąd.

10.3.2 Ograniczenie modułu

Wraz z pamięcią programu i danych, przeznaczoną dla aplikacji, potrzebna jest pamięć dla poszczególnych bloków funkcyjnych.

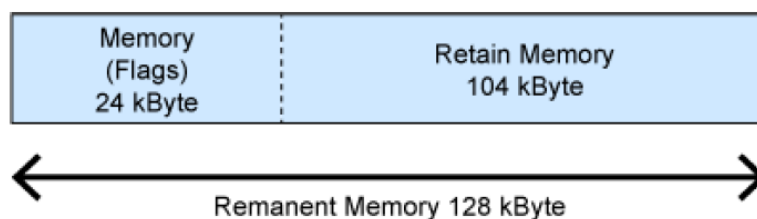
Wielkość zakresu pamięci obliczana jest z ograniczenia modułu * 12 (a więc 4096 bajtów * 12).

Suma globalnej pamięci programu i danych i pamięci ograniczenia modułu określa rzeczywistą wielkość pamięci roboczej zarezerwowanej dla danych w systemie.

10.3.3 Pamięć RAM nieulotna

Dla aplikacji IEC -61131 dostępna pamięć nieulotna wynosi 128 kB.

Część nieulotna podzielona jest na zakres znaczników (Memory) i zakres Retain.



Ilustracja 111: Pamięć RAM nieulotna

11 Modbus – CODESYS V2

11.1 Informacje ogólne

Modbus jest niezależnym od producenta, otwartym standardem sieci obiektowej do różnorodnych zastosowań w automatyce produkcyjnej i procesowej. Protokół komunikacyjny Modbus bazuje na architekturze master/slave lub client/server i wykorzystuje kody funkcyjne do wykonywania poszczególnych usług Modbus, które uzyskują dostęp do jednego lub kilku elementów modelu danych Modbus, w celu odczytu lub zapisu.

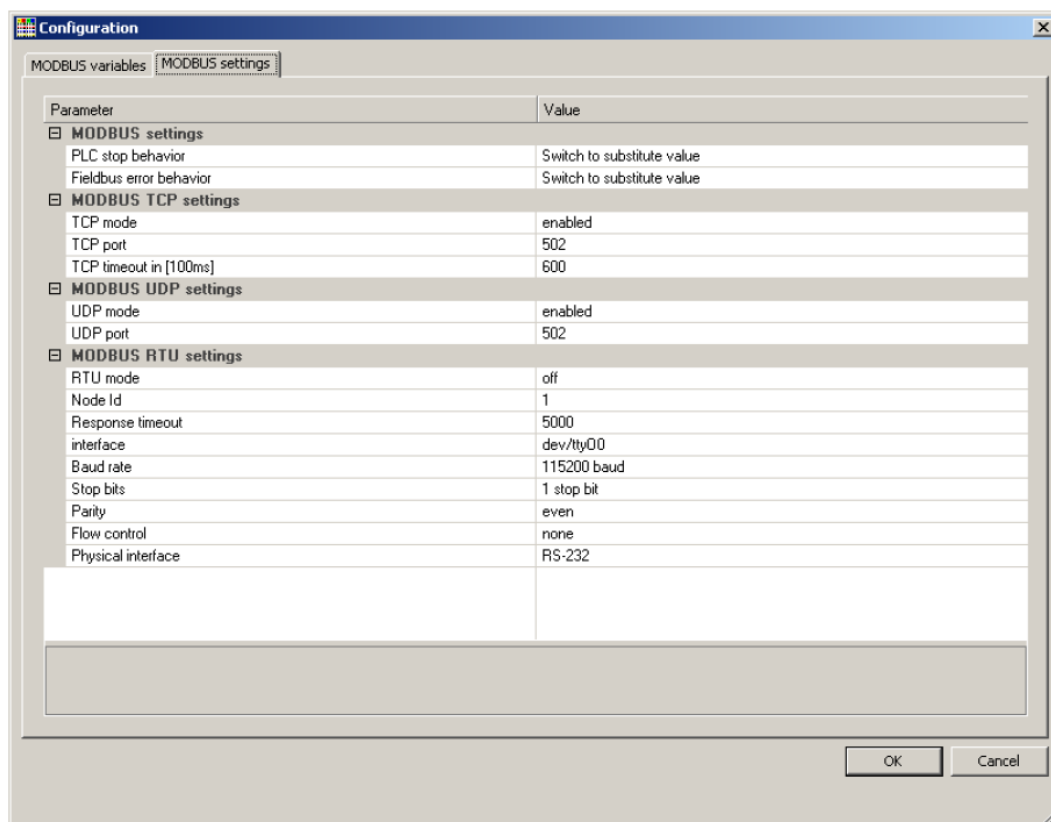
11.2 Właściwości

Modbus slave zaimplementowany w PFC200 Modbus ma następujące właściwości:

- 3 rodzaje pracy: Modbus TCP, Modbus UDP i Modbus RTU, które mogą działać równocześnie i niezależnie od siebie.
- Każdy rodzaj pracy jest konfigurowalny
- 10 obsługiwanych usług Modbus (Function Codes): FC1 do FC6, FC15, FC16, FC22, FC23
- Wymiana danych przez 1000 rejestrów w każdym lokalnym obrazy procesu Modbus
- Zakres 768 bajtów dla adresów bitowych w każdym lokalnym obrazy procesu Modbus
- Maksymalnie 104 kB większy zakres znaczników (w sumie 53248 rejestrów/słów, z tego 3328 dla adresów bitowych, wielkość zależna od podziału pamięci w CODESYS)
- 28 rejestrów informacyjnych i konfiguracyjnych
- Do 1000 połączeń TCP
- Monitorowanie komunikacji Modbus przez programowalną funkcję watchdog
- Konfigurowalna reakcja przy zatrzymaniu PLC
- Konfigurowalna reakcja przy przerwaniu komunikacji Modbus

11.3 Konfiguracja

Konfiguracja wszystkich rodzajów pracy Modbus odbywa się poprzez konfigurację sterownika w CODESYS.



Ilustracja 112: Konfiguracja sterownika w CODESYS – ustawienia Modbus

Konfiguracja Modbus slave składa się z czterech podstawowych grup parametrów:

- Modbus settings,
- Modbus TCP settings,
- Modbus UDP settings,
- Modbus RTU settings.

Wszystkie grupy parametrów zostały dokładnie opisane w kolejnych rozdziałach.

11.3.1 Modbus settings

Grupa „Modbus settings“ zawiera następujące parametry:

Tabela 64: Modbus settings

Parametr	Znaczenie
PLC stop behavior	Reakcja Modbus slave przy zatrzymaniu sterownika (sterownik w stanie STOP)
	Brak wymiany danych Wymiana danych nie jest możliwa. Na zapytania Modbus (Requests) zawsze przychodzi odpowiedź wyjątku „ILLEGAL FUNCTION“ (0x81).
	Załączenie wartości zastępczej* Wymiana danych jest możliwa. W przypadku zapytań odczytu Modbus dostarczana jest wartość zastępcza (0), a w przypadku zapytań zapisu do lokalnego obrazu procesu Modbus przejmowane są wartości bez zmian i nie są przesyłane dalej do sterownika.
	Zatrzymanie ostatniej wartości Wymiana danych jest możliwa. W przypadku zapytań odczytu Modbus dostarczane są ostatnie zatrzymane wartości, a w przypadku zapytań zapisu do lokalnego obrazu procesu Modbus przejmowane są wartości bez zmian i nie są przesyłane dalej do sterownika.
Fieldbus error response	Reakcja Modbus slave przy wykrytych błędach sieci obiektowej (przerwanie komunikacji)
	Brak wymiany danych Wymiana danych nie jest możliwa.
	Załączenie wartości zastępczej* Wymiana danych jest możliwa. Dla funkcji odczytu PLC dostarczane są wartości zastępcze (0) z obrazu procesu Modbus; w przypadku dostępu do zapisu wartości są akceptowane bez zmian w obrazie procesu Modbus bez przekazywania ich do Modbus master.
	Zatrzymanie ostatniej wartości Wymiana danych jest możliwa. Dla funkcji odczytu PLC dostarczane są ostatnie otrzymane wartości z obrazu procesu Modbus dla funkcji odczytu PLC; w przypadku dostępu do zapisu wartości są akceptowane bez zmian w obrazie procesu Modbus bez przekazywania ich do Modbus master.

* ustawienie standardowe

11.3.2 Modbus TCP settings

Grupa „Modbus TCP settings“ zawiera następujące parametry dla rodzaju pracy „Modbus TCP“:

Tabela 65: Modbus TCP settings

Parametr	Znaczenie	
TCP mode	Zezwolenie dla pracy Modbus TCP	
	wył.	Praca niedozwolona
	aktywne*	Praca możliwa
TCP port	Numer portu dla połączenia TCP	
	1	Minimalny numer portu
	502*	Standardowy port Modbus
	65535	Maksymalny numer portu
TCP Timeout	Timeout dla połączenia TCP	
	1	100 ms (1 × 100 ms)
	600*	60 sekund (600 × 100ms)
	65535	1 h 49 min 13 s 500 ms (65535 × 100 ms)

* ustawienie standardowe

11.3.3 Modbus UDP settings

Grupa „Modbus UDP settings“ zawiera następujące parametry dla rodzaju pracy „Modbus UDP“:

Tabela 66: Modbus UDP settings

Parametr	Znaczenie	
UDP mode	Zezwolenie dla pracy Modbus UDP	
	wył.	Praca niedozwolona
	aktywne*	Praca możliwa
UDP Port	Numer portu dla połączenia UDP	
	1	Minimalny numer portu
	502*	Standardowy port Modbus
	65535	Maksymalny numer portu

* ustawienie standardowe

11.3.4 Modbus RTU settings

Grupa „Modbus RTU settings“ zawiera następujące parametry dla rodzaju pracy „Modbus RTU“:

Tabela 67: Modbus RTU settings

Parametr	Znaczenie	
RTU mode	Zezwolenie dla pracy Modbus RTU	
	wyłączone*	Praca niedozwolona
	aktywne	Praca możliwa
Device ID	ID urządzenia (adres urządzenia) dla urządzenia tty	
	1*	min. ID urządzenia
	247	maks. ID urządzenia
Maximum response time	Response Timeout jest Request w [ms]	
	2000	Min. czas odpowiedzi = 2 sekund. Gdy ustawiona wartość jest mniejsza niż 2 sekundy, zostaje wewnętrznie skorygowana do 2 sekund.
	5000*	Standard = 5 sekund
	4294967295	Maks. czas odpowiedzi > 71 godzin.
Interface	Nazwa urządzenia	
	„dev/...”	Nazwa tty w stringu
	„dev/ttyO0“*	Standardowy tty
Baud rate	Prędkość transmisji	
	1200 baud	1200 baud min. prędkość transmisji
	2400 baud	2400 baud
	4800 baud	4800 baud
	9600 baud	9600 baud
	19200 baud	19200 baud
	38400 baud	38400 baud
	57600 baud	57600 baud
	115200 baud*	115200 baud, maks. prędkość transmisji
Stop bits	Liczba bitów stopu	
	1 bit stopu*	1 bit stopu w ramce, musi być wykorzystany, gdy wybrany jest bit parzystości lub nieparzystości.
	2 bity stopu	2 bity stopu w ramce, należy wykorzystać, gdy nie wybrano parzystości
Parity	Kontrola parzystości	
	brak	Brak kontroli parzystości, w konfiguracji muszą być wybrane 2 bity stopu.
	parzyste*	Parzystość obecna
	nieparzyste	Brak parzystości
Flow control	Kontrola przepływu danych (obsługiwana tylko dla ustawienia „RS-232” fizycznego interfejsu)	
	brak*	Brak kontroli przepływu
	RTS/CTS	Kontrola przepływu sprzętu
Physical interface	Rodzaj pracy dla fizycznego interfejsu	
	RS-232*	RS-232 służy jako fizyczny interfejs.
	RS-485	RS-485 służy jako fizyczny interfejs.

* ustawienie standardowe

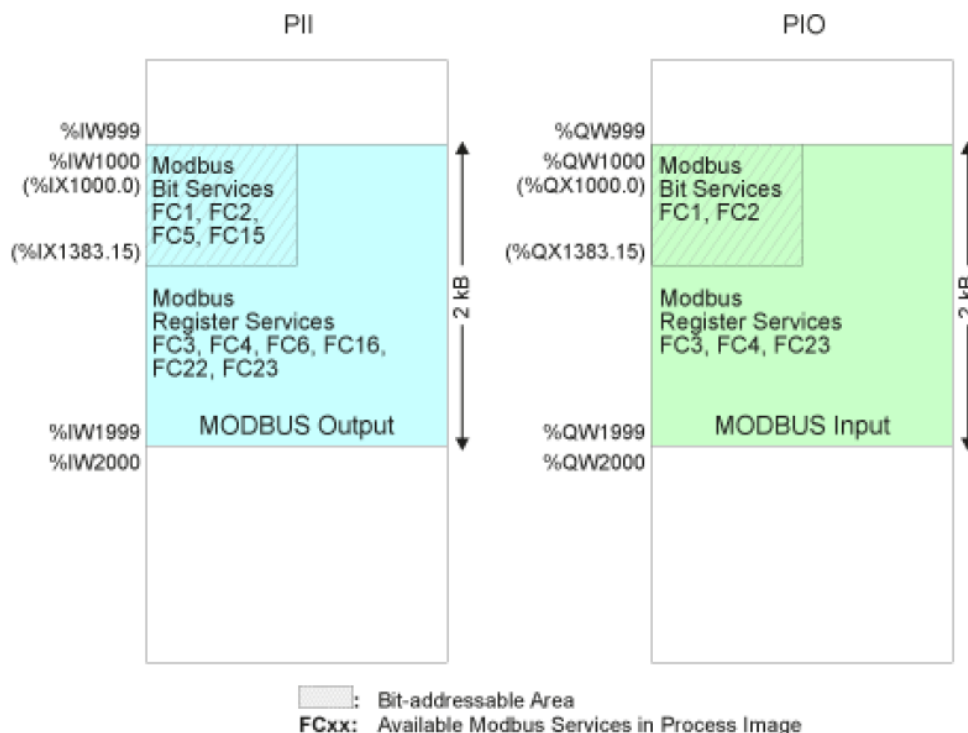
11.4 Wymiana danych

Wymiana danych Modbus odbywa się cyklicznie lub acyklicznie poprzez usługi Modbus. Liczba i rodzaj zastosowanych usług Modbus zależy od zakresu adresów. W PFC200 istnieją zasadniczo cztery zakresy adresów dla Modbus:

- **Obraz procesu wejść Modbus** (Modbus Input) – zakres w PIO, w którym cyklicznie udostępniane są dane z PLC tylko dla usług Modbus typu odczyt.
- **Obraz procesu wyjść Modbus** (Modbus Output) – zakres w PII, w którym usługi Modbus typu zapis udostępniają dane do cyklicznego odczytu przez PLC. W tym zakresie dozwolone są także usługi Modbus typu odczyt.
- **Zakres znaczników Modbus** – zakres, w którym wykonywane są usługi Modbus typu zapis i odczyt.
- **Rejestr Modbus** – zakres, zawierający rejestry konfiguracyjne i informacyjne specyficzne dla WAGO. W tym zakresie można wykonywać zasadniczo tylko usługi rejestrów Modbus.

11.4.1 Obraz procesu

Główne interfejsy danych między PLC a Modbus slave to lokalne obrazy procesu Modbus w obszarze adresów PLC zgodnie z IEC 61131: obraz procesu wejść Modbus (Modbus Input) w PIO i obraz procesu wyjść Modbus (Modbus Output) w PII. Dla lokalnego obrazu procesu wejść i wyjść Modbus przeznaczone są bloki pamięci danych wielkości 2 kB (1000 rejestrów/słów). Ponadto w każdym z tych bloków pierwsze 768 bajtów przewidziane jest także dla realizacji usług bitowych.

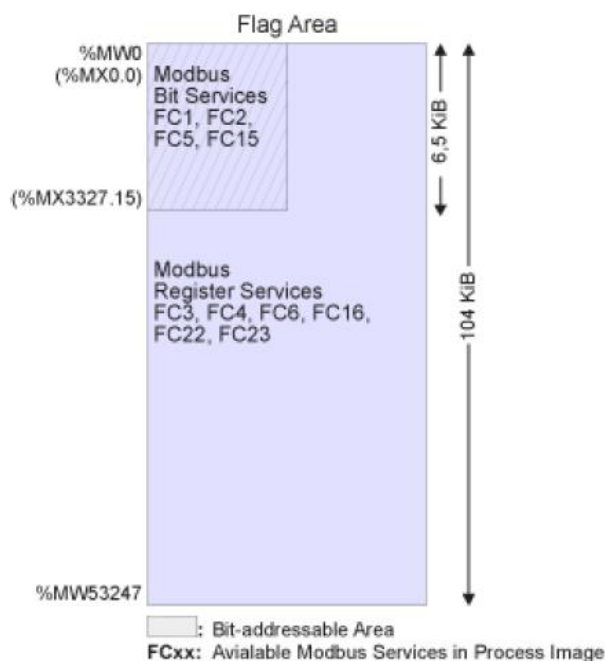


Ilustracja 113: Obraz procesu Modbus

Ponieważ nie jest przewidziany bezpośredni dostęp do modułów I/O, przez ten interfejs można wymieniać dane przeznaczone do przetwarzania w sterowniku (PLC) między PLC a siecią Modbus. Zastosowanie tych danych w poszczególnych modułach I/O podłączonych do PLC może być tylko aplikacyjne.

11.4.2 Zakres znaczników

Modbus może także wymieniać z PLC dane i zmienne sieci obiektywnej przez zakres znaczników. Należy jednak zachować ostrożność przy stosowaniu tych danych i zmiennych, do których mają dostęp zarówno Modbus, jak i PLC, ponieważ te konkurujące ze sobą dostępy nie są chronione przed sobą wzajemnie, co może prowadzić do niezgodności danych.



Ilustracja 114: Zakres znaczników

Ilustracja pokazuje maksymalny adresowalny zakres znaczników o wielkości 104 kB.

Rzeczywisty adresowalny zakres znaczników zależy od aktualnego podziału pamięci w ustawieniach systemu docelowego w CODESYS.

W ustawieniach standardowych ma on wielkość 24 kB.

11.4.3 Rejestry Modbus

W ostatnim zakresie adresów dla Modbus zaimplementowane są specyficzne dla WAGO rejestry, oferujące optymalną podstawę zarówno do odczytu niektórych informacji systemu i sieci Modbus, jak i do konfiguracji.

Zarezerwowany dla tego rejestru zakres adresów Modbus rozciąga się od adresu początkowego Modbus 4096 (0x1000) do końcowego 12287 (0x2FFF) i nie ma przyporządkowania w zakresie adresów IEC 61131. Do rejestrów tych można uzyskać dostęp za pomocą funkcji odczytu FC3, FC4 i FC23 oraz zapisu FC6, FC16 i FC23. Dokładny opis poszczególnych rejestrów znajduje się w rozdziale „Rejestry Modbus WAGO”.

11.4.4 Mapowanie Modbus

11.4.4.1 Mapowanie Modbus dla usług dostępu bitowego typu odczyt FC1, FC2

Poniższa tabela objaśnia mapowane dla usług Modbus dostępu bitowego typu odczyt:

- FC1 – Read Single Coil,
- FC2 – Read Discrete Inputs.

Tabela 68: Mapowanie Modbus dla usług dostępu bitowego typu odczyt FC1, FC2

Adres Modbus (w nawiasach wartości hex)	Adres IEC61131	Opis
0 ... 6143 (0x0000 ... 0x17FF)	%IX1000.0 ... %IX1383.15	Modbus Output: 6144 zmienne bitowe PFC Input w pierwszych 384 rejestrach/słowach (768 bajtów) obrazu procesu wyjść Modbus w PII o wielkości 2 kB. Uwaga: te usługi dostępu bitowego odczytują w tym zakresie treść z PII adresowanego bitowo.
6144 ... 12287 (0x1800 ... 0x2FFF)	%QX1000.0 ... %QX1383.15	Modbus Input: 6144 zmienne bitowe PFC Output w pierwszych 384 rejestrach/słowach (768 bajtów) obrazu procesu wejść Modbus w PIO o wielkości 2 kB.
12288 ... 65535 (0x3000 ... 0xFFFF)	%MX0.0 ... %MX3327.15	Maksymalny zakres znaczników dla adresów bitowych: 53248 znaczników bitu (6,5 kB); Rzeczywisty adresowalny zakres znaczników zależy od aktualnego podziału pamięci w CODESYS.

11.4.4.2 Mapowanie Modbus dla usług dostępu bitowego typu zapis FC5, FC15

Poniższa tabela objaśnia mapowanie dla usług Modbus dostępu bitowego typu zapis:

- FC5 – Write Single Coil,
- FC15 – Write Multiple Coils.

Tabela 69: Mapowanie Modbus dla usług dostępu bitowego typu zapis FC5, FC15

Adres Modbus (w nawiasach wartości hex)	Adres IEC61131	Opis
0 ... 6143 (0x0000 – 0x17FF)	%IX1000.0 ... %IX1383.15	Modbus Output: 6144 zmienne bitowe PFC Input w pierwszych 384 rejestrach/słowach (768 bajtów) obrazu procesu wyjść Modbus w PII o wielkości 2 kB.
6144 ... 12287 (0x1800 ... 0x2FFF)	~~%QX1000.0 ... %QX1383.15~~	Modbus Output: Niedozwolony zakres Modbus dla dostępu bitowego typu zapis Usługi dostępu bitowego typu zapis dla tego zakresu są potwierdzane przez Modbus slave kodem wyjątku Modbus „ILLEGAL DATA ADDRESS“ (0x02).
12288 ... 65535 (0x3000 ... 0xFFFF)	%MX0.0 ... %MX3327.15	Maksymalny zakres znaczników dla adresów bitowych: 53248 znaczników bitu (6,5 kB); Rzeczywisty adresowalny zakres znaczników zależy od aktualnego podziału pamięci w CODESYS.

11.4.4.3 Mapowanie Modbus dla usług dostępu do rejestru typu odczyt FC3, FC4, FC23

Poniższa tabela objaśnia mapowanie dla usług Modbus dostępu do rejestru typu odczyt.

- FC3 – Read Holding Registers,
- FC4 – Read Input Registers,
- FC23 – Read/Write Multiple Registers

Tabela 70: Mapowanie Modbus dla usług dostępu do rejestru typu odczyt FC3, FC4, FC23

Adres Modbus (w nawiasach wartości hex)	Adres IEC61131	Opis
0 ... 999 (0x0000 ... 0x03E7)	%IW1000 ... %IW1999	Modbus Output: 1000 rejestrów/słów PFC Input w obrazie procesu wyjść Modbus w PII o wielkości 2 kB. Uwaga: te usługi dostępu do rejestru odczytują w tym zakresie treść z PII.
1000 ... 1999 (0x03E8 ... 0x07CF)	%QW1000 ... %QW1999	Modbus Input: 1000 rejestrów/słów PFC w obrazie procesu wejść Modbus w PIO o wielkości 2 kB. Uwaga do FC23: tu może być wykonywana tylko część usługi typu odczyt.
2000 ... 4095 (0x07D0 ... 0x0FFF)		Niedozwolony zakres Modbus dla dostępów do rejestru typu odczyt. Usługi dostępu do rejestrów typu odczyt dla tego zakresu są potwierdzane przez Modbus slave kodem wyjątku Modbus „ILLEGAL DATA ADDRESS“ (0x02).
4096 ... 12287 (0x1000 ... 0x2FFF)	Brak adresu IEC61131	Rejestry konfiguracyjne i informacyjne: nie każdy adres Modbus jest w tym zakresie aktualny. Aktualne adresy Modbus zostały opisane w rozdziale „Rejestry Modbus WAGO“. Dostępy do nieaktualnych adresów są potwierdzane przez Modbus slave kodem wyjątku Modbus „ILLEGAL DATA ADDRESS“ (0x02). Uwaga do FC23: dla tego rejestru może być wykonywana tylko część usługi typu zapis.

Tabela 70: Mapowanie Modbus dla usług dostępu do rejestru typu odczyt FC3, FC4, FC23

Adres Modbus (w nawiasach wartości hex)	Adres IEC61131	Opis
12288 ... 65535 (0x3000 ... 0xFFFF)	%MW0 ... %MW53247	Maksymalny adresowalny zakres znaczników: 53248 rejestrów/znaczników słowa (104 kB); Rzeczywisty adresowalny zakres znaczników zależy od aktualnego podziału pamięci w CODESYS.

11.4.4.4 Mapowanie Modbus dla usług dostępu do rejestru typu zapis FC6, FC16, FC22, FC23

Poniższa tabela objaśnia mapowanie dla usług Modbus dostępu do rejestru typu zapis.

- FC6 – Write Single Register,
- FC16 – Write Multiple Registers,
- FC22 – Mask Write Register, nie dla rejestrów informacyjnych i konfiguracyjnych
- FC23 – Read/Write Multiple Registers.

Tabela 71: Mapowanie Modbus dla usług dostępu do rejestru typu zapis FC6, FC16, FC22, FC23

Adres Modbus (w nawiasach wartości hex)	Adres IEC61131	Opis
0 ... 999 (0x0000 ... 0x03E7)	%IW1000 ... %IW1999	Modbus Output: 1000 rejestrów/słów PFC Input w obrazie procesu wyjść Modbus w PII o wielkości 2 kB.
1000 ... 1999 (0x03E8 ... 0x07CF)	Brak dostępu do: %QW1000 ... %QW1999	MODBUS Output: Niedozwolony zakres Modbus dla dostępów do rejestru typu zapis Usługi dostępu do rejestrów typu zapis dla tego zakresu są potwierdzane przez Modbus slave kodem wyjątku Modbus „ILLEGAL DATA ADDRESS“ (0x02).
2000 ... 4095 (0x07D0 ... 0x0FFF)		Niedozwolony zakres Modbus dla dostępów do rejestru typu zapis Usługi dostępu do rejestrów typu zapis dla tego zakresu są potwierdzane przez Modbus slave kodem wyjątku Modbus „ILLEGAL DATA ADDRESS“ (0x02).
4096 .. 12287 (0x1000 ... 0x2FFF) tylko FC6, FC16 i FC23, nie FC22	Brak adresu IEC61131	Rejestry konfiguracyjne i informacyjne: Nie każdy adres Modbus w tym zakresie jest aktualny i nie każdy rejestr jest przeznaczony do zapisu. Aktualne adresy Modbus zostały opisane w rozdziale „Rejestry Modbus WAGO“. Dostępy do nieaktualnych adresów są potwierdzane przez Modbus slave kodem wyjątku Modbus „ILLEGAL DATA ADDRESS“ (0x02).
12288 ... 65535 (0x3000 ... 0xFFFF)	%MW0 ... %MW53247	Maksymalny adresowalny zakres znaczników: 53248 rejestrów/znaczników słowa (104 kB); Rzeczywisty adresowalny zakres znaczników zależy od aktualnego podziału pamięci w CODESYS.

11.5 Rejestry Modbus WAGO

Za pomocą rejestrów Modbus WAGO można odczytywać informacje systemu Modbus oraz konfigurować niektóre parametry Modbus. Poniższa tabela zawiera rejestry Modbus WAGO.

Tabela 72: Rejestry Modbus WAGO

Adres Modbus		Długość danych w słowach	Dostęp	Opis
Dec	Hex			
4130	0x1022	1	ro	Liczba rejestrów w obrazie procesu wejść Modbus w PIO
4131	0x1023	1	ro	Liczba rejestrów w obrazie procesu wyjść Modbus w PII
4132	0x1024	1	ro	Liczba bitów w obrazie procesu wejść Modbus w PIO
4133	0x1025	1	ro	Liczba bitów w obrazie procesu wyjść Modbus w PII
4136	0x1028	1	ro	Konfiguracja IP: BootP(1), DHCP(2) lub zakodowany na stałe adres IP(4)
4138	0x102A	1	ro	Liczba zastosowanych połączeń TCP
4144	0x1030	1	r/w	Modbus TCP Timeout (zmiany dotyczą tylko nowych połączeń)
4145	0x1031	3	ro	MAC-ID interfejsu Ethernet (eth0)
4151	0x1037	1	r/w	Zwłoka odpowiedzi Modbus TCP
4160	0x1040	1	ro	Status PLC
4352	0x1100	1	wo	Watchdog command
4353	0x1101	1	ro	Watchdog status
4354	0x1102	1	rw	Watchdog timeout (rejestr konfiguracyjny)
4355	0x1103	1	rw	Watchdog config (rejestr konfiguracyjny)
4356	0x1104	1	rw	Watchdog operation mode (rejestr konfiguracyjny)
8192	0x2000	1	ro	0x0000 (stała)
8193	0x2001	1	ro	0xFFFF (stała)
8194	0x2002	1	ro	0x1234 (stała)
8195	0x2003	1	ro	0xAAAA (stała)
8196	0x2004	1	ro	0x5555 (stała)
8197	0x2005	1	ro	0x7FFF (stała)
8198	0x2006	1	ro	0x8000 (stała)

Tabela 72: Rejestry Modbus WAGO

Adres Modbus		Długość danych w słowach	Dostęp	Opis
Dec	Hex			
8199	0x2007	1	ro	0x3FFF (stała)
8200	0x2008	1	ro	0x4000 (stała)
8208	0x2010	1	ro	Revision (firmware index)
8209	0x2011	1	ro	Kod serii
8210	0x2012	1	ro	Kod urządzenia
8211	0x2013	1	ro	Wersja firmware major
8212	0x2014	1	ro	Wersja firmware minor
8213	0x2015	1	ro	Wersja MBS

Poniżej opisano bardziej szczegółowo rejestry Modbus WAGO.

11.5.1 Właściwości obrazu procesu

11.5.1.1 Rejestr 0x1022 – Liczba rejestrów w obrazie procesu wejść Modbus

Ten rejestr zawiera liczbę rejestrów udostępnionych w obrazie procesu wejść Modbus (Modbus Input).

11.5.1.2 Rejestr 0x1023 – Liczba rejestrów w obrazie procesu wyjść Modbus

Ten rejestr zawiera liczbę rejestrów udostępnionych w obrazie procesu wyjść Modbus (Modbus Output).

11.5.1.3 Rejestr 0x1024 – Liczba bitów w obrazie procesu wejść Modbus

Ten rejestr zawiera liczbę bitów udostępnionych w obrazie procesu wejść Modbus (Modbus Input).

11.5.1.4 Rejestr 0x1025 – Liczba bitów w obrazie procesu wyjść Modbus

Ten rejestr zawiera liczbę bitów udostępnionych w obrazie procesu wyjść Modbus (Modbus Output).

11.5.2 Konfiguracja sieci

11.5.2.1 Rejestr 0x1028 – Konfiguracja IP

Ten rejestr zawiera informację o ustawionej konfiguracji IP.
Możliwe wartości to:

- 1 = BootP
- 2 = DHCP
- 4 = stały adres IP

11.5.2.2 Rejestr 0x102A – liczba zastosowanych połączeń TCP

Ten rejestr dostarcza liczbę zastosowanych połączeń TCP.
Maksymalna liczba połączeń Modbus TCP wynosi 1000.

11.5.2.3 Rejestr 0x1030 – Modbus TCP Socket Timeout

Ten rejestr zawiera wartość Timeout dla socketów TCP.
Wartość ta podawana jest w jednostkach 100 ms (Ticks). Nowa wartość jest przejmowana tylko dla nowych niezastosowanych jeszcze połączeń. W przypadku zmian połączenia już zastosowane pracują jak dotychczas z ustawioną ostatnio wartością timeout.

11.5.2.4 Rejestr 0x1031 – Adres MAC interfejsu ETHERNET 1 (eth0)

Ten rejestr dostarcza adres MAC pierwszego interfejsu ETHERNET (eth0)
Można również otrzymać częściowy wynik MAC.

11.5.2.5 Rejestr 0x1037 – zwłoka odpowiedzi Modbus TCP

Ten rejestr zapisuje wartość zwłoki odpowiedzi Modbus.
Wartość ta podawana jest w jednostkach ms. Maksymalna możliwa do ustawienia zwłoka wynosi 32 ms, standardowa wartość to 0 ms (brak zwłoki). Wysłanie odpowiedzi na zapytanie Modbus opóźniane jest od momentu przetworzenia (odczyt i/lub zapis wartości rejestru) o ustawiony czas. Zapytania przychodzące w międzyczasie mogą być przetworzone dopiero po wysłaniu poprzedniego zapytania. W przypadku Modbus UDP dotyczy to zasadniczo wszystkich zapytań, a w przypadku Modbus TCP każdego połączenia. Rzeczywisty odstęp czasowy między zapytaniem Modbus i odpowiedzią na nie zależy od liczby równoległych zapytań oraz obciążenia systemu i jest zawsze większy niż ustawiona zwłoka odpowiedzi. Zmiany zwłoki odpowiedzi realizowane są natychmiast dla każdego kolejnego zapytania.

11.5.3 Rejestr statusu PLC

Ten rejestr 0x1040 dostarcza informację o statusie, w którym znajduje się sterownik.

Możliwe wartości to:

- 1 = PLC running – PLC znajduje się w stanie RUNNING (działa).
- 2 = PLC stopped – PLC znajduje się w stanie STOPPED (został zatrzymany).

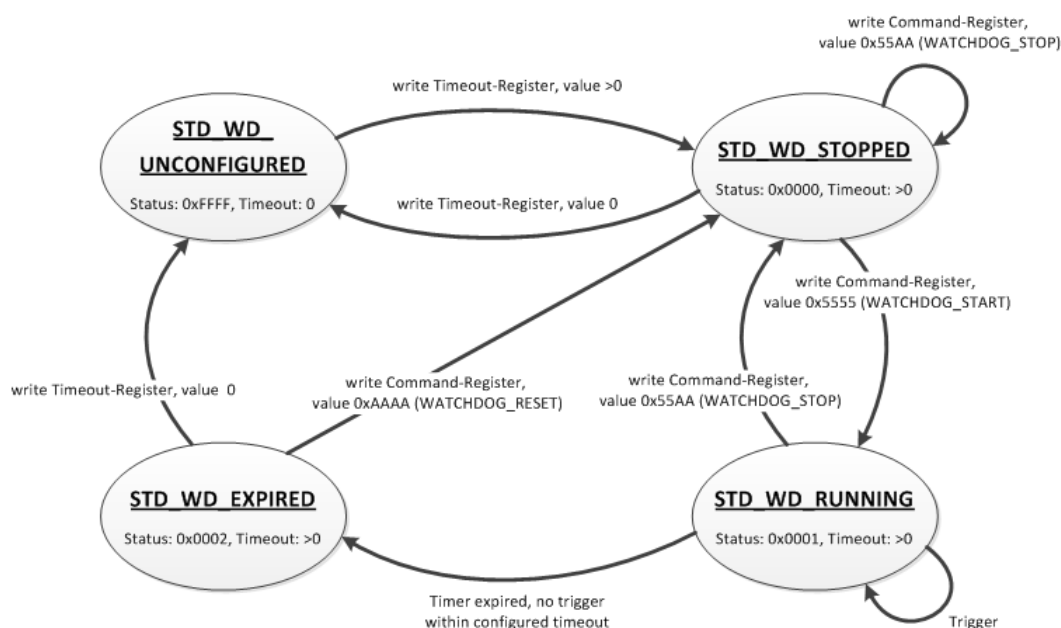
11.5.4 Modbus watchdog

Modbus watchdog monitoruje w Modbus slave bieżącą komunikację Modbus z Modbus master. Wszystkie ważne żądania Modbus pochodzące od Modbus master ze wszystkich usług obsługiwanych przez Modbus slave są zdarzeniami wyzwalającymi Modbus watchdog (patrz rozdział „Mapowanie Modbus”). Nie dotyczy to trybu Explicit Trigger i dostępu do rejestru 0x1101 (Watchdog Status), które konfiguruje się w rejestrze 0x1103 (Watchdog Config).

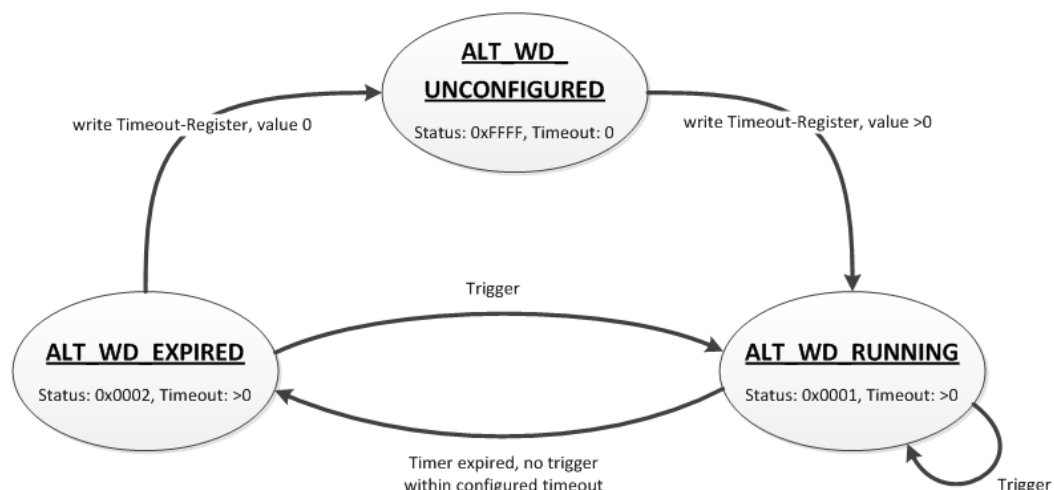
Jeżeli w trakcie czasu monitorowania ustawionego w rejestrze 0x1102 (Watchdog Timeout) podczas działania Watchdog nie nastąpi wyzwolenie, inicjowana jest reakcja „Watchdog Timeout”. Jako reakcję można skonfigurować rozłączenie wszystkich połączeń Modbus TCP, patrz rejestr 0x1103 (Watchdog Config).

Modbus watchdog obsługuje dwa różne tryby pracy: STANDARD_WATCHDOG i ALTERNATIVE_WATCHDOG. Odpowiedni tryb pracy wybiera się w rejestrze 0x1104 (Watchdog Operation Mode).

Poniższe diagramy obrazują możliwe stany Modbus watchdog oraz przejścia stanów dla danego trybu pracy.



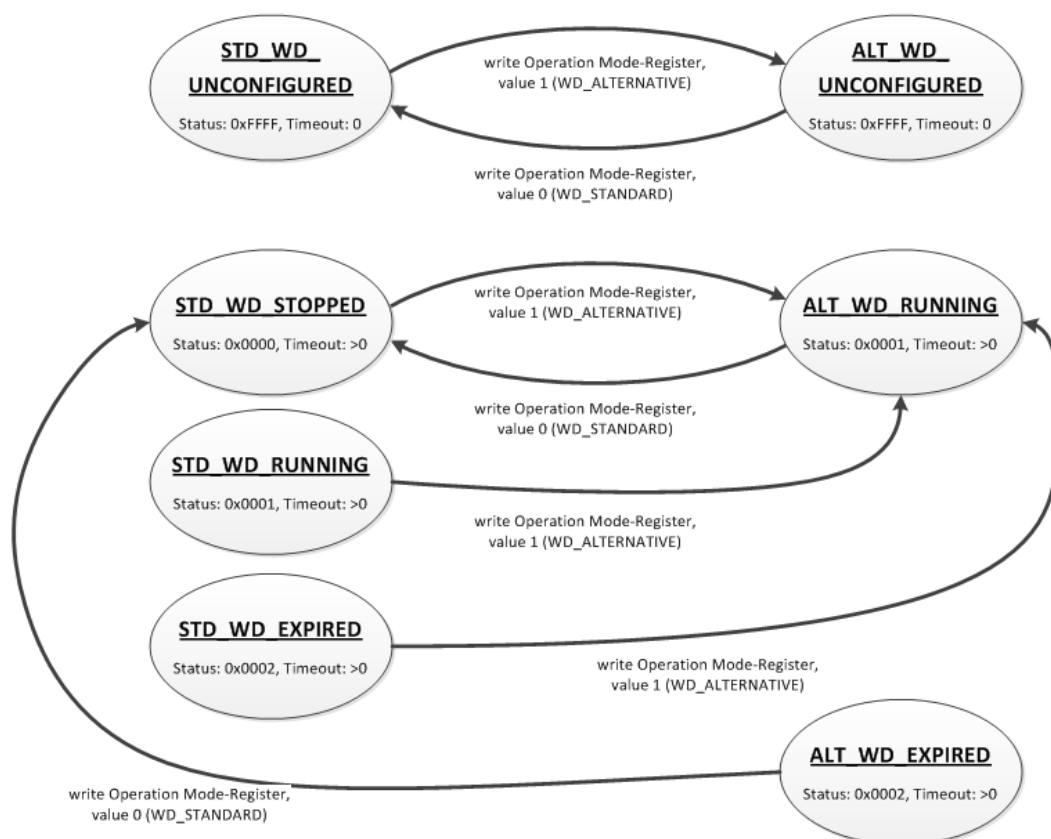
Ilustracja 115: Diagram stanów, tryb pracy STANDARD_WATCHDOG



Ilustracja 116: Diagram stanów, tryb pracy ALTERNATIVE_WATCHDOG

Diagram stanów dla trybu pracy ALTERNATIVE_WATCHDOG pokazuje, że watchdog jest aktywny zawsze wtedy, gdy w rejestrze 0x1102 (Watchdog Timeout) ustawiony czas monitorowania jest >0. Możliwość zapisu poleceń w rejestrze 0x1100 (Watchdog Command) jest w tym trybie pracy ograniczona. Jako wyzwolenie dozwolone jest wyłącznie polecenie WATCHDOG_START. Jedyną możliwością dezaktywowania lub zatrzymania watchdoga w trybie pracy ALTERNATIVE_WATCHDOG jest ustawienie rejestru Timeout na 0 po upływie czasu monitorowania oraz przełączenie na tryb STANDARD_WATCHDOG.

Diagram poniżej obrazuje możliwe przejścia stanów przy przełączaniu trybów pracy.



Ilustracja 117: Diagram ilustrujący możliwe stany przy przełączaniu trybów pracy

11.5.4.1 Rejestr 0x1100 – Watchdog Command

Ten rejestr odbiera polecenia dla Modbus watchdog. Nie ma możliwości odczytu zapisanych poleceń.

Niezależnie od statusu watchdoga, akceptowane są następujące polecenia:

Tabela 73: Polecenia watchdoga

Wartość	Nazwa	Znaczenie
0x5555	WATCHDOG_START	Otwiera skonfigurowanego watchdoga. W stanie WATCHDOG_UNCONFIGURED, gdy czas monitorowania watchdoga nie jest skonfigurowany, odpowiedzią jest wyjątek ILLEGAL_DATA_VALUE (0x03). W stanie WATCHDOG_EXPIRED i przy trybie pracy STANDARD_WATCHDOG odpowiedzią jest wyjątek ILLEGAL_FUNCTION (0x01). Watchdog musi w tym przypadku najpierw zostać zresetowany przez polecenie WATCHDOG_RESET do stanu WATCHDOG_STOPPED. We wszystkich innych przypadkach watchdog jest ponownie uruchamiany i ustawiany jest stan WATCHDOG_RUNNING.
0x55AA	WATCHDOG_STOP	Zatrzymuje uruchomionego watchdoga. W stanie WATCHDOG_UNCONFIGURED, gdy czas monitorowania watchdoga nie jest skonfigurowany, odpowiedzią jest wyjątek ILLEGAL_DATA_VALUE (0x03). W stanie WATCHDOG_EXPIRED i przy trybie pracy STANDARD_WATCHDOG odpowiedzią jest wyjątek ILLEGAL_FUNCTION (0x01). Watchdog musi w tym przypadku najpierw zostać zresetowany przez polecenie WATCHDOG_RESET do stanu WATCHDOG_STOPPED. Przy trybie pracy ALTERNATIVE_WATCHDOG odpowiedzią jest wyjątek ILLEGAL_DATA_VALUE (0x03). W tym trybie pracy polecenie to jest w zasadzie niedozwolone. W każdym innym przypadku watchdog zostaje zatrzymany i ustawiony zostaje stan WATCHDOG_STOPPED. Wielokrotnie odebrane polecenie zatrzymania w stanie WATCHDOG_STOPPED nie ma wpływu na zachowanie watchdoga i nie wymaga potwierdzenia odpowiedzi o błędzie.
0xAAAA	WATCHDOG_RESET	Resetuje watchdoga po przekroczeniu czasu. W stanie WATCHDOG_EXPIRED i przy trybie pracy STANDARD_WATCHDOG watchdog jest resetowany. Następnie powraca do stanu WATCHDOG_STOPPED. W każdym innym przypadku odpowiedzią jest wyjątek ILLEGAL_DATA_VALUE (0x03).

11.5.4.2 Rejestr 0x1101 – Watchdog Status

Ten rejestr dostarcza informację o aktualnym stanie Modbus watchdog. Możliwe są następujące stany:

Tabela 74: Status watchdoga

Wartość	Nazwa	Znaczenie
0xFFFF	WATCHDOG_UNCONFIGURED	Modbus watchdog nie jest konfigurowalny, rejestr 0x1102 (Watchdog Timeout) zawiera wartość 0. Stan ten można zmienić ustawiając czas monitorowania >0.
0x0000	WATCHDOG_STOPPED	Modbus watchdog jest konfigurowalny, rejestr 0x1102 (Watchdog Timeout) zawiera wartość >0. W trybie pracy STANDARD_WATCHDOG watchdog może być aktywowany w tym stanie za pomocą polecenia WATCHDOG_START. W trybie pracy ALTERNATIVE_WATCHDOG stan ten nie jest dostępny, ponieważ watchdog jest aktywowany automatycznie.
0x0001	WATCHDOG_RUNNING	Modbus watchdog jest aktywny, tzn. został skonfigurowany i uruchomiony. Ustawiony czas monitorowania jeszcze nie upłynął.
0x0002	WATCHDOG_EXPIRED	Upłynął czas monitorowania ustawiony w rejestrze 0x1102 (Watchdog Timeout). W trybie pracy STANDARD_WATCHDOG watchdog musi w tym stanie najpierw zostać zresetowany przez polecenie WATCHDOG_RESET do stanu WATCHDOG_STOPPED. W trybie pracy ALTERNATIVE_WATCHDOG watchdog jest aktywowany automatycznie przy następnym wyzwoleniu.

11.5.4.3 Rejestr 0x1102 – Watchdog Timeout

Ten rejestr zawiera wartość czasu monitorowania watchdoga. Skok wynosi 100 ms, a maksymalna wartość to 65535 (odpowiada 6553,5 s). Wartość domyślna wynosi 0. W tym przypadku watchdog nie może być aktywowany i znajduje się w stanie WATCHDOG_UNCONFIGURED.

Odczyt i zapis w rejestrze jest możliwy w stanach WATCHDOG_UNCONFIGURED, WATCHDOG_STOPPED i WATCHDOG_EXPIRED. Natomiast gdy watchdog jest aktywny (stan WATCHDOG_RUNNING), dostęp do tego rejestru jest możliwy tylko w trybie odczytu. W tym przypadku zapis wywołuje odpowiedź wyjątkiem ILLEGAL_FUNCTION (0x01).

11.5.4.4 Rejestr 0x1103 – Watchdog Config

Ten rejestr zawiera parametry konfiguracyjne watchdoga. Rejestr jest zorientowany bitowo (patrz poniższa tabela).

Odczyt i zapis w rejestrze jest możliwy w stanach WATCHDOG_UNCONFIGURED, WATCHDOG_STOPPED i WATCHDOG_EXPIRED. Natomiast gdy watchdog jest aktywny (stan WATCHDOG_RUNNING), dostęp do tego rejestru jest możliwy tylko w trybie odczytu. W tym przypadku zapis wywołuje odpowiedź wyjątkiem ILLEGAL_FUNCTION (0x01).

Tabela 75: Konfiguracja watchdoga

Bit	Nazwa / określenie bitu	Znaczenie	
0	EXPLICIT_TRIGGER_ONLY	Aktywuje tryb Explizit Trigger.	
		0*	Watchdog jest wyzwalany przez wszystkie ważne zapytania Modbus. Wyjątkiem jest tylko dostęp do rejestru 0x1101 (Watchdog Status).
		1	Tylko zapis w rejestrze 0x1100 (Watchdog Command) wartości 0x5555 (WATCHDOG_START) traktowany jest jak wyzwolenie watchdoga. Również w tym przypadku wyjątkiem jest dostęp do rejestru 0x1101 (Watchdog Status).
1	TRIGGER_ON_STATUS_REG	Aktywuje wyzwolenie watchdoga dostępem (typu odczyt) do rejestru 0x1101 (Watchdog Status)	
		0*	Odczyt statusu watchdoga nie jest traktowany jako wyzwolenie watchdoga.
		1	Odczyt statusu watchdoga jest traktowany jako wyzwolenie watchdoga.
2	CLOSE_ALL_TCP_CONNECTIONS	Aktywuje rozłączenie wszystkich połączeń Modbus TCP w momencie zakończenia czasu monitorowania (przejście do stanu WATCHDOG_EXPIRED)	
		0	Istniejące połączenia Modbus TCP pozostają otwarte.
		1*	Wszystkie istniejące połączenia Modbus TCP zostają zamknięte.
* ustawienie standardowe			

Poszczególne opcje są aktywowane, gdy ustawiony jest dany bit lub kombinacja bitów.

11.5.4.5 Rejestr 0x1104 – Watchdog Operation Mode

Ten rejestr zawiera wartość trybu pracy watchdoga.

Rejestr można odczytywać i zapisywać niezależnie od statusu watchdoga. Możliwe są następujące tryby pracy:

Tabela 76: Tryby pracy watchdoga

Wartość	Nazwa	Znaczenie
0x0000	STANDARD_WATCHDOG	Tryb pracy „Standard Watchdog”. Watchdog musi być sterowany wyraźnie za pomocą poleceń (patrz rejestr 0x1100 Watchdog Command).
0x0001	ALTERNATIVE_WATCHDOG	Tryb pracy „Alternative Watchdog”. Watchdog jest aktywowany bezpośrednio z czasem monitorowania > 0 s w rejestrze 0x1102 (Watchdog Timeout). Każde wyzwolenie powoduje restart watchdoga, zarówno działającego jak i tego, dla którego czas upłynął. W tym trybie pracy rejestry 0x1102 (Watchdog Timeout) i 0x1103 (Watchdog Config) są zapisywane zdalnie wraz z trybem pracy. Tym samym po restarcie urządzenia dla trybu pracy „Alternative Watchdog” zostaje zachowana taka sama konfiguracja jak poprzednio i po ustawieniu czasu monitorowania jest on natychmiast ponownie aktywowany

11.5.5 Rejestr stałych Modbus

Rejestry 0x2000 ... 0x2008 dostarczają stałych na podstawie tabeli „Rejestr Modbus WAGO”. Istnieje możliwość jednoczesnego odczytu wszystkich stałych lub ich następujących po sobie części.

11.5.6 Elektroniczna tabliczka znamionowa

Rejestr 0x2010 do 0x2015 zawiera informacje z elektronicznej tabliczki znamionowej. Istnieje możliwość jednoczesnego odczytu całej tabliczki znamionowej lub jej następujących po sobie fragmentów.

11.5.6.1 Rejestr 0x2010 – wersja (firmware index)

Ten rejestr informuje o bieżącym numerze wersji (firmware index) sterownika.

Przykład: 5 dla wersji 5.

11.5.6.2 Rejestr 0x2011 – kod serii

Ten rejestr informuje o numerze serii WAGO (kod serii), przynależnym do sterownika.

Przykład: 750 dla WAGO I/O System 750.

11.5.6.3 Rejestr 0x2012 – kod urządzenia

Ten rejestr informuje o kodzie urządzenia (nr katalogowy WAGO) sterownika.

Przykład: 8206.

11.5.6.4 Rejestr 0x2013 – wersja major firmware

Ten rejestr informuje o części major wersji firmware.

11.5.6.5 Rejestr 0x2014 – wersja minor firmware

Ten rejestr informuje o części minor wersji firmware.

11.5.6.6 Rejestr 0x2015 – wersja MBS

Ten rejestr informuje o wersji biblioteki Modbus slave. Najwyższy bajt zawiera numer wersji major, a najniższy bajt numer wersji minor.

Przykład:

0x010A => numer wersji major = 1, numer wersji minor = 10.

11.6 Diagnostyka

11.6.1 Diagnostyka dla Modbus master

Modbus master może zapytać o status PLC lub systemu sterowania przez odczyt specyficznego dla WAGO rejestru 0x1040 – „PLC Status” za pomocą usług Modbus FC3 (Read Holding Registers) lub FC4 (Read Input Registers). Specyficzny dla WAGO rejestr 0x1040 – „PLC Status” został opisany w rozdziale „Rejestr statusu PLC”.

Status Modbus watchdog można sprawdzić za pomocą usługi odczytu rejestru (FC3 lub FC4) z zapytaniem do specyficznego dla WAGO rejestru 0x1101 – „Watchdog Status Register”. Więcej informacji na ten temat można znaleźć w rozdziale „Modbus watchdog”.

Usługa Modbus „Get Communication Event Counter” (FC11) nie jest obsługiwana w aktualnej wersji V1.0 Modbus slave.

11.6.2 Diagnostyka dla systemu runtime

Ze strony systemu runtime diagnostykę Modbus slave można przeprowadzić poprzez podłączenie biblioteki CODESYS „BusDiag.lib”. W tej bibliotece znajduje się blok funkcyjny „DiagGetBusState()”, udostępniający stan sieci obiektowej, w tym przypadku sieci Modbus. Szczegółowe informacje na temat bloku funkcyjnego znajdują się zarówno w aktualnej dokumentacji, jak również w pomocy online CODESYS.

11.6.3 Diagnostyka przez serwer błędów

Modbus slave obsługuje również funkcjonalność serwera błędów zaimplementowanego w PFC i generuje komunikaty diagnostyczne, które są zapisywane przez cały czas (w pliku) lub czasowo (w RAM) i wyświetlane bezpośrednio przez WBM Client. Modbus slave generuje następujące komunikaty diagnostyczne:

Tabela 77: Diagnostyka przez serwer błędów

ID diagnozy	Tekst diagnozy	Sposób zapisu	Znaczenie
0x00090000	Modbus Slave library loaded	czasowy	Biblioteka Modbus slave pomyślnie załadowana.
0x00090001	Modbus Slave library closed	czasowy	Biblioteka Modbus slave pomyślnie odinstalowana.
0x00090002	Modbus Slave TCP started	czasowy	Modbus slave w trybie pracy TCP pomyślnie uruchomiony.
0x00090003	Modbus Slave TCP start failed	stały	Uruchomienie Modbus slave w trybie pracy TCP nie powiodło się.
0x00090004	Modbus Slave TCP terminated	czasowy	Modbus slave w trybie pracy TCP pomyślnie zakończony.

Tabela 77: Diagnostyka przez serwer błędów

ID diagnozy	Tekst diagnozy	Sposób zapisu	Znaczenie
0x00090005	Modbus Slave UDP started	czasowy	Modbus slave w trybie pracy UDP pomyślnie uruchomiony.
0x00090006	Modbus Slave UDP start failed	stały	Uruchomienie Modbus slave w trybie pracy UDP nie powiodło się.
0x00090007	Modbus Slave UDP terminated	czasowy	Modbus slave w trybie pracy UDP pomyślnie zakończony.
0x00090008	Modbus Slave RTU started	czasowy	Modbus slave w trybie pracy RTU pomyślnie uruchomiony.
0x00090009	Modbus Slave RTU start failed	stały	Uruchomienie Modbus slave w trybie pracy RTU nie powiodło się.
0x0009000A	Modbus Slave RTU terminated	czasowy	Modbus slave w trybie pracy RTU pomyślnie zakończony.
0x0009000B	Modbus Slave data exchange started by PLC	czasowy	Wymiana danych Modbus slave uruchomiona.
0x0009000C	Modbus Slave data exchange stopped by PLC	czasowy	Wymiana danych Modbus slave zatrzymana.
0x0009000F	Modbus Slave PLC watchdog timer expired	stały	Czas monitorowania dla sterownika (PLC) upłynął.
0x00090100	Modbus Slave common configuration failed	stały	Konfiguracja Modbus slave nie powiodła się.
0x00090101	Modbus Slave TCP configured successfully	czasowy	Konfiguracja TCP Modbus slave pomyślnie przeprowadzona.
0x00090102	Modbus Slave TCP configuration failed	stały	Konfiguracja TCP Modbus slave nie powiodła się.
0x00090103	Modbus Slave UDP configured successfully	czasowy	Konfiguracja UDP Modbus slave pomyślnie przeprowadzona.
0x00090104	Modbus Slave UDP configuration failed	stały	Konfiguracja UDP Modbus slave nie powiodła się.
0x00090105	Modbus Slave RTU configured successfully	czasowy	Konfiguracja RTU Modbus slave pomyślnie przeprowadzona.
0x00090106	Modbus Slave RTU configuration failed	stały	Konfiguracja RTU Modbus slave nie powiodła się.

Tabela 77: Diagnostyka przez serwer błędów

ID diagnozy	Tekst diagnozy	Sposób zapisu	Znaczenie
0x00090107	Port for Modbus Slave RTU operation not free	stały	Port szeregowy do konfiguracji RTU Modbus slave jest już zajęty.
0x00090108	Modbus Slave RTU configuration in RS-485 mode failed	stały	Konfiguracja RTU Modbus slave dla trybu RS-485 nie powiodła się.
0x00090200	Modbus Slave Watchdog activated	czasowy	Modbus watchdog aktywowany.
0x00090201	Modbus Slave Watchdog deactivated	czasowy	Modbus watchdog dezaktywowany.
0x00090202	Modbus Slave Watchdog Timer expired	stały	Upłynął czas monitorowania Modbus watchdog.
0x00090203	Modbus Slave terminated all established TCP connections	stały	Wszystkie połączenia Modbus TCP zostały zakończone w wyniku upływu czasu monitorowania.
0x00090300	Modbus Slave: obtaining system resource failed	stały	Żądanie zasobów systemu przez Modbus slave nie powiodło się.
0x00090301	Modbus Slave: processing system resource failed	stały	Dostęp do zasobów systemu przez Modbus slave nie powiódł się.

12 Modbus – e!RUNTIME

12.1 Przegląd adresów Modbus

	Modbus Register Access	Modbus Bit Access
PFC-OUT Modbus-IN Size: 32000 registers	0x0000	0x0000
	Only read access FC3, FC4, FC23, FC66	Only read access FC1, FC2 0x7FFF
	0x7CFF	
PFC-IN Modbus-OUT Size: 32000 registers	0x7D00	0x8000
	Read and write access FC3, FC4, FC6, FC16, FC23, FC66	Read and write access FC1, FC2, FC5, FC15 0xFFFF
	0xF9FF	
Modbus Special registers Size: 1536 registers	0xFA00	
	Read and write access FC3, FC4, FC6, FC16, FC23, FC66	
	0xFFFF	

Ilustracja 118: Przegląd adresów Modbus

12.2 Rejestry Modbus

Tabela 78: Rejestry Modbus WAGO

Adres Modbus		Długość danych w słowach	Dostęp	Opis
Dec	Hex			
Rejestr konfiguracyjny watchdoga				
64.000	0xFA00	1	w	Rejestr Watchdog Command
64.001	0xFA01	1	rw	Rejestr Watchdog Time-out
64.002	0xFA02	1	ro	Rejestr Watchdog Status
64.003	0xFA03	1	rw	Rejestr Watchdog Config
64.004	0xFA04	1	rw	Rejestr Modbus TCP Connection Watchdog
Rejestr statusu				
64.010	0xFA0A	1	ro	Kod migający LED I/O (sekwencja 1 z 3)
64.011	0xFA0B	1	ro	Kod migający LED I/O (sekwencja 2 z 3)
64.012	0xFA0C	1	ro	Kod migający LED I/O (sekwencja 3 z 3)
64.013	0xFA0D	1	ro	PLC-State : 1 = Stop; 2 = Run
Elektroniczna tabliczka znamionowa				
64.016	0xFA10	4	ro	Nr katalogowy, np. 0750810100400001
64.020	0xFA14	1	ro	Wersja firmware
64.021	0xFA15	1	ro	Wersja sprzętu
64.022	0xFA16	1	ro	Firmware loader
Wersja obrazu procesu				
64.023	0xFA17	1	ro	Wersja obrazu procesu Modbus
Konfiguracja sieci				
64.032	0xFA20	3	ro	MAC-ID 1
Rejestr obrazu procesu				
64.064	0xFA40	1	ro	Liczba rejestrów wejść analogowych i dwustanowych (całkowita wielkość zakresu Modbus IN) 0x7D00
64.065	0xFA41	1	ro	Liczba rejestrów wejść analogowych 0x7D00
64.066	0xFA42	1	ro	Liczba rejestrów wejść dwustanowych 0x8000
64.067	0xFA43	1	ro	Liczba rejestrów wyjść analogowych i dwustanowych (całkowita wielkość zakresu Modbus OUT) 0x7D00
64.068	0xFA44	1	ro	Liczba rejestrów wyjść analogowych 0x7D00

Tabela 78: Rejestry Modbus WAGO

Adres Modbus		Długość danych w słowach	Dostęp	Opis
Dec	Hex			
64.069	0xFA45	1	ro	Liczba rejestrów wyjść dwustanowych 0x8000
Rejestr stałych				
64.160	0xFAA0	1	ro	Stała 0x1234
64.161	0xFAA1	1	ro	Stała 0xAAAA
64.162	0xFAA2	1	ro	Stała 0x5555
64.250	0xFAFA	1	ro	Rejestr Live

Poniżej opisano bardziej szczegółowo rejestry Modbus WAGO.

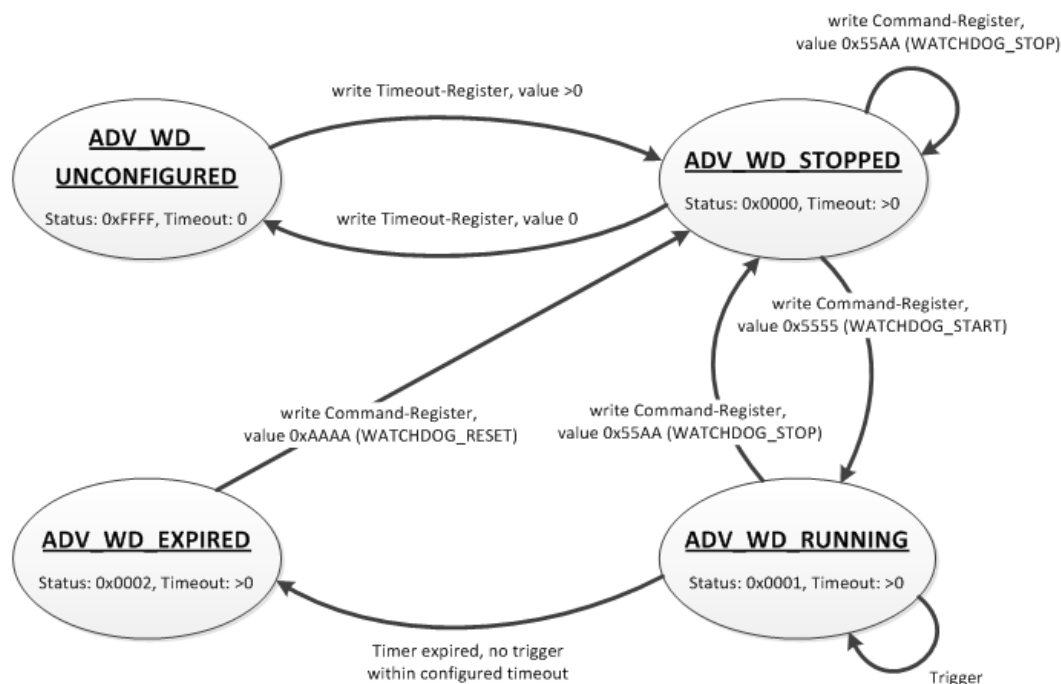
12.2.1 Modbus watchdog

Modbus watchdog monitoruje w Modbus slave bieżącą komunikację Modbus z Modbus master. Wszystkie ważne żądania Modbus pochodzące od Modbus master ze wszystkich usług obsługiwanych przez Modbus slave są zdarzeniami wyzwalającymi Modbus watchdog (patrz rozdział „Mapowanie Modbus”). Wyjątkiem są tu tryb Explizit Trigger i dostęp do rejestru 0xFA02 (Watchdog Status), które konfiguruje się w rejestrze 0xFA03 (Watchdog Config).

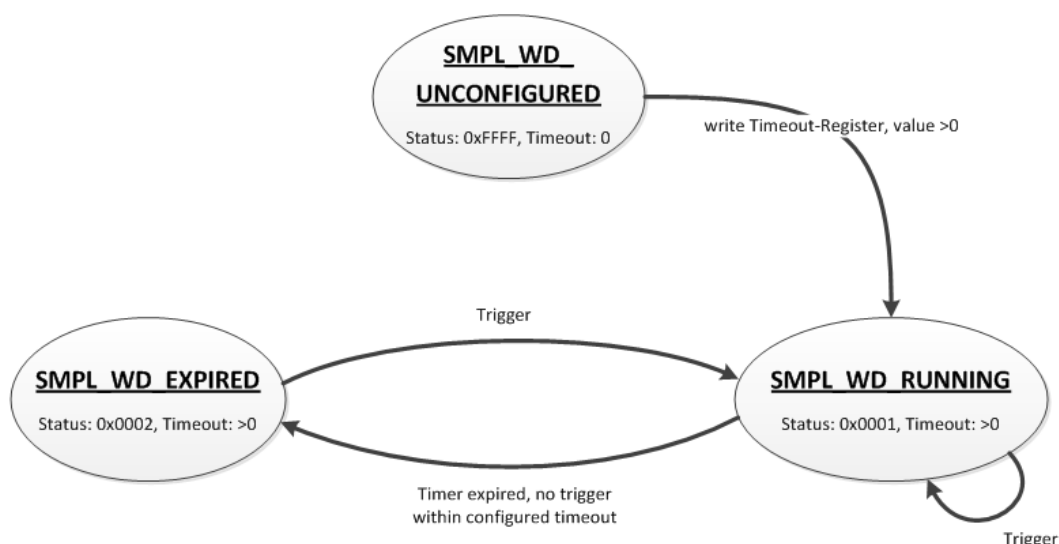
Jeżeli w trakcie czasu monitorowania ustawionego w rejestrze 0xFA01 (Watchdog Timeout) podczas działania watchdoga nie nastąpi wyzwolenie, inicjowana jest reakcja „Watchdog Timeout”. W ramach tej reakcji istnieje możliwość konfiguracji rozłączenia wszystkich połączeń Modbus TCP, patrz rejestr 0xFA03 (Watchdog Config).

Modbus watchdog obsługuje dwa różne tryby pracy: **ADVANCED_WATCHDOG** i **SIMPLE_WATCHDOG**. Odpowiedni tryb pracy wybiera się przez bit 7 w rejestrze 0xFA03 (Watchdog Config).

Poniższe diagramy obrazują możliwe stany Modbus watchdog oraz przejścia stanów dla danego trybu pracy.



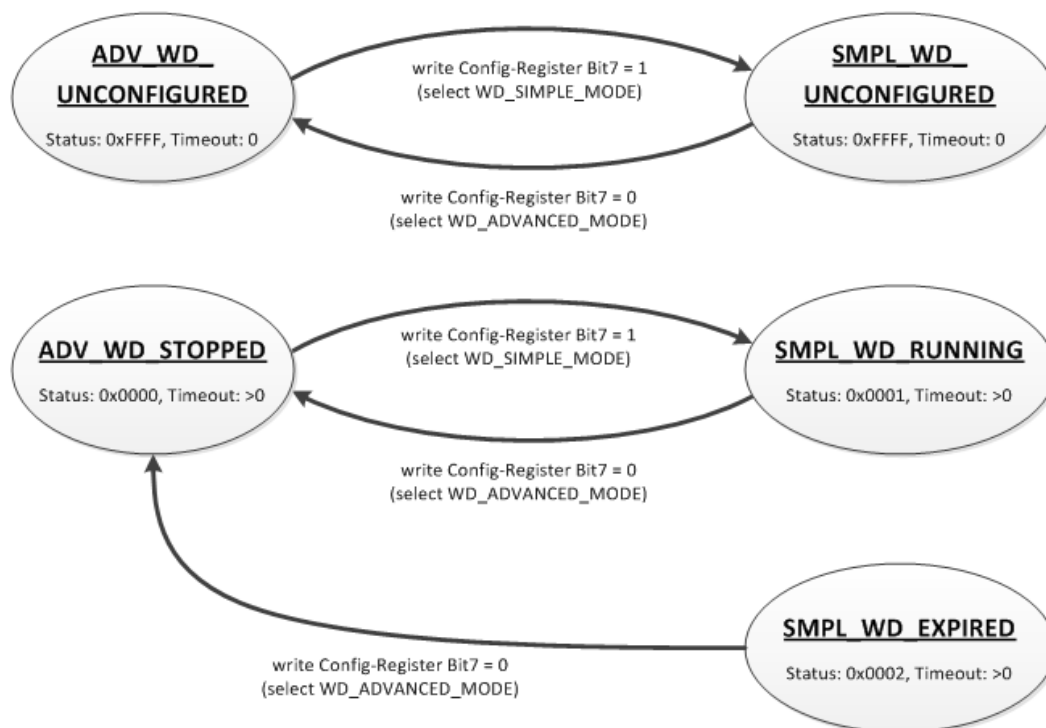
Ilustracja 119: Diagram stanów, tryb pracy **ADVANCED_WATCHDOG**



Ilustracja 120: Diagram stanów, tryb pracy SIMPLE_WATCHDOG

Diagram stanów dla trybu pracy SIMPLE_WATCHDOG pokazuje, że watchdog jest zawsze aktywny wtedy, gdy w rejestrze 0xFA01 (Watchdog Timeout) ustawiony czas monitorowania jest >0. Możliwość zapisu poleceń w rejestrze 0xFA00 (Watchdog Command) jest w tym trybie pracy ograniczona. Jako wyzwolenie dozwolone jest wyłącznie polecenie WATCHDOG_START. Jedyną możliwością dezaktywowania lub zatrzymania watchdoga w trybie pracy SIMPLE_WATCHDOG jest przełączenie z powrotem na tryb ADVANCED_WATCHDOG.

Diagram poniżej obrazuje możliwe przejścia stanów przy przełączaniu trybów pracy.



Ilustracja 121: Diagram ilustrujący możliwe stany przy przełączaniu trybów pracy

12.2.1.1 Rejestr 0xFA00 – Watchdog Command

Ten rejestr odbiera polecenia dla Modbus watchdog. Nie ma możliwości odczytu zapisanych poleceń.

Niezależnie od statusu watchdoga, akceptowane są następujące polecenia:

Tabela 79: Polecenia watchdoga

Wartość	Nazwa	Znaczenie
0x5555	WATCHDOG_START	Otwiera skonfigurowanego watchdoga. W stanie WATCHDOG_UNCONFIGURED, gdy czas monitorowania watchdoga nie jest skonfigurowany, odpowiedzią jest wyjątek ILLEGAL_DATA_VALUE (0x03). Ten sam wyjątek zwracany jest także, gdy watchdog minął (stan WATCHDOG_EXPIRED) i przy trybie pracy ADVANCED_WATCHDOG. Watchdog musi w tym przypadku najpierw zostać zresetowany przez polecenie WATCHDOG_RESET do stanu WATCHDOG_STOPPED. We wszystkich innych przypadkach watchdog jest ponownie uruchamiany i ustawiany jest stan WATCHDOG_RUNNING.
0x55AA	WATCHDOG_STOP	Zatrzymuje uruchomionego watchdoga. W stanie WATCHDOG_UNCONFIGURED, gdy czas monitorowania watchdoga nie jest skonfigurowany, odpowiedzią jest wyjątek ILLEGAL_DATA_VALUE (0x03). Ten sam wyjątek zwracany jest także, gdy watchdog minął (stan WATCHDOG_EXPIRED) i przy trybie pracy ADVANCED_WATCHDOG. Watchdog musi w tym przypadku najpierw zostać zresetowany przez polecenie WATCHDOG_RESET do stanu WATCHDOG_STOPPED. Przy typie pracy SIMPLE_WATCHDOG odpowiedzią jest wyjątek ILLEGAL_DATA_VALUE (0x03). W tym trybie pracy polecenie to jest w zasadzie niedozwolone. W każdym innym przypadku watchdog zostaje zatrzymany i ustawiany jest stan WATCHDOG_STOPPED. Wielokrotnie odebrane polecenie zatrzymania w stanie WATCHDOG_STOPPED nie ma wpływu na zachowanie watchdoga i nie wymaga potwierdzenia odpowiedzi o błędzie.

Tabela 79: Polecenia watchdoga

Wartość	Nazwa	Znaczenie
0xAAAA	WATCHDOG_RESET	Resetuje watchdoga po przekroczeniu czasu. W stanie WATCHDOG_EXPIRED i przy trybie pracy ADVANCED_WATCHDOG watchdog jest resetowany. Następnie powraca do stanu WATCHDOG_STOPPED. W każdym innym przypadku odpowiedzią jest wyjątek ILLEGAL_DATA_VALUE (0x03).

12.2.1.2 Rejestr 0xFA01 – Watchdog Timeout

Ten rejestr zawiera wartość czasu monitorowania watchdoga. Skok wynosi 1 ms, a maksymalna wartość to 65535 (odpowiada 65,535 s). Wartość domyślna wynosi 0. W tym przypadku watchdog nie może być aktywowany i znajduje się w stanie WATCHDOG_UNCONFIGURED.

Odczyt i zapis w rejestrze możliwy jest w stanach WATCHDOG_UNCONFIGURED i WATCHDOG_STOPPED. Natomiast gdy watchdog jest aktywny lub upłynął (stan WATCHDOG_RUNNING lub WATCHDOG_EXPIRED), dostęp do rejestru jest możliwy tylko w trybie odczytu. W tym przypadku zapis wywołuje odpowiedź wyjątkiem ILLEGAL_FUNCTION (0x01).

12.2.1.3 Rejestr 0xFA02 – Watchdog Status

Ten rejestr dostarcza informację o aktualnym stanie Modbus watchdog. Możliwe są następujące stany:

Tabela 80: Status watchdoga

Wartość	Nazwa	Znaczenie
0xFFFF	WATCHDOG_UNCONFIGURED	Modbus watchdog nie jest konfigurowalny, rejestr 0xFA01 (Watchdog Timeout) zawiera wartość 0. Stan ten można zmienić ustawiając czas monitorowania >0 s.
0x0000	WATCHDOG_STOPPED	Modbus watchdog jest konfigurowalny, rejestr 0xFA01 (Watchdog Timeout) zawiera wartość >0. W trybie pracy ADVANCED_WATCHDOG watchdog może być aktywowany w tym stanie za pomocą polecenia WATCHDOG_START. W trybie pracy SIMPLE_WATCHDOG stan ten nie jest dostępny, ponieważ watchdog jest aktywowany automatycznie.
0x0001	WATCHDOG_RUNNING	Modbus watchdog jest aktywny, tzn. został skonfigurowany i uruchomiony. Ustawiony czas monitorowania jeszcze nie upłynął.

Tabela 80: Status watchdoga

Wartość	Nazwa	Znaczenie
0x0002	WATCHDOG_EXPIRED	Upłynął czas monitorowania ustawiony w rejestrze 0xFA01 (Watchdog Timeout). W trybie pracy ADVANCED_WATCHDOG watchdog musi w tym stanie najpierw zostać zresetowany przez polecenie WATCHDOG_RESET do stanu WATCHDOG_STOPPED. W trybie pracy SIMPLE_WATCHDOG watchdog jest aktywowany automatycznie przy następnym wyzwoleniu.

12.2.1.4 Rejestr 0xFA03 – Watchdog Config

Ten rejestr zawiera parametry konfiguracyjne watchdoga. Rejestr jest zorientowany bitowo (patrz poniższa tabela).

W trybie pracy SIMPLE_WATCHDOG rejestr ten można odczytywać i zapisywać niezależnie od statusu watchdoga.

Natomiast w trybie pracy ADVANCED_WATCHDOG odczyt i zapis w tym rejestrze możliwy jest tylko w stanach WATCHDOG_UNCONFIGURED i WATCHDOG_STOPPED.

Gdy watchdog jest aktywny (stan WATCHDOG_RUNNING lub WATCHDOG_EXPIRED), dostęp do rejestru jest możliwy tylko w trybie odczytu. W tym przypadku zapytanie o zapis wywołuje odpowiedź wyjątkiem ILLEGAL_FUNCTION (0x01).

Tabela 81: Konfiguracja watchdoga

Bit	Nazwa/określenie bitu	Znaczenie
0	EXPLICIT_TRIGGER_ONLY	Aktywuje tryb Explizit Trigger.
		0* Watchdog jest wyzwalany przez wszystkie ważne zapytania Modbus. Wyjątkiem jest tylko dostęp do rejestru 0xFA02 (Watchdog Status).
		1 Tylko zapis w rejestrze 0xFA00 (Watchdog Command) wartości 0x5555 (WATCHDOG_START) traktowany jest jak wyzwolenie watchdoga. Również w tym przypadku wyjątkiem jest dostęp do rejestru 0xFA02 (Watchdog Status).
1	TRIGGER_ON_STATUS_REG	Aktywuje wyzwolenie watchdoga dostępem (typu odczyt) do rejestru 0xFA02 (Watchdog Status)
		0* Odczyt statusu watchdoga nie jest traktowany jako wyzwolenie watchdoga.
		1 Odczyt statusu watchdoga jest traktowany jako wyzwolenie watchdoga.

Tabela 81: Konfiguracja watchdoga

Bit	Nazwa/określenie bitu	Znaczenie	
2	CLOSE_ALL_TCP_CONNECTIONS	Aktywuje rozłączenie wszystkich połączeń Modbus TCP w momencie zakończenia czasu monitorowania (przejście do stanu WATCHDOG_EXPIRED)	
		0	Istniejące połączenia Modbus TCP pozostają otwarte.
		1*	Wszystkie istniejące połączenia Modbus TCP zostają zamknięte.
7	SELECT_ADVANCED_SIMPLE_MODE	Określa tryb pracy watchdoga	
		0*	Advanced Mode: watchdog musi być sterowany wyraźnie za pomocą poleceń (patrz rejestr 0xFA00 Watchdog Command).
		1	Simple Mode: watchdog jest aktywowany bezpośrednio przez czas monitorowania > 0 s w rejestrze 0xFA01 (Watchdog Timeout). Każde wyzwolenie powoduje restart watchdoga, zarówno działającego jak i tego, dla którego czas upłynął. Watchdog może być zatrzymany tylko przez przełączenie w Advanced Mode.
* ustawienie standardowe			

Poszczególne opcje zostają aktywowane, gdy ustawiony jest dany bit lub kombinacja bitów.

12.2.1.5 Rejestr Modbus TCP Connection Watchdog

Rejestr 0xFA04 zawiera czas trwania monitorowania połączenia TCP Modbus. Czas bazowy wynosi 10 ms. Dzięki temu długość czasu trwania można ustawić na maksymalnie 655350 ms. Jeśli rejestr zawiera wartość > 0 s podczas akceptowania nowego połączenia TCP z Modbus master, uruchamia się monitorowanie tego połączenia. Późniejsze zmiany rejestru nie mają wpływu na monitorowanie istniejących połączeń. Jeśli przy uruchomionych monitorowaniu w trakcie podanego czasu podłączony Modbus master nie odbierze żadnego telegramu, połączenie to zostaje jednostronnie zakończone resetem.

12.2.2 Rejestr statusu

12.2.2.1 Rejestr statusu PLC

Rejestr 0xFA0D dostarcza informację o statusie, w którym znajduje się sterownik. Możliwe wartości to:

- 1 = PLC Stop - PLC znajduje się w stanie STOP (został zatrzymany).
- 2 = PLC Run - PLC znajduje się w stanie RUN (działa)

12.2.3 Elektroniczna tabliczka znamionowa

Rejestr 0xFA10 ... 0xFA17 zawiera informacje z elektronicznej tabliczki znamionowej. Możliwe jest jednocześnie odczytanie całej tabliczki znamionowej lub jej następujących po sobie fragmentów.

12.2.3.1 Nr katalogowy

Rejestr 0xFA10 ... 0xFA13 informuje o numerze katalogowym sterownika WAGO.

Przykład: 0750-8202/0025-0001.

0xFA10 = 0750,
0xFA11 = 8202,
0xFA12 = 0025,
0xFA13 = 0001

12.2.3.2 Wersja firmware

Rejestr 0xFA14 zawiera wersję firmware sterownika.

12.2.3.3 Wersja sprzętu

Rejestr 0xFA15 zawiera wersję sprzętu sterownika.

12.2.3.4 Firmware loader / Boot loader

Rejestr 0xFA16 zawiera wersję firmware loader / boot loader sterownika.

12.2.4 Wersja obrazu procesu Modbus

Rejestr 0xFA17 zawiera wersję obrazu procesu Modbus sterownika.

12.2.5 Rejestr obrazu procesu Modbus

Rejestr 0xFA40 ... 0xFA45 zawiera dane o wielkości zakresów obrazu procesu sterownika dla dostępów bitowych i do rejestrów.

12.2.6 Rejestr stałych

Rejestry 0xFAA0 ... 0xFAA2 dostarczają stałych na podstawie tabeli „Rejestr Modbus WAGO”. Istnieje możliwość jednoczesnego odczytu wszystkich stałych lub ich następujących po sobie części.

0xFAA0 = 0x1234,
0xFAA1 = 0xAAAA,
0xFAA2 = 0x5555

12.2.7 Rejestr Live

Rejestr 0xFAFA służy tylko do odczytu i zawiera licznik, który jest inkrementowany każdym cyklem zadania systemu runtime przy odczycie i zapisie danych procesowych Modbus.

12.3 Obliczanie mocy CPU Modbus master

Na podstawie właściwości czasu rzeczywistego zastosowanego jądra Linux wiele punktów danych może generować wiele zmian kontekstów.

Dla jednorazowej aktualizacji (wysłanie i odebranie kodu funkcji) czas CPU może wynosić ok. 800 μ s.

Obciążenie CPU (cpu_load) w procentach można obliczyć na podstawie czasu cyklu (t_z) dla zapytania za pomocą przybliżonego wzoru:

$$\text{cpu\_load} = 800 \mu\text{s} / t_z * 100$$

Przy czasie trwania cyklu 100 ms obciążenie CPU wynosi 0,8%.

Obciążenie dla połączenia może wynosić maksymalnie ok. 20%, ponieważ jest ograniczane przez protokół sieciowy. Aby utrzymać jak najniższe obciążenie CPU,

- należy wybrać jak największy czas trwania cyklu,
- w zapytaniu należy zebrać jak najwięcej punktów danych,
- można zwiększyć minimalny interwał zapytania (wartość domyślna: 0 ms).

13 CANopen master i slave

Obraz procesu jest przetwarzany w sterowniku zgodnym z IEC 61131-3. Efektem działania sterownika jest wysterowanie wyjść (elementów wykonawczych) i/lub udostępnienie obrazu procesu do systemu nadrzędnego.

Wymiana danych procesowych odbywa się przez PDO i SDO. Aby wysłać dane procesowe przez sieć CANopen, sterownik obsługuje 512 TX PDO i 512 RX PDO oraz SDO.

W lokalnym obrazie procesu jako obszar wejść i wyjść dla wymiany danych przez interfejs CANopen przewidziany jest obszar 4000 bajtów. Znajduje się on przy adresach od 6000 do 9999. Bezpośredni dostęp do modułów I/O przez sieć obiektową nie jest przewidziany.

Pozycje wykazu obiektów mogą być w razie potrzeby mapowane na RX PDO i TX PDO. Pełny zakres danych wejściowych i wyjściowych może być transmitowany przez SDO.

13.1 Katalog obiektów

Wszystkie obiekty komunikacyjne i obiekty urządzeń zebrane są w katalogu obiektów. Poniższa tabela przedstawia ich ogólne zestawienie:

Tabela 82: Przegląd adresów w katalogu obiektów

Zakres indexów	Zastosowanie
0000	Brak zastosowania
0001-009F	Typy danych
00A0-0FFF	Zarezerwowany (adresy wykorzystywane do innych usług)
1000-1FFF	Profil komunikacji
2000-5FFF	Zakres specyficzny dla producenta
6000-9FFF	Maks. 8 standaryzowanych profili urządzeń
A000-AFFF	Obrazy procesu urządzeń IEC 61131
B000-BFFF	Obrazy procesu bramek CANopen zgodnie z CiA 302-7
C000-FFFF	Zarezerwowany

Poniżej opisano obiekty udostępniane przez sterownik.

13.2 Profil komunikacji

0x1000 Device type

Stos zgłasza się w sieci jako urządzenie DS-405 (IEC61131-3 programmable device), niezależnie od tego, czy jest skonfigurowany jako master, czy jako slave. Ponieważ nie jest możliwy bezpośredni dostęp do modułów I/O przez sieć, bity dla informacji przez wejścia/wyjścia wynoszą 0.

Wpis 0x000195 = DS 405 dla master i slave

0x1001 Error Register

Ten wpis zawiera 8-bitową informację o stanie błędu. W tym momencie wykorzystywane są następujące bity: 4 dla komunikacji i 5 dla profilu urządzenia. Bit 0 ustawiany jest przy każdym błędzie.

0x1003 Pre-defined Error Field

Ten wpis zawiera listę błędów, które zostały zasygnalizowane w rejestrze błędów 0x1001. Subindex 0 zawiera liczbę wpisów. Nowy błąd jest dodawany do subindexu 1, a wszystkie istniejące już błędy są przesuwane o jeden subindex w dół. Obsługiwanych jest maksymalnie 20 błędów. Gdy wystąpi więcej niż 20 błędów, kolejny błąd jest nadpisywany w subindexie 20. Przez wpisanie „0” w subindexie 0 cała pamięć błędów zostaje usunięta.

Standardowa wartość: 0 we wszystkich wpisach

0x1005 COB ID Sync

Obiekt definiuje COB ID dla komunikatu o synchronizacji.

Standardowa wartość: 0x80

0x1006 Communication Cycle Period

Czas trwania cyklu synchronizacji w μ s lub 0 przy braku cyklicznej synchronizacji. Wewnętrzna rozdzielczość wynosi 1 ms. Jeśli wartość wynosi 0, nie ma monitorowania synchronizacji.

Standardowa wartość: 0

0x1008 Manufacturer Device Name

Obiekt podaje nazwę urządzenia.

Wpis: nr katalogowy sterownika PFC200, np. „750-8206”

0x1009 Manufacturer Hardware Version

Wpis: „V 1.0“ lub nowsza

0x100A Manufacturer Software Version

Wpis: „V 1.00“ lub nowsza

0x100C Node Guarding Time

Obiekt podaje Guarding Time w milisekundach. NMT master odpytuje cyklicznie NMT slave o stan. Guard Time to czas między dwoma zapytaniem.

Standardowa wartość: 0 (Node Guarding dezaktywowany)

0x100D Life Time Factor

Life Time Factor jest częścią protokołu Node Guarding. NMT slave sprawdza, czy został odpytany w trakcie Node Life Time (Guardtime pomnożony przez Life Time Factor). Jeśli tak się nie stało, slave musi założyć, że NMT master nie znajduje się w normalnym trybie pracy i wyzwala Life Guarding Event.

Standardowa wartość: 0 (Node Guarding wyłączony)

0x1012h COB-ID Time Stamp Object

Obiekt Time Stamp umożliwia synchronizację zegarów we wszystkich urządzeniach w sieci. Tu podawany jest ID tego obiektu. Sygnał synchronizacji nie jest weryfikowany przez system runtime, ale może być wykorzystany z funkcjami bibliotek.

Standardowa wartość: 0x100 (Time Stamp Consumer)

0x1014h Emergency COB-ID

W przypadku błędów urządzenia CANopen wysyłany jest komunikat Emergency Message. Tu podawany jest ID tego obiektu (przy master Read-Only).

Standardowa wartość: 0x80 + ID urządzenia

0x1015h Emergency Inhibit time

Ten obiekt podaje minimalny czas, jaki musi upłynąć, zanim zostanie wysłany następny Emergency Message. Parametr 0 dezaktywuje wysyłanie z opóźnieniem. Jednostka czasu wynosi 100 μs.

Standardowa wartość: 0

0x1016h Consumer heartbeat time

Ten wpis umożliwia monitorowanie innych urządzeń w sieci. Sprawdzane jest, czy każdy moduł zdefiniowany w tym obiekcie wygenerował heartbeat w trakcie zadanego czasu. Gdy zadany czas został przekroczony, wyzwalany jest heartbeat event. Heartbeat time określany jest w milisekundach. Jeśli czas wynosi 0, monitorowanie jest dezaktywowane. Liczba monitorowanych urządzeń jest wpisywana do indexu 0, inne parametry zawierają czas heartbeat w milisekundach w najniższym bicie 16 i ID urządzenia sieciowego w bicie 8.

Standardowa wartość:

Index 0: 0 (127 = liczba możliwych parametrów)

Wszystkie inne parametry 0 (ta funkcja nie jest obsługiwana przez CAN master w wersji firmware 1.0)

0x1017h Producer heartbeat time

Obiekt określa czas między dwoma wysłanymi komunikatami heartbeat (w milisekundach). Jeśli ten czas wynosi 0, heartbeat nie jest wysyłany.

Standardowa wartość: 0

0x1200 Server SDO Parameter Channels

Tu wprowadza się parametry komunikacyjne transferu SDO jako serwera. Maksymalnie obsługiwany jest 1 kanał serwera SDO.

0x1280 ... 0x128E Client SDO Parameter Channels

Tu wprowadza się parametry komunikacyjne transferu SDO jako client. Maksymalnie obsługiwanych jest 16 kanałów Client SDO.

0x1018h Identity

Obiekt określa zastosowane urządzenie. ID producenta zawiera unikatową liczbę charakterystyczną dla producenta. Dla WAGO to ID wynosi 33. Opis urządzenia obejmuje rodzinę produktów.

Nr wersji zawiera określone zachowanie CANopen. Major Rev. No. określa funkcjonalność CANopen. Przy zmianie funkcjonalności zwiększa się także Major Rev. No. Na podstawie Minor Rev. No. można rozróżnić różne wersje o tym zachowaniu CANopen.

Subindex 0 liczba wpisów: 4

Subindex 1 Vendor ID: 33

Subindex 2 Product_code: np.8206 dla 750-8206

Subindex 3 Revision_number: 0x00010001 lub wyższa

Subindex 4 Serial_number odpowiada ostatnim 4 bajtom adresu MAC.

0x1029h Error behavior

Ten obiekt określa, jak zachowuje się slave w przypadku błędu.

Subindex 0 liczba wpisów: 1

Subindex 1 Communication Error:

- 1 brak zmiany (standard)
- 0 zmiana z Operational na Preoperational
- 2 zmiana na Stop

0x1F51 Programm Control

Przy tym obiekcie można odczytać stan PLC. Zapis jest niedozwolony.

Parametry: 0 = Stop 1 = Run 2 = Reset 3 = Clear

13.2.1 Konfiguracja mastera

Te obiekty dostępne są tylko od strony sieci, gdy master jest skonfigurowany.

0x102A NMT Inhibit Time

Ten obiekt podaje minimalny czas, jaki musi upłynąć, zanim zostanie wysłany następny telegram NMT. Parametr 0 dezaktywuje wysyłanie z opóźnieniem. Jednostka czasu wynosi 100 µs.

Standardowa wartość: 0

0x1F80 NMT Startup

Ten obiekt zawiera bity konfiguracyjne dla statusu mastera. Gdy automatyczny start jest nieaktywny, master może być uruchomiony przez zapis 0x1F w tym obiekcie.

0x1F81 ... 0x1F8A Slave Configuration

Na te listy wpisywane są skonfigurowane urządzenia slave. Wszystkie wpisy są sprawdzane lub przesyłane do urządzeń slave podczas uruchamiania mastera.

0x1F81 NMT Slave Assignment

Subindex 0:	128 = liczba możliwych wpisów
Subindex 1 ... 128	bit 0: slave obecny bit 2: slave wymagany do uruchomienia bit 3: slave resetowany przy uruchomieniu bit 8 ... 15: Guard Retry Factor bit 16 ... 31: Guard Time
Subindex 128:	cała sieć (Write-Only)

0x1F82 Request NMT

Subindex 0: 127	= liczba możliwych wpisów
Subindex	= Master Node ID Master NMT State

0x1F84 Device Type Identification

Subindex 0: 127	= liczba możliwych wpisów
Subindex 1 ... 127:	Slave Device Type

0x1F85 Vendor Identification

Subindex 0: 127 = liczba możliwych wpisów

Subindex 1 ... 127: Slave Device Type (standardowo niewykorzystywane)

0x1F86 Product Code

Subindex 0: 127 = liczba możliwych wpisów

Subindex 1 ... 127: Slave Device Type (standardowo niewykorzystywane)

0x1F87 Revision Number

Subindex 0: 127 = liczba możliwych wpisów

Subindex 1 ... 127: Slave Device Type (standardowo niewykorzystywane)

0x1F88 Serial Number

Subindex 0: 127 = liczba możliwych wpisów

Subindex 1 ... 127: Slave Device Type (standardowo niewykorzystywane)

0x1F89 Boot Time

Czas w ms między uruchomieniem urządzeń slave a gotowością operacyjną wszystkich urządzeń slave.

Standardowa wartość: 0 = dezaktywowane

0x1F8A Restore Configuration

Subindex 0: 127 = liczba możliwych wpisów

Subindex 1 ... 127: bit 0 = 1 wysyłanie Restore Configuration do slave przy starcie

13.3 Wymiana danych

W przypadku sterownika CANopen wymiana danych procesowych odbywa się przez obiekty komunikacyjne.

Każdy obiekt składa się z telegramu CAN, zawierającego maksymalnie 8 bajtów danych użytkowych i unikatowy w sieci COB-ID (Communication Object Identifier).

Za pomocą obiektów komunikacyjnych realizowana jest transmisja danych, wyzwalanie zdarzeń, sygnalizacja błędów itp.

Parametry wymagane dla obiektów komunikacyjnych oraz parametry i dane urządzenia CANopen zapisywane są w katalogu obiektów.

13.3.1 Obiekty komunikacyjne sterownika

PFC200 obsługuje następujące obiekty komunikacyjne:

512 Tx PDO dla wymiany danych procesowych wejściowych węzła sieciowego,

512 Tx PDO dla wymiany danych procesowych wyjściowych węzła sieciowego,

obiekty synchronizacyjne (SYNC) do synchronizacji sieci,

obiekty Emergency (EMCY) oraz

obiekty do zarządzania siecią

- Module Control Protocols,
- Error Control Protocols,
- Bootup Protocol.

13.3.2 Adresowanie specyficzne dla sieci obiektowej

Po skonfigurowaniu interfejsu CAN jako master lub slave, zmienne CODESYS dla sieci CAN (%QB6000 ... %QB9999 i %IB6000 ... %IB9999) są mapowane w katalogu obiektów (inicjalizacja). Urządzenie sieci CANopen stosuje 16-bitowe indexy i 8-bitowe subindexy katalogu obiektów w celu adresowania danych przez PDO lub SDO i dostępu do nich. Pozycja danych w obrazie procesu nie ma więc dla użytkownika CANopen po stronie sieci obiektowej większego znaczenia.

Wpisanie zmiennych do katalogu obiektów odbywa się osobno w zależności od typu danych (Integer8, Unsigned8, Boolean, Integer16, itd.) oraz wejścia i wyjścia. Dostęp przez PDO może mieć charakter zapisu lub odczytu. Bezpośredni dostęp przez SDO może mieć tylko charakter odczytu.

Ponieważ CANopen nie transmituje danych w sposób bitowy, zmienne zostają zebrane przez typ danych Boolean w bajtach i przyporządkowane

do odpowiedniego indexu: zmienne wejściowe przez Boolean do indexu 0xA080, zmienne wyjściowe przez Boolean do indexu 0xA500.

Przyporządkowanie danych zmiennych, które reprezentowane są w obrazie procesu 1 bajtem lub kilkoma, odbywa się analogicznie do odpowiedniego indexu.

Wskazówka



Przestrzegać kierunku transmisji danych!

Zmienne wejściowe IEC 61131-3 są definiowane z punktu widzenia sieci CAN, z punktu widzenia PFC są to zmienne wyjściowe. Odpowiednio zmienne wyjściowe IEC 61131-3 są dla PFC zmiennymi wejściowymi.

Przegląd indexów zmiennych „IEC 61131-3” zawiera poniższa tabela.

Tabela 83: Indeksowanie zmiennych „IEC 61131-3” w katalogu obiektów

Typ danych	IEC 61131-3 Zmienne wyjściowe	IEC 61131-3 Zmienne wejściowe
	Index	
Integer8	0xA000	0xA480
Unsigned8	0xA040	0xA4C0
Boolean	0xA080	0xA500
Integer16	0xA0C0	0xA540
Unsigned16	0xA100	0xA580
Integer24	0xA140	0xA5C0
Unsigned24	0xA180	0xA600
Integer32	0xA1C0	0xA640
Unsigned32	0xA200	0xA680
Float32	0xA240	0xA6C0
Unsigned40	0xA280	0xA700
Integer40	0xA2C0	0xA740
Unsigned48	0xA300	0xA780
Integer48	0xA340	0xA7C0
Unsigned56	0xA380	0xA800
Integer56	0xA3C0	0xA840
Integer64	0xA400	0xA880
Unsigned64	0xA440	0xA8C0

Przez indexy przyporządkowane dla typów danych reprezentowanych w obrazie procesu 1 bajtem (Integer8, Unsigned8 i Boolean) można od strony sieci obiektowej odczytywać bitowo dane w pamięci sterownika.

Subindex służy do wyboru określonego bajtu.

Przy zastosowaniu indexów dla większych bloków danych możliwy jest natomiast dostęp do większej ilości bajtów równocześnie.

Index Integer16 (0xA0C0) lub Unsigned16 (0xA100) pozwala uzyskać dostęp np. w postaci słowa do opisanych zmiennych wyjściowych PFC, a index 0xA140 w Integer24 do 3 bajtów.

Przykład:

Do pierwszych trzech bajtów danych wyjściowych PFC dostęp od strony sieci obiektowej uzyskuje się przez typy danych Integer lub Unsigned:

Tabela 84: Dostęp od strony sieci obiektowej do danych wyjściowych PFC

Dostęp	Dane wyjściowe PFC	Odczyt przez index (Integer / Unsigned)	Subindex
Bitowo (przez Integer8 / Unsigned8)	Bajt 6000	(0xA000 / 0xA040)	1
	Bajt 6001	(0xA000 / 0xA040)	2
	Bajt 6002	(0xA000 / 0xA040)	3
W postaci słowa (przez Integer16 / Unsigned16)	Słowo 3000 (bajt 6000/6001)	(0xA0C0 / 0xA100)	1
	Słowo 3001 (bajt 6002/6003)	(0xA0C0 / 0xA100)	2
3 bajty (przez Integer24 / Unsigned24)	Bajty 6000 ... 6002	(0xA140 / 0xA180)	1

Poniższe tabele przedstawiają przegląd adresowania danych o różnych reprezentacjach w obrazie procesu.

Każde miejsce zapisu dla zmiennych sieci obiektowej (bajt 6000 do 9999) ma przyporządkowany index w zależności od reprezentacji w obrazie procesu.

Indeksowanie ujęte w tabelach uwzględnia maksymalny index i subindex.

Wskazówka

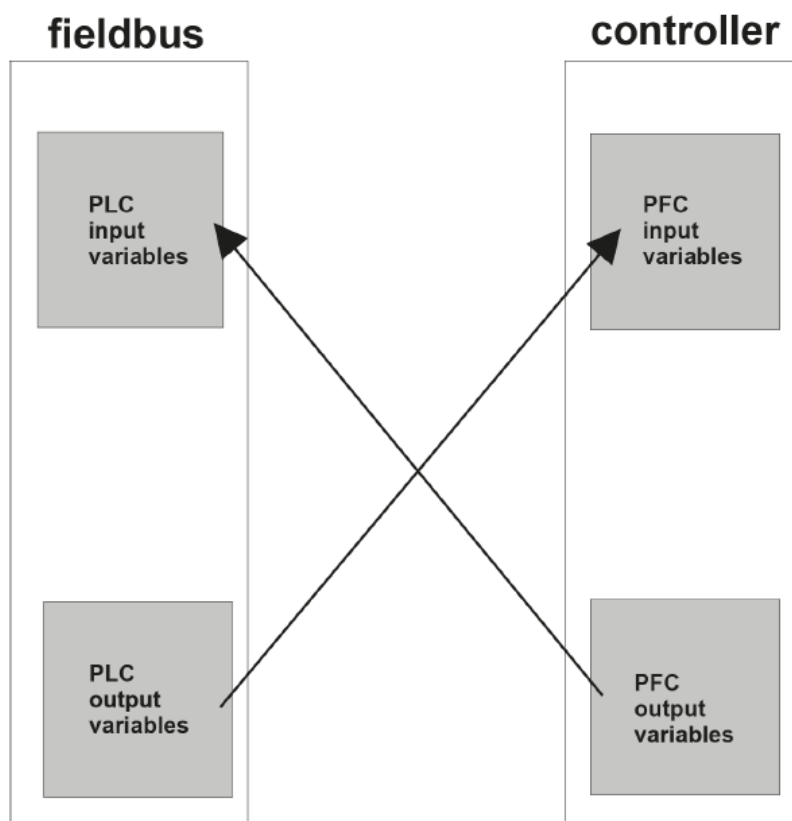


Przestrzegać kierunku transmisji danych!

Zmienne wyjściowe PFC są definiowane z punktu widzenia sterownika, z punktu widzenia sieci obiektowej CAN chodzi tu o zmienne wejściowe. Odpowiednio zmienne wejściowe PFC są dla dostępu IEC 61131-3 od strony sieci obiektowej zmiennymi wyjściowymi.

Tzn. zmienna wejściowa IEC 61131-3 = zmienna wyjściowa PFC

zmienna wejściowa PFC = zmienna wyjściowa IEC 61131-3.



Ilustracja 122: Zależność między zmiennymi „IEC 61131-3” i PFC

13.3.3 Przykłady definicji zmiennych sieciowych PFC

Poniższe przykłady przedstawiają kilka definicji zmiennych PFC o różnych typach danych w zestawieniu z odpowiadającymi im pozycjami w katalogu obiektów.

13.3.3.1 Dostęp w CODESYS do zmiennych PFC

Tabela 85: Przykłady dla dostępu w CODESYS do zmiennych PFC

Typ danych zmiennych PFC	Zmienne wejściowe PFC		Zmienne wyjściowe PFC	
	Definicja wg IEC 61131-3	Index / subindex	Definicja wg IEC 61131-3	Index / subindex
Unsigned8	InByte0 AT %IB6000: BYTE;	0xA4C0/1	OutByte0 AT %QB6000: BYTE;	0xA040/1
	InByte0 AT %IB6001: BYTE;	0xA4C0/2	OutByte0 AT %QB6001: BYTE;	0xA040/2
Integer16	InInt0 AT %IW3000: INT;	0xA540/1	OutInt0 AT %QW3000: INT;	0xA0C0/1
	InInt1 AT %IW3001: INT;	0xA540/2	OutInt1 AT %QW3001: INT;	0xA0C0/2
Unsigned16	InWord0 AT %IW3000: WORD;	0xA580/1	OutWord0 AT %QW3000: WORD;	0xA100/1
	InWord0 AT %IW3001: WORD;	0xA580/2	OutWord0 AT %QW3001: WORD;	0xA100/2
Unsigned32	InDWord0 AT %ID1500: DWORD;	0xA680/1	OutDWord0 AT %QD1500: DWORD;	0xA200/1
	InDWord0 AT %ID1501: DWORD;	0xA680/2	OutDWord0 AT %QD1501: DWORD;	0xA200/2

13.3.3.2 Indeksy maksymalne

Maksymalne indeksy i subindeksy tworzone są na podstawie wielkości pamięci sterownika sieciowego 4000 bajtów i reprezentacji w obrazie procesu tych typów danych.

Przegląd maksymalnych indexów i subindexów zmiennych IEC 61131-3 zawiera poniższa tabela.

Tabela 86: Maksymalne indeksy i subindeksy zmiennych „IEC 61131-3”

Typ danych	IEC 61131-3 Zmienne wejściowe		IEC 61131-3 Zmienne wyjściowe	
	Maks. index	Maks. subindex	Maks. index	Maks. subindex
Integer8	0xA00F	0xFF	0xA487	0xFF
Unsigned8	0xA04F	0xFF	0xA4C7	0xFF
Boolean	0xA08F	0xFF	0xA507	0xFF
Integer16	0xA0C7	0xFF	0xA543	0xFF
Unsigned16	0xA107	0xFF	0xA583	0xFF
Integer24	0xA145	0x55	0xA5C0	0x55
Unsigned24	0xA185	0x55	0xA600	0x55
Integer32	0xA1C3	0xFF	0xA643	0xFF
Unsigned32	0xA203	0xFF	0xA683	0xFF
Float32	0xA243	0xFF	0xA6C3	0xFF
Unsigned40	0xA283	0x33	0xA703	0x33
Integer40	0xA2C3	0x33	0xA743	0x33
Unsigned48	0xA302	0xAA	0xA780	0xAA
Integer48	0xA342	0xAA	0xA7C0	0xAA
Unsigned56	0xA382	0x49	0xA802	0x49
Integer56	0xA3C2	0x49	0xA842	0x49
Integer64	0xA401	0xFF	0xA880	0xFF
Unsigned64	0xA441	0xFF	0xA8C0	0xFF

Przykład:

514 bajtów zmiennych wyjściowych adresowanych jest w postaci słowa za pomocą typu danych Unsigned16.

Adresowanie 257 słów danych odbywa się w następujący sposób:

- Index 0xA580, subindex 1 do 255
- Index 0xA581, subindex 1 i 2.

Tabela 87: Przykład dla zmiennych wyjściowych „IEC 61131-3“

Index	Subindex	Spis treści	Opis
0xA580	1	D1 *)	1. blok zmiennych wyjściowych
	2	D2 *)	2. blok zmiennych wyjściowych
	...	...	...
	255	D255 *)	255. blok zmiennych wyjściowych
0xA581	1	D256 *)	256. blok zmiennych wyjściowych
	2	D257 *)	257. blok zmiennych wyjściowych

*) D1 = słowo danych zmiennych wyjściowych 1, D255 = słowo danych zmiennych wyjściowych 255, itd.

13.3.4 Konfiguracja CANopen master

Wskazówka Wywołanie na podstawie adresów lub symbolicznych nazw wejść i wyjść

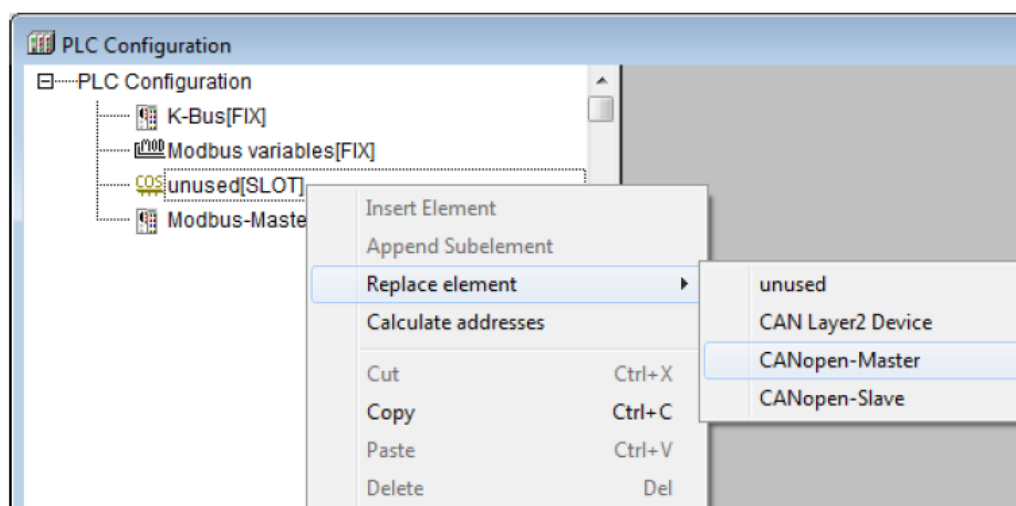


Wskazane jest jawne wywołanie adresów lub symbolicznych nazw wejść i wyjść, gdyż w przeciwnym razie obraz procesu nie zostanie zaktualizowany. Alternatywnie można również utworzyć przy adresach IB%6000 lub QB%6000 Array wielkość maks. 240 bajtów. Ten Array można wywołać w programie PLC.

Zanim aplikacja uzyska dostęp do podłączonej sieci CAN, sieć musi zostać skonfigurowana w CODESYS.

13.3.4.1 Wybór mastera

W celu dodania urządzenia CANopen master do konfiguracji sterownika należy kliknąć prawym przyciskiem myszy „COS unused[Slot]” i wybrać „Replace element -> CANopen Master”.



Ilustracja 123: Dodawanie CANopen master

13.3.4.2 Ustawianie parametrów mastera

W zakładce parametrów bazowych nie trzeba nic wpisywać.

The screenshot shows a software window with three tabs: 'Base parameters', 'CAN parameters', and 'Module parameters'. The 'Base parameters' tab is active. It contains the following fields:

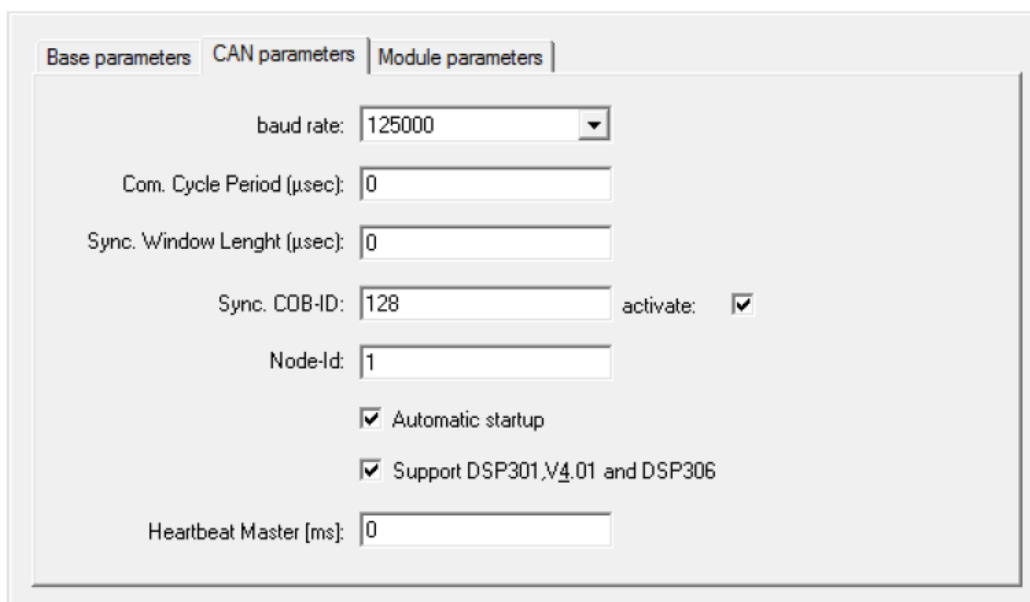
- Module id: 5
- Node id: 3
- Input address: %I6000
- Output address: %Q6000
- Diagnostic address: %M6000
- Comment: (empty text box)

Ilustracja 124: Zakładka parametrów bazowych (master)

Tabela 88: Opis parametrów bazowych (master)

Parametr	Znaczenie
Module ID	Parametry wykorzystywane w systemie runtime CODESYS
Node ID	
Input address	
Output address	
Diagnostic address	
Comment	Pole na komentarz

W zakładce parametrów CAN konieczne jest z reguły tylko sprawdzenie prędkości transmisji.



The screenshot shows the 'CAN parameters' configuration window. It includes the following settings:

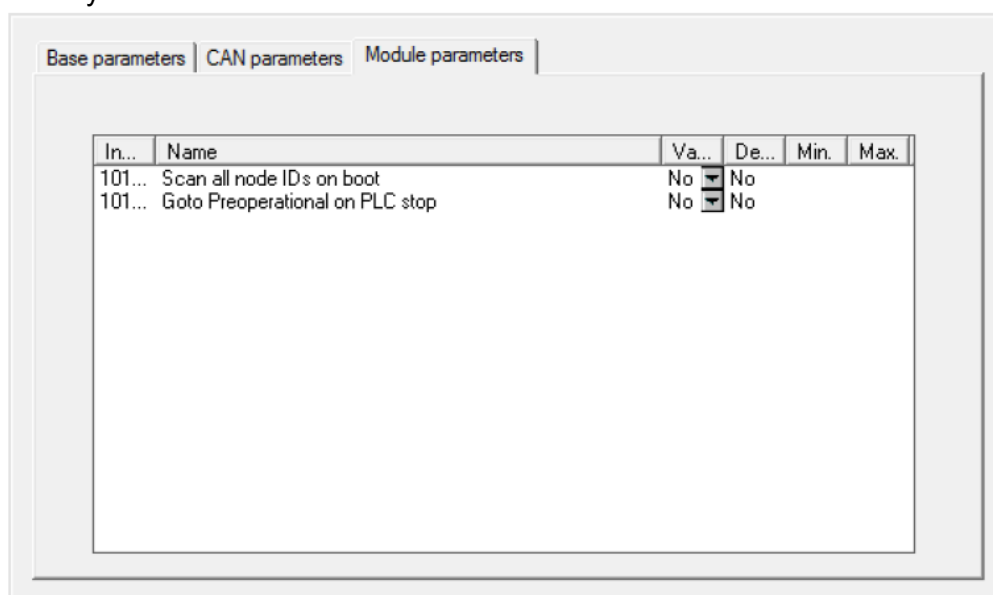
- baud rate:** 125000 (selected from a dropdown menu)
- Com. Cycle Period (µsec):** 0
- Sync. Window Length (µsec):** 0
- Sync. COB-ID:** 128, with the **activate:** checkbox checked.
- Node-Id:** 1
- ☒ Automatic startup
- ☒ Support DSP301,V4.01 and DSP306
- Heartbeat Master [ms]:** 0

Ilustracja 125: Zakładka parametrów CAN (master)

Tabela 89: Opis parametrów CAN (master)

Parametr	Znaczenie
Baud rate	Tu wybiera się żadaną prędkość transmisji w sieci CAN (ustawienie fabryczne: 125000 Bd).
Com. Cycle Period (µsec)	Tu wpisuje się interwał czasowy (w µsec), z jakim sterownik ma wysyłać komunikat synchronizacyjny. Najmniejszy interwał czasowy: 1000 µsec
Sync. Window Lenght (µsec)	Aktualnie niezaimplementowany.
Sync. COB-ID	Tu można aktywować lub dezaktywować wysyłanie komunikatów synchronizacyjnych sterownika. ustawienie fabryczne: COB-ID 128 (0x80).
Node-ID	Adres stacji (Node-ID) sterownika w sieci CAN
Automatic startup	Po zaznaczeniu tego pola sterownik ustawia automatycznie urządzenia CAN master i slave w tryb „Operational“ na podstawie zdefiniowanych parametrów. Po dezaktywowaniu tego pola uruchomienie można wykonać za pomocą polecenia biblioteki CIA405NMT.
Support ... DSP 301	Po zaznaczeniu tego pola konfiguracja sterownika obsługuje modułarne urządzenia CAN slave oraz niektóre dodatkowe rozszerzenia wynikające z norm DSP301 V3.01 i DSP306.
Heartbeat master	Gdy opcja „Heartbeat Generation“ jest aktywna, urządzenie CAN wysyła heartbeats w interwałach (liczonych w ms) zadanych w „Heartbeat Producer Time“. Aktualnie użycie heartbeat nie jest zaimplementowane.

W zakładce parametrów modułu można zdefiniować reakcję mastera przy starcie i zatrzymaniu.



Ilustracja 126: Zakładka parametrów modułu (master)

Tabela 90: Opis parametrów modułu (master)

Parametr	Znaczenie
Scan all node IDs on boot	Gdy ta opcja jest ustawiona, przy starcie odpytywane są wszystkie Node-ID. Jeśli Node istnieje, odbierane są od niego wiadomości EMC.
Goto Preoperational on PLC stop	Gdy ta opcja jest ustawiona, master zmienia stan na „Operational” dopiero wtedy, gdy runtime CODESYS znajduje się w stanie „Run”. Kiedy runtime przechodzi w stan „Stop”, master zmienia stan na „Preoperational”.

13.3.4.3 Dodawanie urządzeń slave

W celu wyboru jednego lub kilku urządzeń CANopen slave należy kliknąć prawym przyciskiem myszy CANopen master i wybrać „Attach subelements”. W poniższym przykładzie jako slave wybrano urządzenie 750-337.

Wskazówka



Pliki EDS dla urządzeń pochodzących od innych producentów

Pliki EDS aktualnych komponentów WAGO I/O System są zintegrowane w plikach docelowych sterownika. Do integracji urządzeń nie pochodzących od WAGO wymagane są pliki EDS specyficzne dla tych urządzeń. W tym celu na pasku menu wystarczy kliknąć „Tools” > „Add configuration file”.

Wskazówka



Dołączone pliki EDS stosować tylko w CODESYS 2.3!

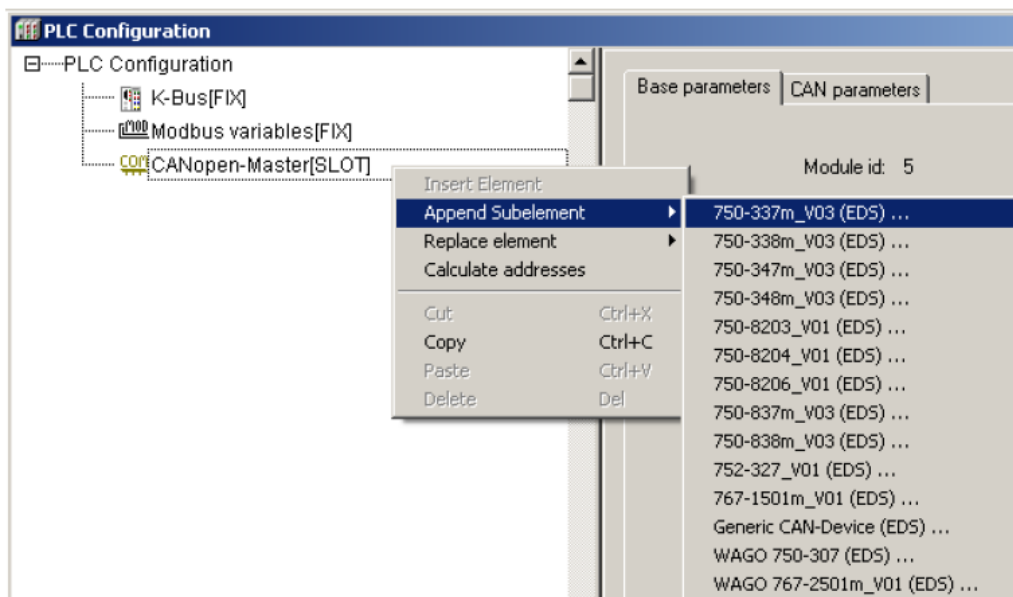
Pliki EDS dla PFC200 CANopen slave, znajdujące się w plikach docelowych sterownika, mogą być zastosowane tylko wtedy, gdy w sterowniku wykorzystany jest system runtime CODESYS 2.3!

Wskazówka



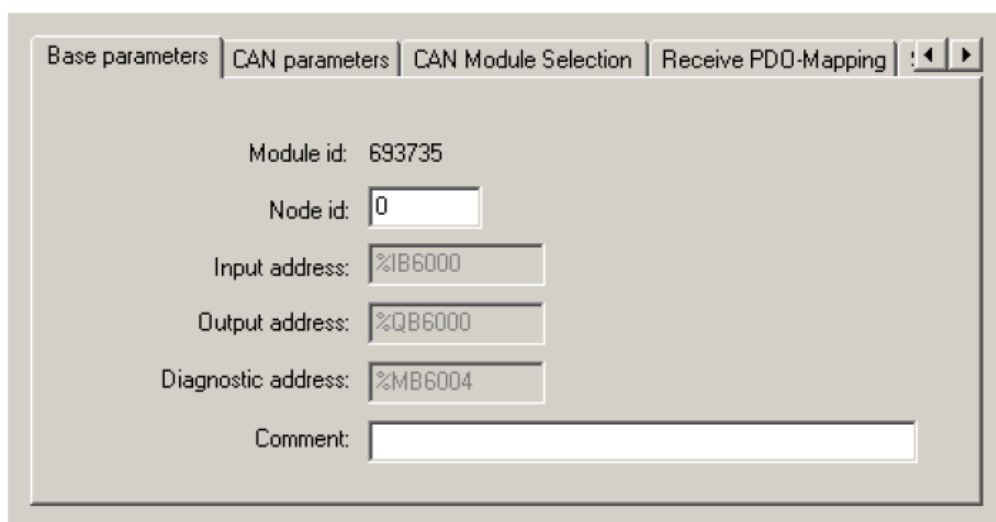
Stosować tylko pliki EDS dostosowane do wersji firmware!

Należy stosować tylko pliki EDS dostosowane do wersji firmware sterownika! W przeciwnym razie podczas pracy mogą wystąpić błędy. Te pliki EDS zintegrowane są w plikach docelowych dostosowanych do wersji firmware.



Ilustracja 127: Dodawanie urządzeń CANopen slave

W zakładce parametrów bazowych nie trzeba nic wpisywać.



Ilustracja 128: Zakładka parametrów bazowych (slave)

Tabela 91: Opis parametrów bazowych (slave)

Parametr	Znaczenie
Module ID	Pozwala rozpoznać urządzenie slave.
Node ID	Numer węzła urządzenia slave zastosowany w środowisku CODESYS.
Input address	Początkowy adres danych wejściowych: przestrzeń adresowa rozpoczyna się zawsze na %IB 6000 i jest nadawana automatycznie.
Output address	Początkowy adres danych wyjściowych: przestrzeń adresowa rozpoczyna się zawsze na %QB 6000 i jest nadawana automatycznie.
Diagnostic address	Obszar pamięci dla przetwarzania wewnętrznych informacji diagnostycznych.
Comment	Pole na komentarz

W zakładce „CAN parameters” wystarczy z reguły sprawdzić tylko Node ID.

The screenshot shows the 'CAN parameters' configuration window. It has four tabs: 'Base parameters', 'CAN parameters' (selected), 'CAN Module Selection', and 'Receive PDO-Mapping'. The 'CAN parameters' tab contains several sections:

- General:** Includes a 'Node ID' field set to 2. Below it are checkboxes for 'Write DCF', 'Create all SDO's', 'Reset Node', 'MappingSDOs' (checked), 'CommSDOs' (checked), and 'BasicSDOs' (checked).
- Node guard:** Includes a checked 'Nodeguarding' checkbox. Below it are fields for 'Guard COB-ID' (0x700+NodeID), 'Guard time (ms)' (0), and 'Life time factor' (0). An 'Info...' button is to the right.
- Heartbeat settings:** Includes checked checkboxes for 'Activate heartbeat generation' and 'Activate heartbeat consumer'. A 'Heartbeat producer time' field is set to 0 ms.
- Emergency telegram:** Includes a checked 'Emergency' checkbox and a 'COB-ID' field set to \$NodeID+0x80.
- Communication Cycle:** Includes an unchecked 'Cycle' checkbox and a 'Period (µsec)' field set to 0.

Ilustracja 129: Zakładka „CAN parameters” (slave)

Tabela 92: Opis parametrów CAN (slave)

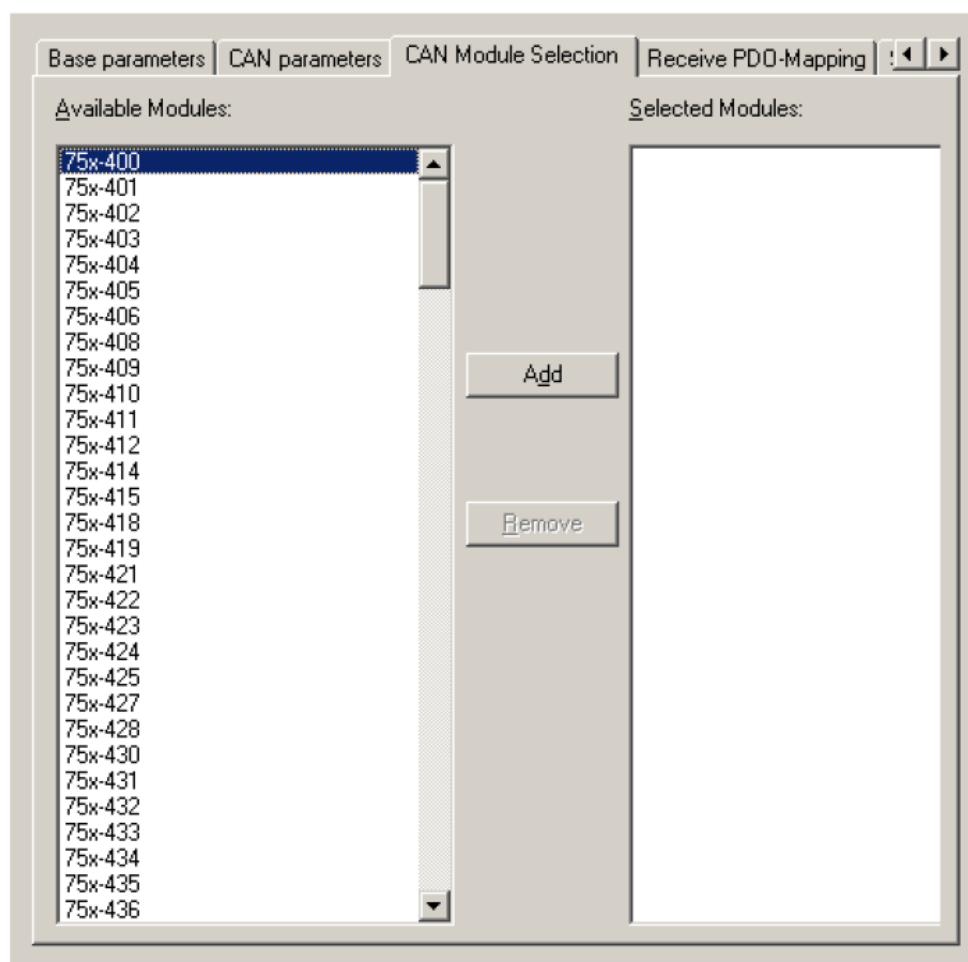
Parametr	Znaczenie
Informacje ogólne	
Node ID	Node ID (1 ... 126) jest adresem stacji, pod którym sterownik komunikuje się z urządzeniem slave w sieci CAN.
Write DCF	Aktualnie niezaimplementowane.
Generate all SDOs	Gdy pole to jest zaznaczone, tworzone są SDO dla wszystkich obiektów z pliku EDS. Dodatkowo można aktywować także wymagane opcje. Jeśli np. mają być zapisane obiekty Nodeguarding, należy aktywować także opcję „Nodeguarding”. Gdy pole nie jest zaznaczone, tworzone są SDO tylko dla tych obiektów, przy których występuje odstępstwo od wartości domyślnych z pliku EDS.
Reset node	Gdy pole to jest zaznaczone, slave jest resetowany przez sterownik PFC200 (otrzymuje „Reset-Node”), zanim zostanie wysłana do niego konfiguracja. Funkcja nie jest aktualnie zaimplementowana.
Mapping SDOs	Tu aktywuje się i dezaktywuje każdy z trzech zakresów SDO konfiguracji slave.
Comm SDOs	Mapping SDOs: Obiekty 0x1600 ... 0x1620 Obiekty 0x1A00 ... 0x1A20 Comm SDOs:
Basic SDOs	Obiekty 0x1400 ... 0x1420 Obiekty 0x1800 ... 0x1820 Basics SDOs: Obiekty 0x100C ... 0x1017
Nodeguard	
Nodeguarding	Gdy Nodeguarding jest aktywny, slave monitoruje sterownik pod kątem ewentualnej przerwy w komunikacji w ramach sieci obiektowej.
Guard COB-ID	Ustawienie fabryczne: 0x700 + Node-ID.
Guard Time (ms)	Przy „Guard Time” należy podać interwał, określający czas oczekiwania PFC na potwierdzenie („Confirmation”) od slave.
Life Time Factor	W polu „Life Time Factor” (≥ 2) ustawia się wartość zwielokrotnienia dla „Guard Time”. Po upływie czasu zadanego w polu „Guard Time” i zwielokrotnionego przez „Life Time Factor” („Node Life Time”) slave wraca do pierwotnie zdefiniowanego stanu. „0” dezaktywuje tę funkcję.
Heartbeat Settings	
Activate heartbeat generation	Gdy opcja „Heartbeat Generation” jest aktywna, urządzenie CAN wysyła heartbeats w interwałach

Tabela 92: Opis parametrów CAN (slave)

Parametr	Znaczenie
Heartbeat Producer Time (ms)	(liczonych w ms) zadanych w „Heartbeat Producer Time”. „0” dezaktywuje tę funkcję.
Activate heartbeat consumption	Gdy opcja „Heartbeat Consumption” jest aktywna, urządzenie CAN monitoruje „Heartbeat” mastera. Do monitorowania może być użyty tylko „Heartbeat” lub „Nodeguarding”.
Emergency Telegram	
Emergency	Gdy pole to jest zaznaczone, slave wysyła komunikaty o błędzie/statusie, które są podłączane jako komunikaty Emergency do adresu diagnostycznego w obszarze znaczników. Te komunikaty o błędzie i statusie można odczytać za pomocą „BusDiag.lib”. Gdy pole to nie jest zaznaczone, SDO 0x1014 nie jest przesyłany do urządzenia slave. Domyślne ustawienie slave jest tym samym ponownie aktualne.
COB-ID	Ustawienie domyślne: Node-ID + 0x80
Communication Cycle	
Cycle	Funkcja ta nie jest aktualnie zaimplementowana.
Period (µsec)	

Za pomocą przycisku **[Info ...]** można wyświetlić parametry „FileInfo” i „DeviceInfo” z pliku EDS.

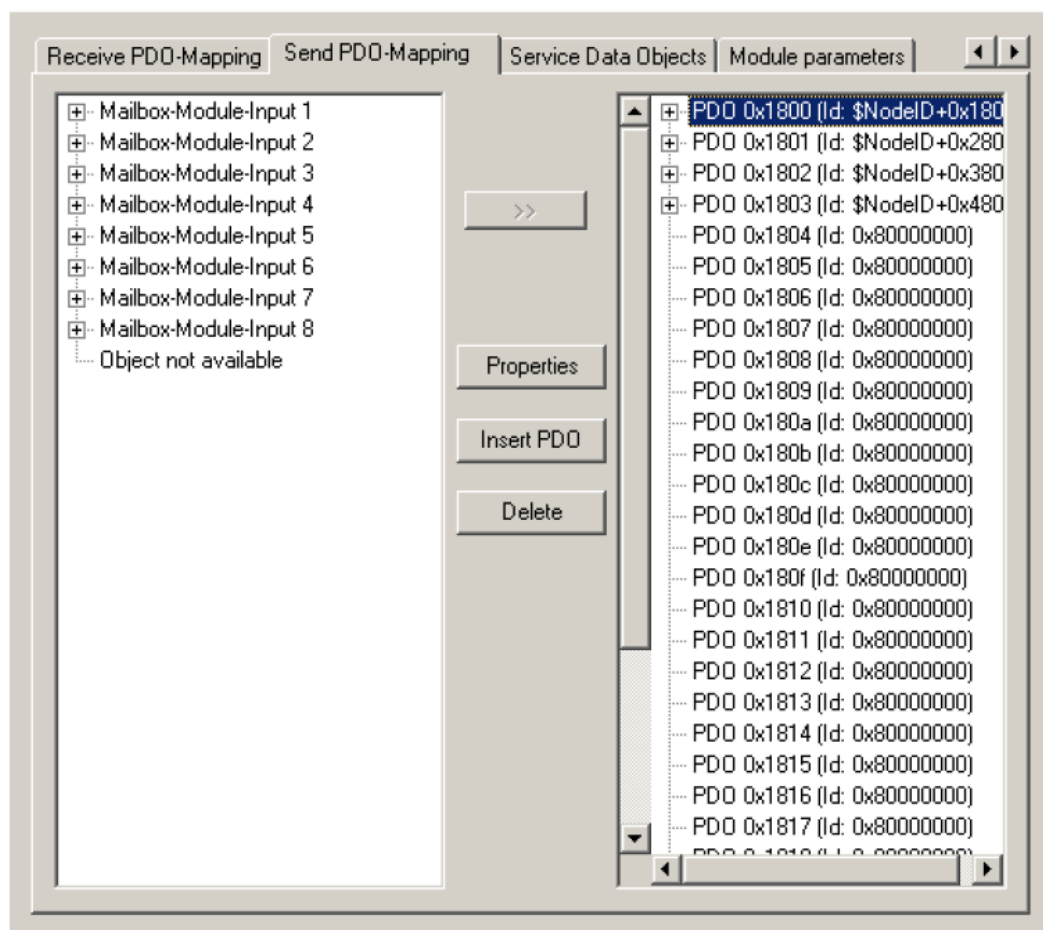
W zakładce „CAN Module Selection” wyświetlane są podłączone moduły I/O.
W tym przykładzie uwzględniono po jednym 8-bitowym module wejść i wyjść.



Ilustracja 130: Zakładka „CAN Module Selection”

13.3.4.4 Konfiguracja PDO dla urządzeń slave

Tutaj należy skonfigurować dla urządzeń slave odbiorcze PDO (wyjście z punktu widzenia sterownika) oraz nadawcze PDO. PDO dla modułów zostały już utworzone przez konfigurator. W pierwszym PDO umieszczono 8 bitów.

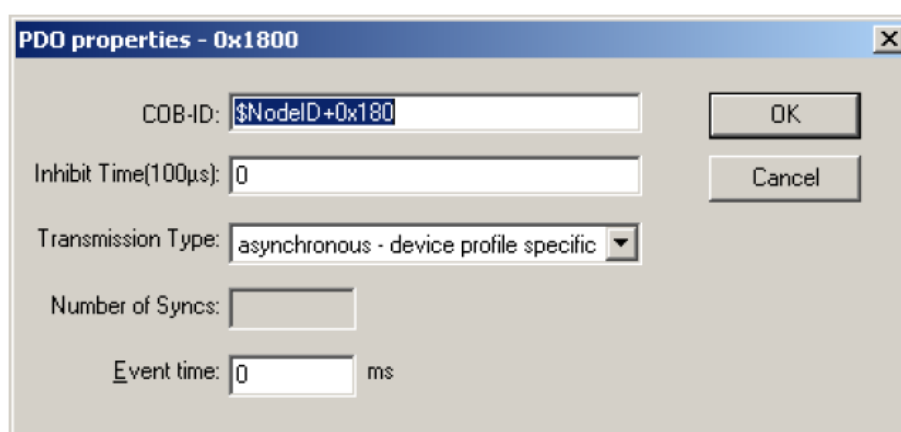


Ilustracja 131: Zakładka „PDO-Mapping“

Tabela 93: Opis mapowania PDO nadawczych i odbiorczych

Parametr	Znaczenie
Insert PDO	W zależności od wybranych modułów I/O dla CANopen slave w zakładce „Receive PDO-Mapping“ (PFC → Slave) i „Send PDO-Mapping“ (Slave → PFC) pojawiają się odpowiednie obiekty CANopen. W tych zakładkach można zmienić „Default-Mapping“ opisany w pliku EDS. Za pomocą przycisku [Insert PDO] można dopasować PDO do topologii modułów I/O. Otworzy się okno właściwości PDO, w którym można przypisać określone właściwości do PDO. Więcej informacji na ten temat można znaleźć w sekcji „Features”. Aby przyporządkować PDO do obiektu z lewego okna, należy zaznaczyć zarówno dany obiekt, jak i odpowiedni PDO i kliknąć [>>]. Obiekt jest następnie wstawiany poniżej PDO w prawym oknie. Pierwsze 64 dwustanowe i pierwszych 12 analogowych wejść i wyjść zostaje automatycznie przyporządkowanych do PDO 1 ... 4.
Remove	Za pomocą przycisku [Remove] usuwa się z konfiguracji pozycję widoczną w prawym oknie.
Features	Otwiera okno dialogowe właściwości PDO (patrz następna strona).

Przycisk ten służy do dalszej konfiguracji PDO.



Ilustracja 132: Okno właściwości PDO

Tabela 94: Opis okna właściwości PDO

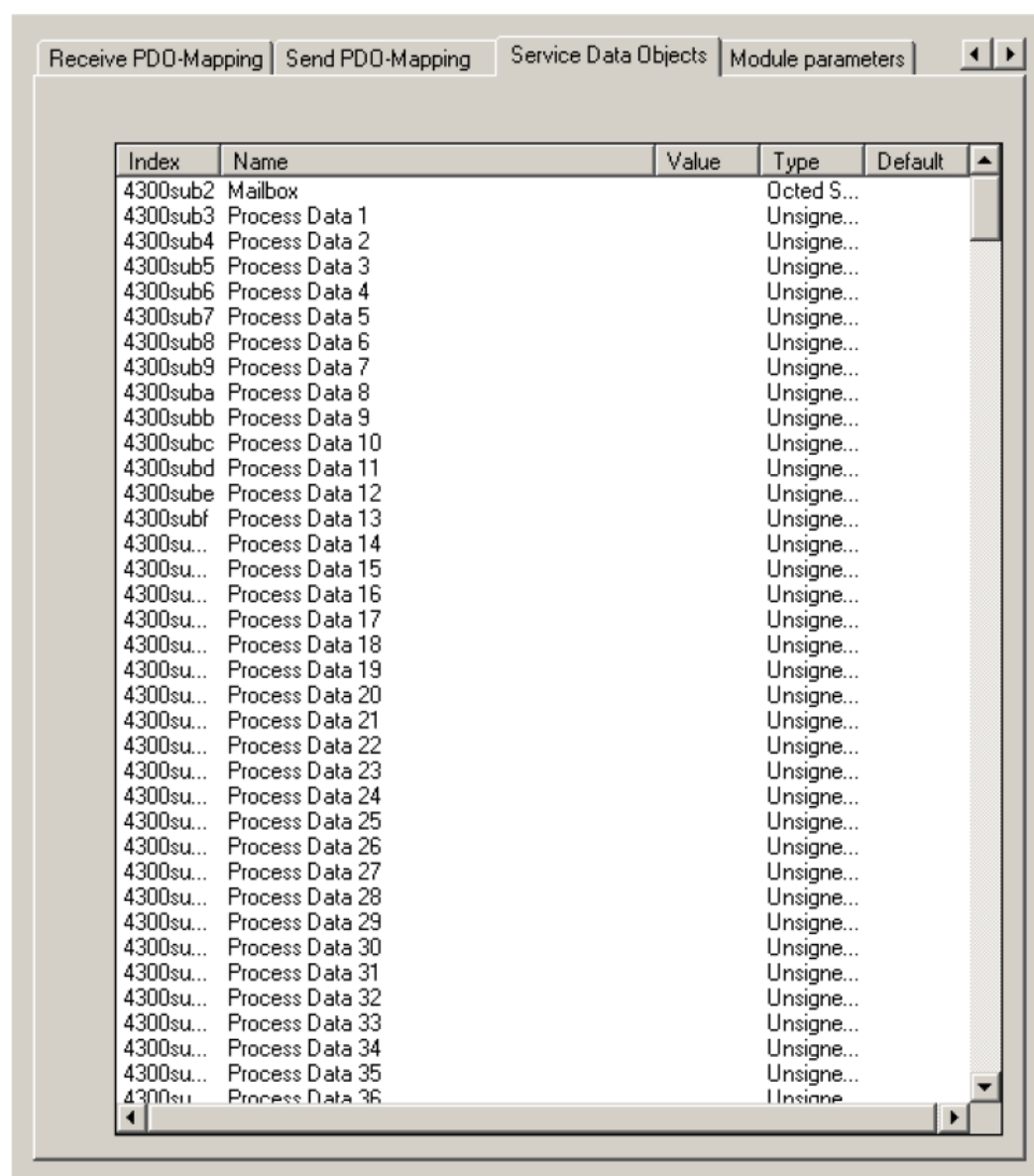
Parametr	Znaczenie
COB-ID	Identyfikator CAN
Inhibit Time (* 100 μ s)	Tu ustawia się czas, jaki musi upłynąć, aby PDO mógł znowu być wysłany. Przy komunikacji synchronicznej wartość ta nie jest wykorzystywana. W przypadku odbiorczego PDO wartość ta nie ma znaczenia.
Transmission Type	Tu wybiera się tryb transmisji dla PDO: acykliczny-synchroniczny: (typ transmisji 0) PDO przesyłany jest synchronicznie, ale nie periodycznie. Dla odbiorczych PDO typy transmisji 0 – 240 traktowane są na równi. cykliczny-synchroniczny: (typ transmisji 1 – 240) PDO przesyłany jest synchronicznie, przy czym „Number of Syncs” oznacza liczbę komunikatów synchronizacyjnych między dwoma transmisjami PDO. Dla odbiorczych PDO typy transmisji 0 – 240 traktowane są na równi. synchroniczny - tylko RTR: (typ transmisji 252) PDO jest aktualizowany po komunikacie synchronizacyjnym, ale nie jest wysyłany. Transmisja następuje tylko na wyraźne żądanie „Remote Transmission Request” (niezaimplementowane). asynchroniczny – tylko RTR: (typ transmisji 253) PDO jest aktualizowany i przesyłany tylko na wyraźne żądanie „Remote Transmission Request” (niezaimplementowane). asynchroniczny-specyficzny dla producenta: (typ transmisji 254) PDO jest przesyłany tylko po określonych zdarzeniach. asynchroniczny-specyficzny dla urządzenia: (typ transmisji 255) PDO jest przesyłany tylko po określonych zdarzeniach.

Tabela 94: Opis okna właściwości PDO

Parametr	Znaczenie
Number of Syncs	W zależności od „Transmission Type“ w polu tym można wpisać liczbę komunikatów synchronizacyjnych 1 ... 240. W przypadku odbiorczego PDO wartość ta nie ma znaczenia.
Event-Time	W zależności od „Transmission Type“, w tym miejscu należy wprowadzić odstęp czasu (w ms) między dwiema transmisjami PDO. W przypadku odbiorczego PDO wartość ta nie ma znaczenia.

13.3.4.5 Konfiguracja obiektów Service Data

Oprócz konfiguracji w omówionych wyżej zakładkach można dodatkowo konfigurować obiekty Service Data.



Ilustracja 133: Zakładka „Service Data Objects“

Tutaj wymienione są wszystkie obiekty pliku EDS, które znajdują się w obszarze indexów 0x2000 do 0x9FFF.

Dla każdego z nich podano index, wartość, typ i wartość domyślną.

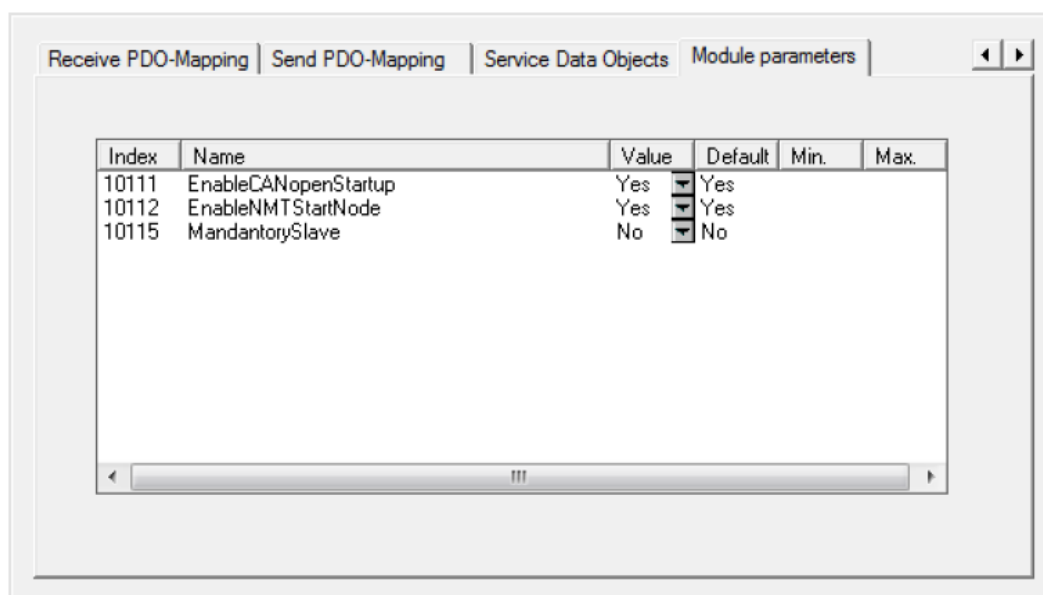
Wartość obiektów można zmieniać. W tym celu należy zaznaczyć odpowiednie pole w kolumnie „Value” i wprowadzić swoją wartość, a następnie nacisnąć klawisz **[Enter]**. Przy instalacji sieci CAN, ustawione wartości są przesyłane do urządzeń slave w postaci SDO.

Przykładem tego jest aktywacja transmisji PDO przy zmianie wartości analogowych, która jest domyślnie wyłączona:

5201su...	module 57	0	Unsigne...	0
5201su...	module 58	0	Unsigne...	0
5201su...	module 59	0	Unsigne...	0
5201su...	module 60	0	Unsigne...	0
5201su...	module 61	0	Unsigne...	0
5201su...	module 62	0	Unsigne...	0
5201su...	module 63	0	Unsigne...	0
5201su...	module 64	0	Unsigne...	0
6005	Global Interrupt Enable Digital 8-Bit	0x01	Unsigne...	0x01
6423	Analogue Input Global Interrupt Enable	0x01	Unsigne...	0x00
67fesub1	Communication error	0	Unsigne...	0

Ilustracja 134: Dostosowanie SDO

W zakładce „Module parameters” można ustawić parametry początkowe urządzenia slave.



Ilustracja 135: Zakładka „Module parameters” (slave)

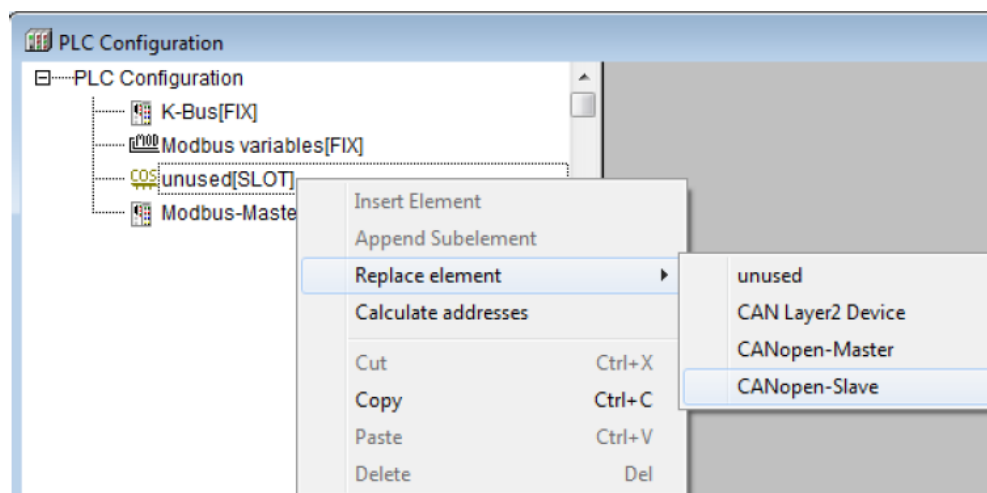
Tabela 95: Opis parametrów modułu (slave)

Parametr	Znaczenie
EnableCANopenStartup	Yes (domyślnie): Podczas fazy rozruchu sieci CANopen wszystkie Basic-SDO-Frames są wysyłane do CANopen slave. No: W tym ustawieniu SDO-Frames nie są wysyłane do CANopen slave.
EnableNMTStartNode	Yes (domyślnie): W fazie rozruchu sieci CANopen do wybranego urządzenia slave wysyłany jest komunikat NMT „Start remote node” (nawiązywane jest połączenie komunikacyjne). No: W tym ustawieniu komunikat startu nie jest wysyłany. CANopen slave może być potem uruchomiony w dowolnym momencie za pomocą polecenia „Start remote node”. Wskazówka: należy dezaktywować parametr „Start automatically”.
MandantorySlave	Gdy ta opcja jest ustawiona, master zmienia stan na „Operational” tylko wtedy, gdy obecny jest dany slave.

13.3.5 Konfiguracja CANopen slave

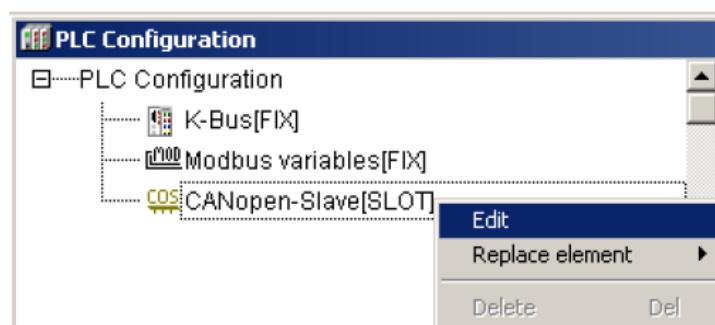
Zanim aplikacja uzyska dostęp do podłączonej sieci CAN, sieć musi zostać skonfigurowana w CODESYS.

W celu dodania CANopen slave do konfiguracji sterownika należy kliknąć prawym przyciskiem myszy „COS unused[Slot]” i wybrać „Replace element -> CANopen Slave”.



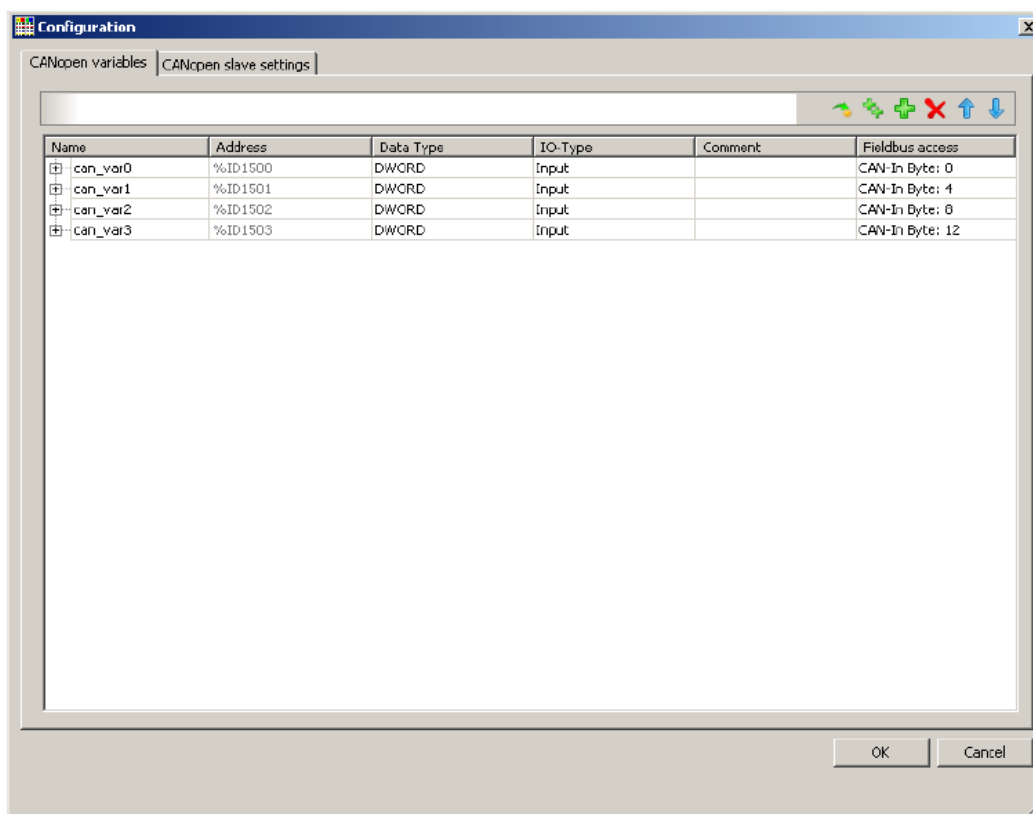
Ilustracja 136: Dodawanie CANopen slave

W celu skonfigurowania urządzenia slave należy kliknąć prawym przyciskiem myszy CANopen slave i wybrać „Edit”.



Ilustracja 137: Konfiguracja CANopen slave

13.3.5.1 Konfiguracja zmiennych CANopen



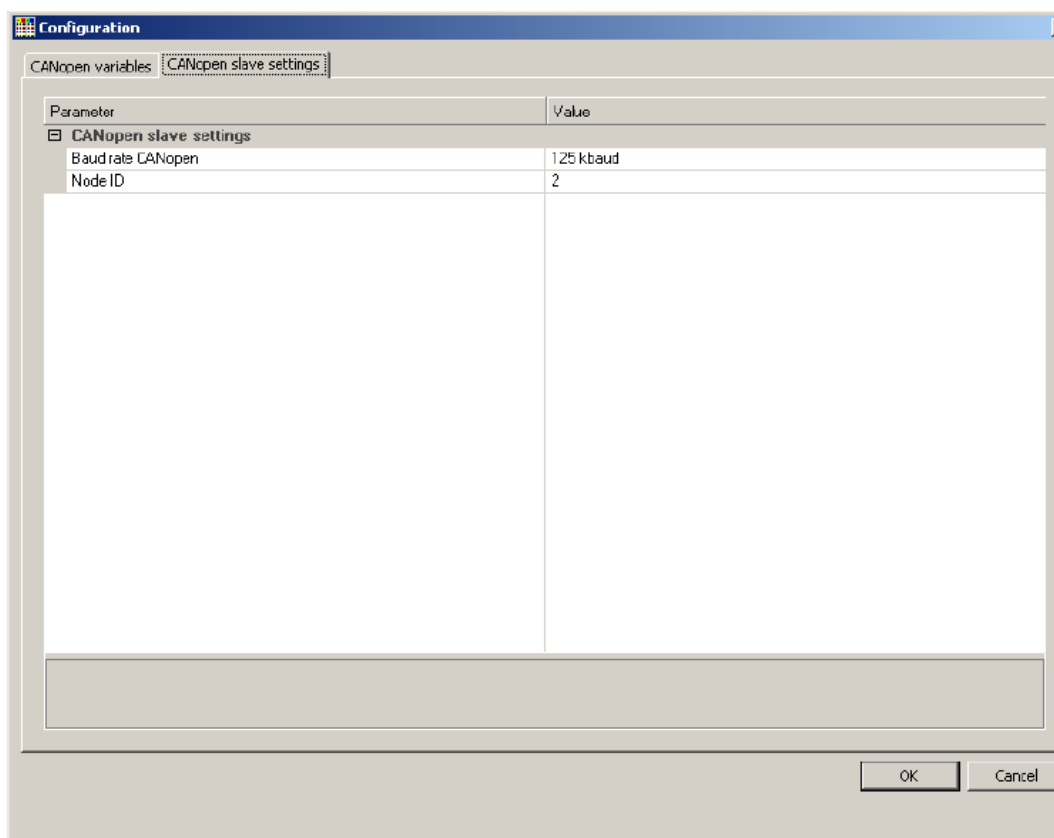
Ilustracja 138: Konfiguracja zmiennych CANopen slave

Za pomocą przycisku **[+]** (Add) można dodać zmienne CANopen. Ustawiany jest wówczas typ danych i kierunek komunikacji (typ I/O).

Tabela 96: Opis okna „CANopen Variables“ (slave)

Parametr	Znaczenie
Name	Tutaj można edytować nazwę zmiennej lub jej bity.
Address	Adres CODESYS w obszarze wejść lub wyjść w zależności od typu danych.
Data Type	Możliwe są następujące typy danych: BOOL, BYTE, WORD, DWORD, SINT, INT, DINT, USINT, UINT, UDINT, REAL, BYTE(Array) Byte-Array można rozszerzyć do żądanego rozmiaru przez dodanie bajtów. Maksymalna długość Array wynosi 8 bajtów.
Comment	Pole na komentarz
I/O type	Wejście lub wyjście (Input / Output)
Fieldbus access	Offset adresów w bajtach względem początku zakresu danych CAN

13.3.5.2 Konfiguracja parametrów CANopen



Ilustracja 139: Konfiguracja parametrów sieci CANopen slave

Tabela 97: Opis ustawień CANopen slave

Parametr	Znaczenie
Baud rate	Tu wybiera się żądaną prędkość transmisji w sieci CAN (ustawienie fabryczne: 125000 Baud).
Node ID	Identyfikator węzła PFC w sieci CAN

13.4 Diagnostyka interfejsu sieciowego

Ten rozdział wymaga dobrej znajomości środowiska programistycznego CODESYS. Opisano w nim procedurę tworzenia diagnostyki na przykładzie dla mastera sieci obiektowej

Warunkiem przeprowadzenia diagnostyki w sieciach obiektowych jest obecność konfigurowalnych urządzeń slave, jak np. interfejs lub sterownik sieciowy.

Dla celów diagnostycznych dostępne są bloki funkcyjne DiagGetBusState() i DiagGetState() z biblioteki BusDiag.lib oraz blok funkcyjny CANopenDiag() z biblioteki WagoCANopenDiag.lib.

13.4.1 BusDiag.lib

Do analizy diagnostyki wymagane są następujące bloki funkcyjne z bibliotek BusDiag.lib:

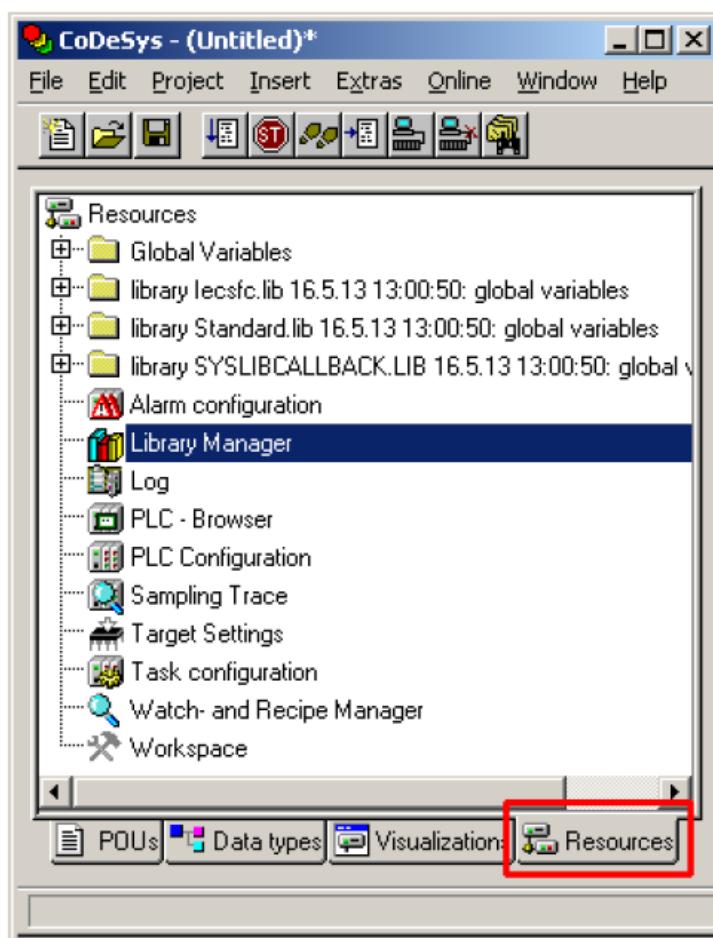
- DiagGetBusState() do diagnostyki sieci
Ten moduł funkcyjny dostarcza ogólnych informacji o podłączonych urządzeniach slave (np. ich liczba).
- DiagGetState() do diagnostyki urządzeń
Ten blok funkcyjny dostarcza szczegółowych informacji na temat każdego urządzenia slave (np. informacje o diagnostyce).

13.4.1.1 Tworzenie funkcji diagnostycznych w CODESYS 2.3

Aby przeprowadzić diagnostykę sieci i urządzeń slave, konieczne jest zaimplementowanie biblioteki BusDiag.lib w CODESYS. Znajdują się w niej bloki funkcyjne DiagGetBusState() do diagnostyki sieci i DiagGetState() do diagnostyki urządzeń.

Implementacja BusDiag.lib w CODESYS:

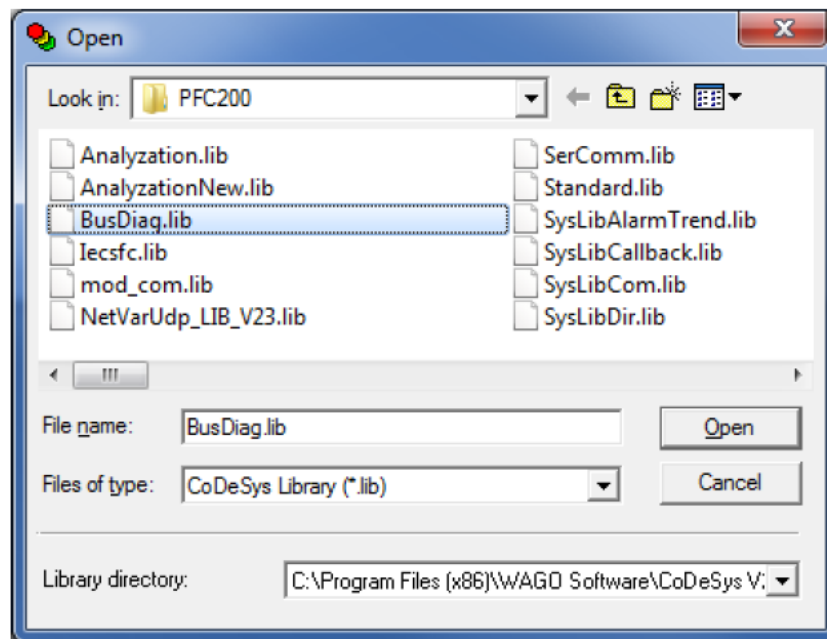
1. Kliknąć zakładkę „Resources“.



Ilustracja 140: Zakładka „Resources“

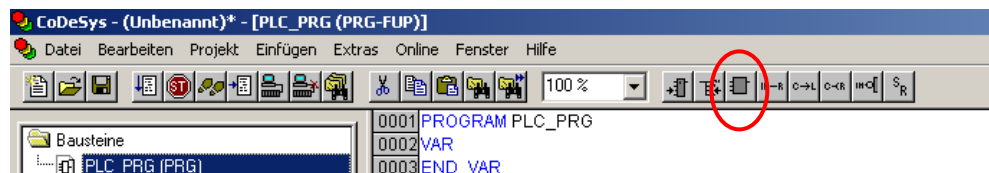
2. Kliknąć dwukrotnie w lewej kolumnie „Library Manager“

3. Na pasku menu kliknąć **Insert > Additional library**. Otworzy się okno dialogowe „Open”. Wybrać „BusDiag.lib” i kliknąć **[Open]**, aby dodać tę bibliotekę do projektu.



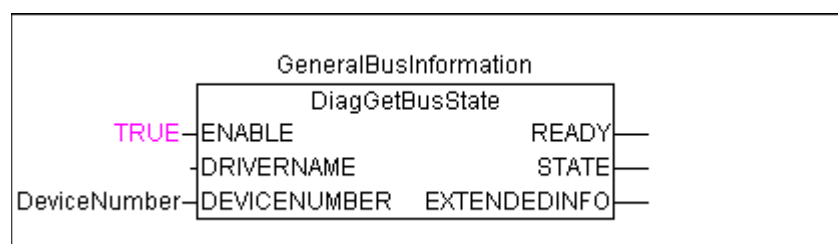
Ilustracja 141: Okno dialogowe „Open”

4. Na pasku menu kliknąć symbol „Module”.



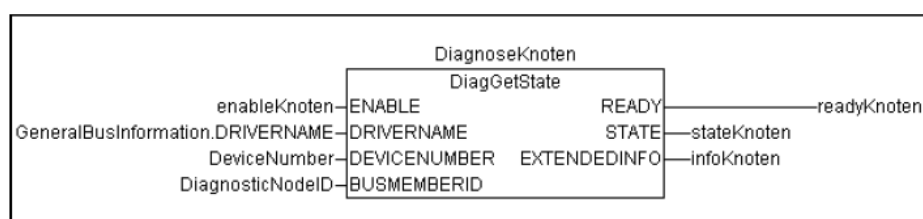
Ilustracja 142: Symbol modułu na pasku menu; język programowania FDB

5. Na klawiaturze nacisnąć klawisz **[F2]**. Otworzy się okno dialogowe „Input Assistant”. Kliknąć opcję „Standard function blocks” i wybrać blok DiagGetBusState().
6. Utworzyć instancję bloku funkcyjnego DiagGetBusState(). W tym celu wpisać nazwę nad blokiem funkcyjnym. W podanym przykładzie jest nią „GeneralBusInformation”.



Ilustracja 143: Instancja bloku funkcyjnego DiagGetBusState() w FBD

- **DRIVERNAME:**
Parametr wejściowy DRIVERNAME nie musi być podawany.
 - **DEVICENUMBER:**
DEVICENUMBER zależy od urządzenia, a zmienna „DeviceNumber” musi być dopasowana zgodnie z instrukcją zawartą w rozdziale „Załącznik” > ... > „BusDiag.lib”.
7. Z biblioteki BusDiag.lib wywołać blok funkcyjny DiagGetBusState(), służący do diagnostyki urządzeń slave.
 8. Utworzyć instancję bloku funkcyjnego DiagGetState().
W podanym przykładzie jest nią „DiagnoseKnoten”.



Ilustracja 144: Blok funkcyjny DiagGetState() w FBD

W tym przykładzie oba bloki funkcyjne są wywoływane podczas sekwencji programu. Aby uniknąć wydłużenia czasu cyklu podczas sekwencji programu, ustawić wejście „ENABLE” dla DiagGetState() na „TRUE” tylko podczas wykonywania operacji diagnostycznych.

13.4.1.2 Wywołanie bloku diagnostycznego

Blok funkcyjny należy wywołać zgodnie z poniższymi ilustracjami.

```

PLC_PRG (PRG-FUP)
0001 PROGRAM PLC_PRG
0002 VAR
0003   GeneralBusInformation AT%MB0: DiagGetBusState;
0004   DeviceNumber: INT;
0005   enableKnoten: BOOL;
0006
0007 (*===== DiagGetState =====*)
0008   DiagnoseKnoten: DiagGetState;
0009   DiagnosticNodeID: DWORD;
0010
0011   readyKnoten: BOOL;
0012   stateKnoten: NDSTATE;
0013   infoKnoten: ARRAY[0..99] OF BYTE;
0014 END_VAR

```

Ilustracja 145: Widok offline okna zmiennych w CODESYS

13.4.1.3 Przeprowadzanie diagnostyki sieci za pomocą DiagGetBusState()

W celu przeprowadzenia diagnostyki sieci należy postępować w sposób następujący:

1. Zalogować się do CODESYS. W tym celu na pasku menu kliknąć **Online > Login**. W oknie zmiennych wyświetlą się informacje o zmiennych (widok online).
2. Aby uruchomić program PLC, na pasku menu kliknąć **Online > Start**. Uruchomienie powoduje wywołanie bloku funkcyjnego DiagGetBusState() i wyświetlenie informacji diagnostycznych w Array EXTENDEDINFO.

W widoku online okna zmiennych Array EXTENDEDINFO dostarcza informacje o stanie urządzeń slave. Dla każdego urządzenia slave w Array zarezerwowany jest jeden wpis. Adres slave jest przypisany do Array index. W tym przykładzie są to urządzenia slave z adresami stacji 2 i 5, które zawierają informacje diagnostyczne. Jeśli urządzenie jest skonfigurowane jako slave, dostępne są tylko informacje o jego własnym adresie.

Wskazówka



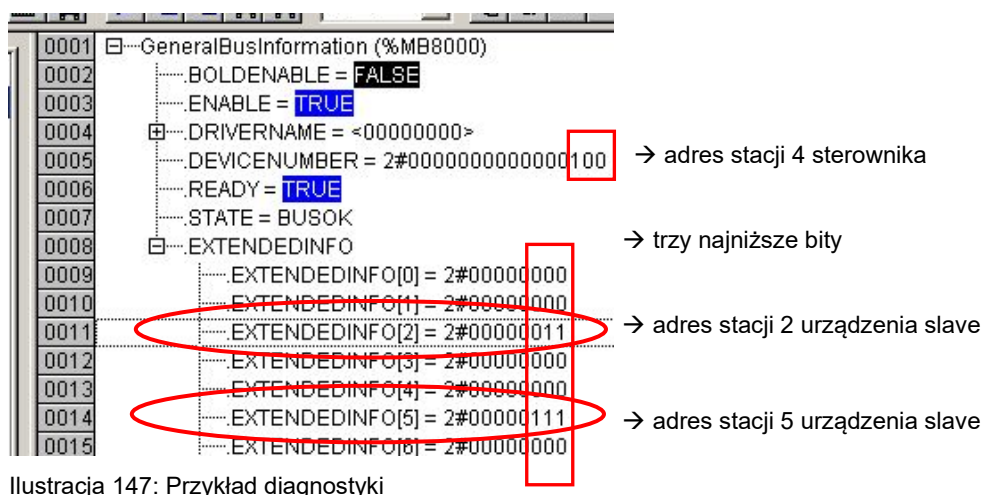
Wyświetlanie informacji diagnostycznych

Informacje diagnostyczne wyświetlane są tylko przez czas trwania cyklu. Jeśli mają być dostępne dłużej, należy napisać odpowiedni program.

0: nieskonfigurowany slave lub jego brak
≠ 0: skonfigurowane urządzenia slave

Ilustracja 146: Widok offline okna zmiennych w CODESYS (górne okno) w FBD

3. Forma binarna ułatwia weryfikację bitu diagnostycznego. Informacje diagnostyczne z Array EXTENDEDINFO można wyświetlić w formie binarnej. Aby to zrobić, kliknąć prawym przyciskiem myszy w oknie zmiennych i wybrać opcję „binary”.



4. Porównać trzy najniższe bity informacji diagnostycznej urządzeń slave o adresach stacji 2 i 5 z bitami z poniższej tabeli:

Tabela 98: Bity informacji diagnostycznej

2. bit		1. bit		0. bit	
1	0	1	0	1	0
Informacje diagnostyczne dostępne w slave.	Brak dostępnych informacji diagnostycznych w slave.	Slave jest aktywny.	Slave nie jest aktywny.	Slave jest zainstalowany.	Slave nie jest zainstalowany.

- Slave z adresem stacji 2 dostarcza wartość 011. Oznacza ona, że slave jest zainstalowany i aktywny.
- Slave z adresem stacji 5 dostarcza wartość 111. Oznacza ona, że slave jest zainstalowany i aktywny i występuje dla niego informacja o błędzie. W celu weryfikacji informacji o błędzie należy przeprowadzić diagnostykę urządzenia. Więcej informacji na ten temat zawarto w rozdziale „Przeprowadzanie diagnostyki urządzenia za pomocą DiagGetState()”.

Wskazówka



Informacje diagnostyczne

Gdy READY = TRUE, STATE informuje o aktualnym statusie sieci z jedną z poniższych wartości:

BUSOK: wszystkie skonfigurowane urządzenia slave uczestniczą w wymianie danych z DP master.

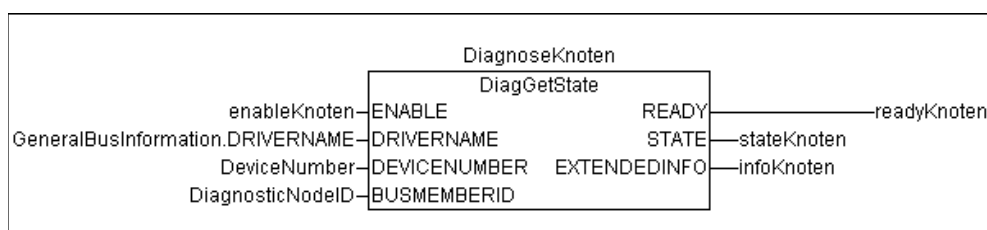
BUSFAULT: jeden lub kilka skonfigurowanych urządzeń slave nie uczestniczy w wymianie danych z DP master

BUSNOTCOMMUNICATION: żadne ze skonfigurowanych urządzeń slave nie uczestniczy w wymianie danych z DP master.

13.4.1.4 Przeprowadzanie diagnostyki urządzenia za pomocą DiagGetState()

Jeśli diagnostyka sieci wykazała, że występuje informacja diagnostyczna, należy na danym urządzeniu slave przeprowadzić diagnostykę. W tym celu postępować w następujący sposób:

1. Wywołać blok funkcyjny DiagGetState() i ustawić w nim wejście ENABLE na „True“.
2. W zmiennych wejściowych BUSMEMBERID wprowadzić urządzenie slave, dla którego występuje informacja diagnostyczna. W naszym przykładzie jest to slave z adresem sieci 5.



Ilustracja 148: Wywołanie diagnostyki DiagGetState()

- **DRIVERNAME:**
Parametr wejściowy DRIVERNAME nie musi być podawany.
- **DEVICENUMBER:**
DEVICENUMBER zależy od urządzenia, a zmienna „DeviceNumber” musi być dopasowana zgodnie z instrukcją zawartą w rozdziale „Załącznik” > ... > „BusDiag.lib”.

13.4.1.5 Weryfikacja diagnostyki CANopen (komunikaty Emergency)

Elementy Array [0] do [3] na ilustracji poniżej zawierają informacje o statusie CANopen w bajtach. Od elementu Array [4] zaczynają się komunikaty Emergency urządzeń slave.

16	EXTENDEDINFO		
17	EXTENDEDINFO[0] = 2#00000010	→ Bajt 1	Zakres informacji o statusie CANopen
18	EXTENDEDINFO[1] = 2#00000000	→ Bajt 2	
19	EXTENDEDINFO[2] = 2#00000000		
20	EXTENDEDINFO[3] = 2#00000000	→ ...	
21	EXTENDEDINFO[4] = 2#00000000		
22	EXTENDEDINFO[5] = 2#00011100		Zakres dla komunikatów Emergency urządzeń slave
23	EXTENDEDINFO[6] = 2#00000101		
24	EXTENDEDINFO[7] = 2#00000001		
25	EXTENDEDINFO[8] = 2#00001000		
26	EXTENDEDINFO[9] = 2#00001100		
27	EXTENDEDINFO[10] = 2#00000000		
28	EXTENDEDINFO[11] = 2#00000001		
29	EXTENDEDINFO[12] = 2#10110111		
30	EXTENDEDINFO[13] = 2#01010100		
31	EXTENDEDINFO[14] = 2#01001001		
32	EXTENDEDINFO[15] = 2#00001000		
33	EXTENDEDINFO[16] = 2#00000000		
34	EXTENDEDINFO[17] = 2#00000000		
35	EXTENDEDINFO[18] = 2#00000000		
36	EXTENDEDINFO[19] = 2#00000000		
37	EXTENDEDINFO[20] = 2#00000000		
38	EXTENDEDINFO[21] = 2#00000000		
39	EXTENDEDINFO[22] = 2#00000000		
40	EXTENDEDINFO[23] = 2#00000111		
41	EXTENDEDINFO[24] = 2#10100000		
42	EXTENDEDINFO[25] = 2#00000000		
43	EXTENDEDINFO[26] = 2#00000000		
44	EXTENDEDINFO[27] = 2#00000000		
45	EXTENDEDINFO[28] = 2#00000000		
46	EXTENDEDINFO[29] = 2#00000000		
47	EXTENDEDINFO[30] = 2#10000100		
48	EXTENDEDINFO[31] = 2#01000000		
49	EXTENDEDINFO[32] = 2#10101000		
50	EXTENDEDINFO[33] = 2#10000100		
51	EXTENDEDINFO[34] = 2#01000001		
52	EXTENDEDINFO[35] = 2#10101000		
53	EXTENDEDINFO[36] = 2#00000000		

Ilustracja 149: Widok Online dla Array EXTENDEDINFO w formie binarnej

Informacje o statusie CANopen i komunikaty Emergency urządzeń slave zostały opisane na kolejnych stronach.

**Opis informacji diagnostycznej bloku funkcyjnego
DiagGetState.EXTENDEDINFO dla CANopen**

Array EXTENDEDINFO zawiera następujące informacje o statusie:

Bajt 0

- Bit 0: Slave wprowadzony
- Bit 1: Slave wprowadzony i skonfigurowany
- Bit 2: Niewłaściwa konfiguracja slave
- Bit 3: Diagnostyka: zdarzenie Emergency aktywne
- Bit 4: Status slave „Operational“
- Bit 5: Status slave „Stop“
- Bit 6: Status slave „Preoperational“
- Bit 7: Błędna struktura konfiguracji (z mastera)

Bajt 1

- Bit 0: Struktura konfiguracji nie pasuje do slave
- Bit 1: Błędny kod slave

Bajt 2

- Bit 0: Komunikat Emergency jest już obecny na liście

Bajt 3

niewykorzystany

Bajt 4 ... 11

Ostatni komunikat Emergency na liście

13.4.2 WagoCANopenDiag.lib

Ta biblioteka udostępnia blok funkcyjny, umożliwiający łatwiejsze monitorowanie węzłów CANopen. Diagnostyki i EMCY-Messages generowane są w formie tekstu. Więcej informacji można znaleźć w opisie WagoCANopenDiag.lib.

13.5 Wymiana danych pomiędzy Simple CAN Subscribers i sterownikiem w sieci CANopen

W celu uproszczenia konfiguracji sterownika, przy podłączaniu urządzeń CAN Layer2 został utworzony zredukowany plik EDS „Generic CAN-Device”. Ten plik EDS zawiera 16 PDO nadawczych i odbiorczych, z których każdy ma przypisanych 8 wpisów 1-bajtowych. Dla tych urządzeń należy jedynie dezaktywować telegramy konfiguracyjne i monitorujące typowe dla CANopen.

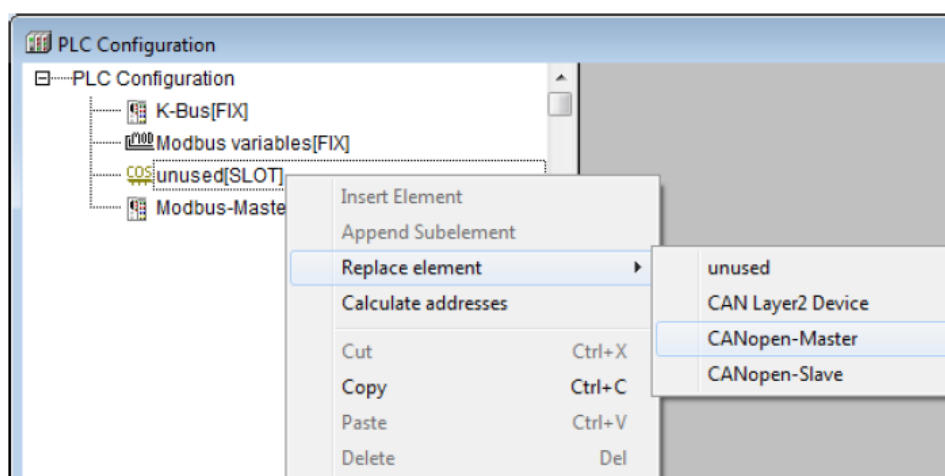
Wskazówka **Dołączone pliki EDS stosować tylko w CODESYS 2.3!**



Pliki EDS dla generycznych urządzeń CAN Layer2, znajdujące się w plikach docelowych sterownika, mogą być zastosowane tylko wtedy, gdy w sterowniku wykorzystany jest system runtime CODESYS 2.3!

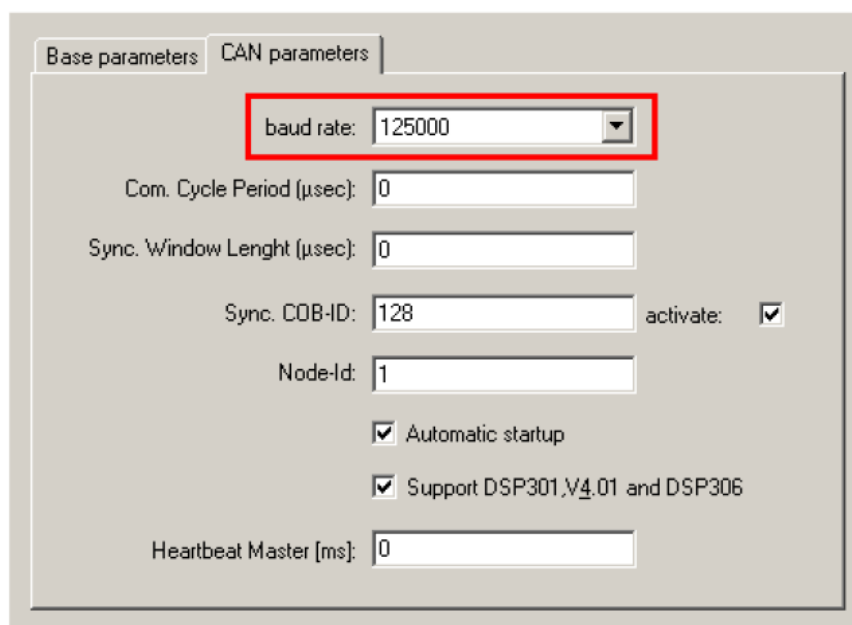
Konfigurację sterownika można przeprowadzić także za pomocą dowolnego pliku EDS dla CANopen.

1. W celu dodania CANopen master do konfiguracji sterownika kliknąć prawym przyciskiem myszy „COS unused[Slot]” i wybrać „Replace element -> CANopen Master”.



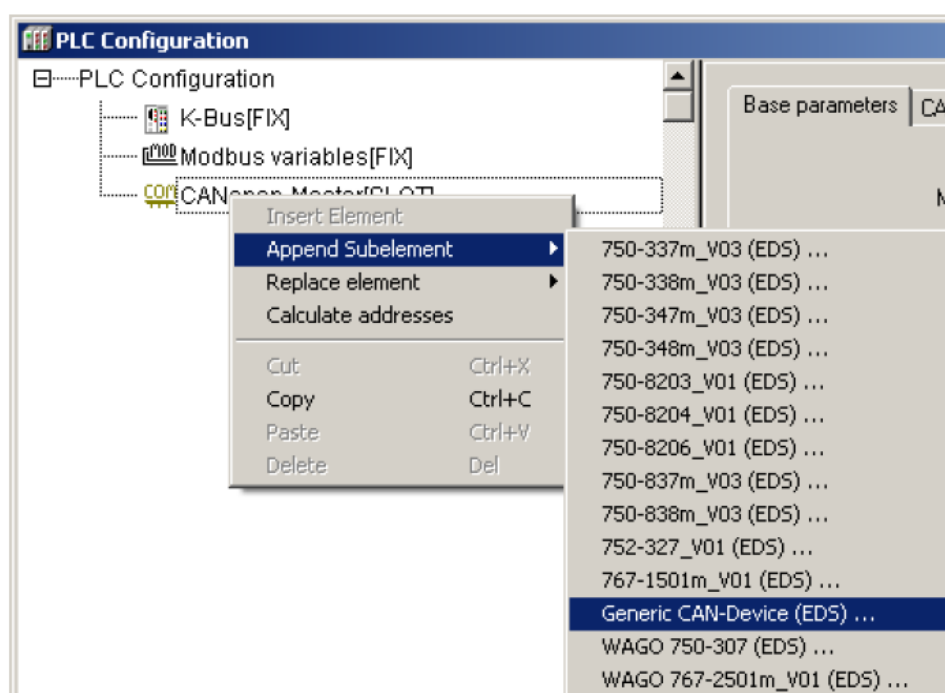
Ilustracja 150: Dodawanie CANopen master

2. W zakładce „CAN Parameters” wybrać żądaną prędkość transmisji.



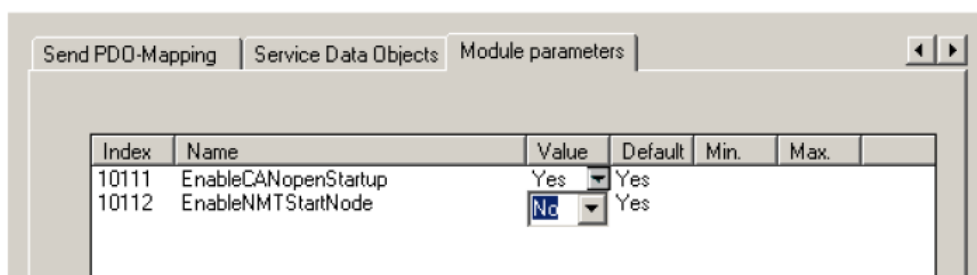
Ilustracja 151: Dodawanie prędkości transmisji

3. W celu dodania urządzenia slave kliknąć prawym przyciskiem myszy **CANopen-Master[SLOT]** i wybrać w menu kontekstowym **Attach sub-element > Generic CAN Device (EDS)**



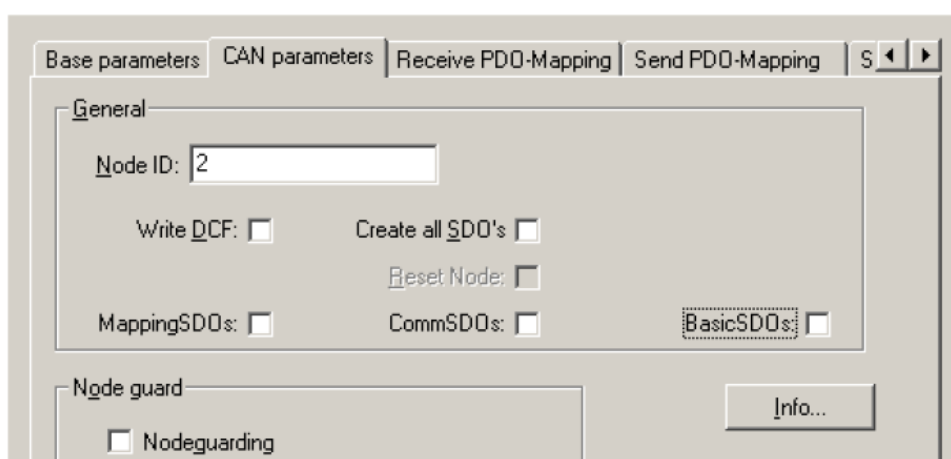
Ilustracja 152: Plik EDS „Generic CAN-Device”

4. Otworzyć zakładkę „**Module parameters**” urządzenia slave W przypadku komunikacji z prostymi urządzeniami CAN Layer2 należy wyłączyć transmisję konfiguracji do urządzenia slave za pomocą **EnableCANopenStartup** (= „No”).



Ilustracja 153: Zakładka „Module parameters”

5. Otworzyć zakładkę „**CAN parameters**” urządzenia slave. Dezaktywować parametry **CommSDO**, **MappingSDO**, **Basic SDO** i **Nodeguarding**.



Ilustracja 154: Zakładka „CAN parameters”

6. Za pomocą poleceń biblioteki CANLayer2 (patrz rozdział „Biblioteki CODESYS” > ... > „WagoCANLayer2_01.lib”) można uzyskać dostęp do urządzeń.
Informacje na temat konfiguracji ramek CAN dla urządzeń CAN Layer2 zawarto w rozdziale „CANopen master i slave” > ... > „Konfiguracja PDO dla urządzeń slave”.

13.6 Wymiana danych między prostymi urządzeniami sieci CAN i PFC200 w sieci CAN Layer2

Gdy w sieci znajdują się tylko urządzenia CAN Layer2, funkcje CANopen nie są potrzebne. W tym celu zdefiniowano własne urządzenie, które udostępnia tylko podstawowe funkcje CAN Layer2.

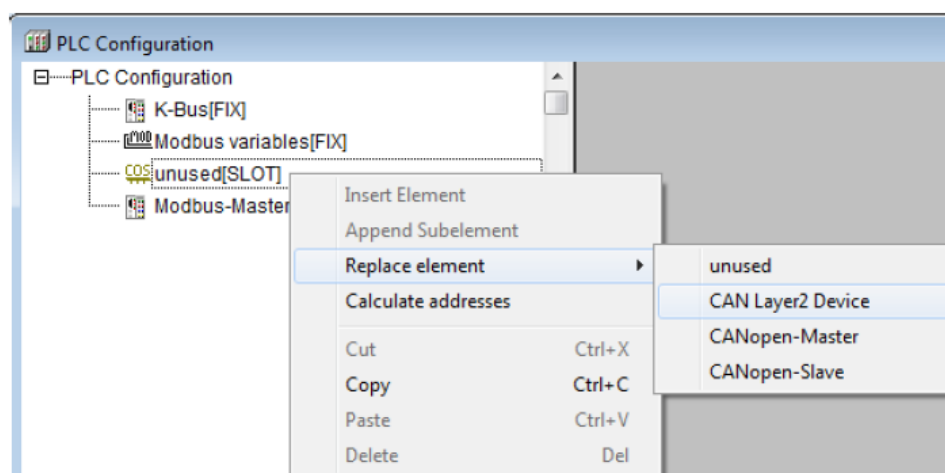
Wskazówka



Dołączone pliki EDS stosować tylko w CODESYS 2.3!

Pliki EDS dla urządzeń CAN Layer2, znajdujące się w plikach docelowych sterownika, mogą być zastosowane tylko wtedy, gdy w sterowniku wykorzystany jest system runtime CODESYS 2.3!

1. W celu dodania urządzenia CAN Layer2 do konfiguracji sterownika kliknąć prawym przyciskiem myszy „COS unused[Slot]” i wybrać „Replace element -> CAN Layer2 Device”.



Ilustracja 155: Dołączanie urządzenia CAN Layer2

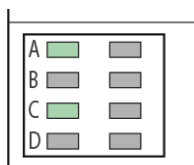
2. Teraz za pomocą bloku funkcyjnego WagoCANLayer2_02.lib można otworzyć interfejs CAN, zdefiniować CAN LED i przeprowadzić wymianę danych.

14 Diagnostyka

14.1 Komunikaty o pracy i statusie

W poniższych tabelach opisane są komunikaty o pracy i statusie sterownika, sygnalizowane przez LED.

14.1.1 LED dla zasilania



Ilustracja 156: LED dla zasilania

14.1.1.1 LED „A“

LED „A“ (zasilanie systemu) wskazuje następujące stany diagnostyczne:

Tabela 99: Diagnostyka zasilania systemowego

Status	Znaczenie	Środek zaradczy
zielony	Zasilanie napięciem magistrali systemowej 24 V	---
wyłączony	Brak zasilania napięciem magistrali systemowej 24 V	Włączyć napięcie zasilania. Sprawdzić napięcie zasilania.

14.1.1.2 LED „C“

LED „C“ (zasilanie obiektowe) wskazuje następujące stany diagnostyczne:

Tabela 100: Diagnostyka zasilania sieciowego

Status	Znaczenie	Środek zaradczy
zielony	Zasilanie napięciem zasilania obiektowego 24 V	---
wyłączony	Brak napięcia zasilania obiektowego 24 V	Włączyć napięcie zasilania. Sprawdzić napięcie zasilania.

14.1.2 LED dla systemu / sieci obiektowej

U6   SYS
U5   RUN
U4   I/O
U3   MS
U2   NS
U1   CAN

Ilustracja 157: LED dla systemu / sieci obiektowej

14.1.2.1 LED „SYS“

Wskazanie LED „SYS“ jest zależne od aktywowanego systemu runtime (CODESYS V2 lub **e!RUNTIME**).

Dla systemu runtime CODESYS V2 wyświetlane są następujące komunikaty diagnostyczne:

Tabela 101: Diagnostyka LED „SYS“

Status	Znaczenie	Środek zaradczy
zielony	Gotowość do pracy – start systemu zakończony bez błędu.	---
pomarańczowy	Urządzenie znajduje się w trakcie procesu rozruchu/bootowania i przycisk RST nie jest wciśnięty.	---
	Obciążenie powyżej wartości granicznej 1 – system jest obciążony, nie można zagwarantować reakcji w czasie rzeczywistym.	Spróbować odciążyć system: - Zmienić program CODESYS. - Zakończyć niepotrzebne komunikacje sieci obiektowej lub zmienić konfigurację sieci. - Usunąć ewentualnie niekrytyczne zadania z obszaru RT. - Wybrać dłuższy czas trwania cyklu dla zadań IEC.
pomarańczowy migający	Tryb „Fix IP Address” – tymczasowe ustawienie do następnego restartu	Należy połączyć się przez standardowy adres (192.168.1.17) z urządzeniem lub zrestartować urządzenie, aby odtworzyć pierwotnie ustawione wartości.
czerwony	Obciążenie powyżej wartości granicznej 2 – system jest przeciążony, nie można zagwarantować reakcji w czasie rzeczywistym.	Spróbować odciążyć system: - Zmienić program CODESYS. - Zakończyć niepotrzebne komunikacje sieci obiektowej lub zmienić konfigurację sieci. - Usunąć ewentualnie niekrytyczne zadania z obszaru RT. - Wybrać dłuższy czas trwania cyklu dla zadań IEC.
zielony/czerwony migający	Tryb aktualizacji firmware	---

Dla systemu **e!RUNTIME** wyświetlane są następujące komunikaty diagnostyczne:

Tabela 102: Diagnostyka LED „SYS“

Status	Znaczenie	Środek zaradczy
zielony	Gotowość do pracy – start systemu zakończony bez błędu.	---
pomarańczowy	Urządzenie znajduje się w trakcie procesu rozruchu/bootowania i przycisk RST nie jest wciśnięty.	---
pomarańczowy migający	Tryb „Fix IP Address“, – tymczasowe ustawienie do następnego restartu	Należy połączyć się przez standardowy adres (192.168.1.17) z urządzeniem lub zrestartować urządzenie, aby odtworzyć pierwotnie ustawione wartości.
zielony/czerwony migający	Tryb aktualizacji firmware	---
pomarańczowy/czerwony migający	Brak licencji, test trwa.	Dane biblioteki lub funkcje urządzeń wyświetlane są w e!COCKPIT . Przed zakończeniem testu aktywować odpowiednie licencje lub usunąć te biblioteki lub funkcje urządzeń z aplikacji. Tak długo, jak trwa test, funkcjonalność urządzenia jest nieograniczona.
czerwony migający	Brak licencji, czas testu minął.	Dane biblioteki lub funkcje urządzeń wyświetlane są w e!COCKPIT . Aktywować niezwłocznie odpowiednie licencje lub usunąć te biblioteki lub funkcje urządzeń z aplikacji. W przeciwnym razie nie będzie możliwe ponowne uruchomienie aplikacji po ponownym wgraniu lub starcie aplikacji bootowalnej po restarcie urządzenia.

14.1.2.2 LED „RUN“

Wskazanie LED „RUN“ jest zależne od aktywowanego systemu runtime (CODESYS V2 lub **e!RUNTIME**).

Dla systemu runtime CODESYS V2 wyświetlane są następujące komunikaty diagnostyczne:

Tabela 103: Diagnostyka LED „RUN“

Status	Znaczenie	Środek zaradczy
zielony	Program PLC ma status „Run“.	---
zielony migający	Program PLC znajduje się w punkcie debugowania.	Należy kontynuować program w podłączonym IDE pojedynczym krokiem i startem. Gdy połączenie zostało przerwane, należy ustawić przełącznik trybu pracy na „STOP“, a potem znów na „RUN“, aby ponownie uruchomić program.
zielony/ czerwony migający	Program PLC znajduje się w punkcie debugowania a przełącznik trybu pracy został ustawiony na „Stop“.	Aby kontynuować program, należy ustawić przełącznik trybu pracy na „RUN“.
czerwony	Program nie jest załadowany lub program PLC ma status „Stop“.	Należy załadować program PLC. Aby uruchomić aktualny program, ustawić przełącznik trybu pracy na „RUN“.

Dla systemu **e!RUNTIME** wyświetlane są następujące komunikaty diagnostyczne:

Tabela 104: Diagnostyka LED „RUN“

Status	Znaczenie	Środek zaradczy
zielony	Aplikacje załadowane i wszystkie ze statusem „RUN“	---
zielony migający	Brak aplikacji i załadowanego projektu bootowalnego	Załadować aplikację lub projekt bootowalny.
czerwony	Aplikacje załadowane i wszystkie ze statusem „STOP“.	Aby uruchomić aplikację, należy ustawić przełącznik trybu pracy na „RUN“.
zielony/czerwony migający	Co najmniej jedna aplikacja ze statusem „RUN“ i jedna ze statusem „STOP“	Uruchomić zatrzymaną aplikację.
czerwony, gasnący na krótko	Wykonano gorący reset	---
czerwony, gasnący na dłużej	Wykonano zimny reset	---
czerwony migający	Co najmniej jedna aplikacja po wyjątku (np. błędzie dostępu do zapisu) ma status „STOP“	Uruchomić ponownie aplikację, wykonując reset za pomocą przełącznika trybu pracy lub w powiązonym IDE. Jeśli aplikacja nie została uruchomiona, należy zrestartować sterownik. Jeżeli błąd nie zostanie usunięty, należy skontaktować się ze wsparciem WAGO.
pomarańczowy/zielony migający	Obciążenie przekraczające wartość progową 1	Należy spróbować odciążyć system: - Zmienić program CODESYS. - Zakończyć niepotrzebne komunikacje sieci obiektowej lub zmienić konfigurację sieci. - Usunąć ewentualnie niekrytyczne zadania z obszaru RT. - Wybrać dłuższy czas trwania cyklu dla zadań IEC.

Tabela 104: Diagnostyka LED „RUN”

Status	Znaczenie	Środek zaradczy
pomarańczowy	System runtime w stanie debugowania (breakpoint, pojedynczy krok, pojedynczy cykl)	Kontynuować program w podłączonym IDE pojedynczym krokiem i startem. Usunąć punkty zatrzymania. Jeśli połączenie zostanie przerwane, ustawić przełącznik trybu pracy w pozycji „STOP”, a następnie z powrotem w pozycji „RUN”, aby umożliwić dalsze działanie aplikacji.
wyłączony	System Runtime niezaladowany	Aktywować system runtime, np. przez WBM.

14.1.2.3 LED „I/O“

LED „I/O“ wskazuje następujące stany diagnostyczne:

Tabela 105: Diagnostyka LED „I/O“

Status	Znaczenie	Środek zaradczy
zielony	Cykl danych w magistrali systemowej, normalny stan pracy	---
pomarańczowy migający	Faza rozruchu, inicjalizacja magistrali systemowej. Rozruch jest sygnalizowany miganiem co 1 ... 2 sekundy.	Zaczekać, aż proces ten zostanie zakończony.
czerwony	Uszkodzenie sprzętu	Należy skontaktować się ze wsparciem WAGO.
czerwony migający (2 Hz)	Błąd możliwy do usunięcia	Spróbować usunąć błąd przez wyłączenie i włączenie zasilania urządzenia. Sprawdzić cały węzeł sieciowy pod kątem ewentualnych błędów. Jeżeli nie można usunąć błędu, należy skontaktować się ze wsparciem WAGO.
czerwony migający (sekwencja migania)	Błąd magistrali systemowej	Znaczenie sekwencji migania opisano w rozdziale „Komunikaty diagnostyczne przy użyciu sekwencji migania“.
wyłączony	Biblioteka nie została załadowana lub funkcja biblioteki nie została wywołana.	Uruchomić ponownie urządzenie. Jeżeli nie można usunąć błędu, należy skontaktować się ze wsparciem WAGO.

14.1.2.4 LED „MS“

LED „MS“ wskazuje następujące stany diagnostyczne:

Tabela 106: Diagnostyka LED „MS“

Status	Znaczenie	Środek zaradczy
wyłączony	Brak błędu	---
czerwony migający (sekwencja migania)	Błąd konfiguracji	Znaczenie sekwencji migania opisano w rozdziale „Komunikaty diagnostyczne przy użyciu sekwencji migania“.

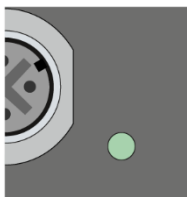
14.1.2.5 LED „CAN“

LED „CAN“ wskazuje następujące stany diagnostyczne:

Tabela 107: Diagnostyka LED „CAN“

Status	Znaczenie	Środek zaradczy
wyłączony	Interfejs CAN jest nieskonfigurowany.	---
na zmianę: czerwony 50 ms / zielony 50 ms	Trwa konfiguracja	---
na zmianę: czerwony 200 ms / zielony 200 ms	Błędna konfiguracja	Sprawdzić konfigurację w konfiguratorze CODESYS.
zielony 200 ms / wyłączony 800 ms	Interfejs CANopen ma status „Stop“.	---
zielony 200 ms / wyłączony 200 ms	Interfejs CANopen ma status „Preoperational“.	---
zielony	Interfejs CANopen ma status „Operational“.	---
czerwony	Interfejs CANopen ma status „Bus Off“ (zwarcie lub inne poważne zakłócenie).	Sprawdzić połączenia sieciowe i prędkość transmisji.
Błąd ma status „Preoperational“		
1 × czerwony migający / 2 × zielony migający	Bus Warning Level przekroczony.	Sprawdzić oprzewodowanie sieci CAN.
2 × czerwony migający / 2 × zielona migająca	Guarding Error, slave źle skonfigurowany lub nie istnieje.	Sprawdzić urządzenia slave i konfigurację.
3 × czerwony migający / 2 × zielony migający	Sync Error	Zmienić interwał czasowy dla komunikatu synchronizacyjnego.
Błąd w statusie „Operational“		
1 x czerwony migający/ zielony 800 ms włączony	Bus Warning Level przekroczony.	Sprawdzić oprzewodowanie sieci CAN.
2 x czerwony migający / zielony 800 ms włączony	Guarding Error	Sprawdzić urządzenia slave i konfigurację.
3 x czerwony migający / zielony 800 ms włączony	Sync Error	Zmienić interwał czasowy dla komunikatu synchronizacyjnego.

14.1.3 LED dla złącz sieciowych



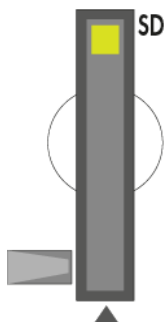
Ilustracja 158: LED "LNK"

LED "LNK" obok odpowiedniego złącza M12 wskazuje następujące stany diagnostyczne:

Tabela 108: Diagnostyka LED „LNK”

Status	Znaczenie	Środek zaradczy
wyłączony	Brak połączenia	---
zielony	Nawiązano połączenie	---

14.1.4 LED gniazda karty pamięci



Ilustracja 159: LED gniazda karty pamięci

LED gniazda karty pamięci wskazuje następujące stany diagnostyczne:

Tabela 109: Diagnostyka LED gniazda karty pamięci

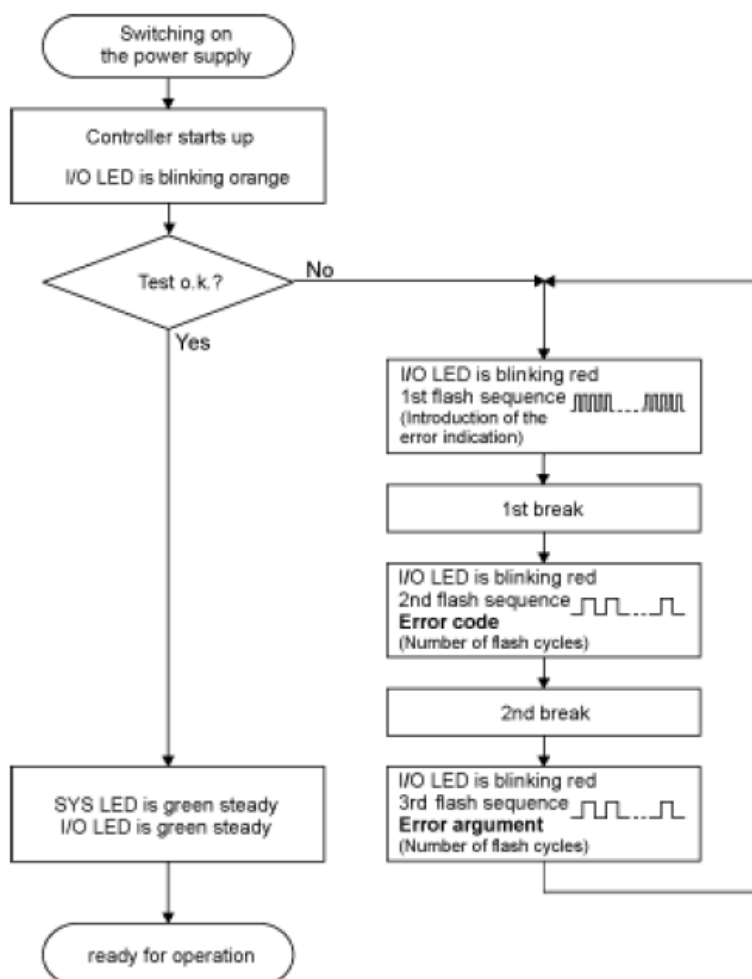
Status	Znaczenie	Środek zaradczy
wyłączony	Brak możliwości zapisu i odczytu danych na karcie pamięci	---
pomarańczowy świecący	Możliwość zapisu i odczytu danych na karcie pamięci	---
pomarańczowy migający		

14.2 Komunikaty diagnostyczne przy użyciu sekwencji migania

14.2.1 Przebieg sekwencji migania

Diagnostyka zakłócenia jest zawsze sygnalizowana cyklicznie trzema sekwencjami migania:

1. Pierwsza sekwencja (migotanie) rozpoczyna sygnalizację zakłócenia.
2. Po 1-sekundowej przerwie pojawia się druga sekwencja. Liczba impulsów migania podaje **kod błędu**, który opisuje rodzaj błędu.
3. Po kolejnej przerwie pojawia się trzecia sekwencja. Liczba impulsów migania podaje **argument błędu**, dostarczający bardziej szczegółowy opis, np. w których modułach I/O podłączonych do sterownika występuje błąd.



Ilustracja 160: Diagram przebiegu sekwencji migania

14.2.2 Przykład komunikatu diagnostycznego przy użyciu sekwencji migania

Przykład objaśnia budowę komunikatu diagnostycznego przy użyciu sekwencji migania. LED „I/O” sygnalizuje błąd danych magistrali systemowej. Wyświetlany jest błąd danych, spowodowany usunięciem jednego z modułów I/O, znajdującego się w węźle sieciowym na pozycji 6.

Faza początkowa

1. LED „I/O” miga przez 1 cykl ok. 10 Hz (10 mignięć na sekundę).
2. Potem następuje ok. 1-sekundowa przerwa.

Kod błędu 4: błąd danych magistrali systemowej

3. LED „I/O” miga przez 4 cykle ok. 1 Hz.
4. Potem następuje ok. 1-sekundowa przerwa.

Argument błędu 5: moduł I/O na pozycji 6.

5. LED „I/O” miga przez 5 cykli 1 Hz.
Oznacza to, że w magistrali systemowej wystąpił błąd po 5. module I/O.
6. Sekwencja migania rozpoczyna migotaniem pierwszą fazę sygnalizacji.
Gdy występuje tylko jedno zakłócenie, cały proces sygnalizacji zostaje powtórzony.

14.2.3 Kody migania LED „I/O” i sposoby usuwania błędu

W tym rozdziale opisano diagnostykę wyświetlaną przez LED „I/O” w postaci kodu migania.

Jeśli przedstawionych poniżej błędów nie da się usunąć opisanymi sposobami, należy skontaktować się ze wsparciem WAGO. Prosimy podać kod migania.

tel.: +48 71 360 29 33

e-mail: wsparcie.techniczne@wago.com

Tabela 110: Przegląd kodów błędu LED „I/O”

Kod błędu	Znaczenie
1	Błąd sprzętu i konfiguracji
2	Błąd konfiguracji
3	Błąd protokołu magistrali systemowej
4	Fizyczny błąd magistrali systemowej
5	Błąd inicjalizacji magistrali systemowej
6	Brak zastosowania
7	Nieobsługiwany moduł I/O
8	Brak zastosowania
9	Błąd wyjątku CPU

Tabela 111: Kod błędu 1, znaczenie kodu migania i sposoby usuwania błędu

Argument błędu	Przyczyna	Środek zaradczy
-	Niewłaściwa suma kontrolna parametrów interfejsu magistrali systemowej	- Wyłączyć zasilanie sterownika i go wymienić. - Włączyć ponownie zasilanie.
1	Podczas generowania kodu Inline wewnętrzny bufor pamięci przekroczył maksymalną liczbę danych.	- Wyłączyć zasilanie sterownika. - Zredukować liczbę modułów I/O. - Włączyć z powrotem zasilanie.
2	Moduł(y) I/O z nieobsługiwanym typem danych	- Zaktualizować firmware sterownika. Jeśli błąd nadal występuje, przyczyna leży w module I/O. Można go wykryć w następujący sposób: - Wyłączyć zasilanie. - Umieścić moduł końcowy w środku, między podłączonymi modułami I/O. - Włączyć z powrotem zasilanie. - Jeśli LED nadal miga na czerwono, wyłączyć ponownie zasilanie, włożyć moduł końcowy w środek pierwszej połowy węzła (patrząc od strony sterownika sieciowego). - Jeśli LED przestała migać, wyłączyć zasilanie i włożyć moduł końcowy w środek drugiej połowy węzła (patrząc od strony sterownika sieciowego). - Włączyć z powrotem zasilanie. - Powtarzać procedurę do momentu, aż uszkodzony moduł I/O zostanie zlokalizowany. Wymienić uszkodzony moduł.
3	Nieznany typ modułu pamięci programowej flash	- Wyłączyć zasilanie sterownika i go wymienić. - Włączyć ponownie zasilanie.
4	Błąd przy zapisie w pamięci flash	- Wyłączyć zasilanie sterownika i go wymienić. - Włączyć ponownie zasilanie.
5	Błąd przy usuwaniu sektora pamięci flash	

Tabela 111: Kod błędu 1, znaczenie kodu migania i sposoby usuwania błędu

Argument błędu	Przyczyna	Środek zaradczy
6	Konfiguracja modułów I/O po resecie magistrali systemowej nie zgadza się z konfiguracją po ostatnim uruchomieniu sterownika.	- Zrestartować sterownik przez odłączenie i włączenie zasilania lub za pomocą przycisku Reset na sterowniku.
7	Błąd przy opisie szeregowego EEPROM	- Wyłączyć zasilanie sterownika i go wymienić. - Włączyć ponownie zasilanie.
8	Nieprawidłowa kombinacja sprzętu i firmware	
9	Nieprawidłowa suma testowa w szeregowym EEPROM	
10	Inicjalizacja szeregowego EEPROM zakończona niepowodzeniem	
11	Błąd przy odczycie z szeregowego EEPROM	- Wyłączyć zasilanie sterownika i zredukować liczbę modułów I/O. - Włączyć ponownie zasilanie.
12	Przekroczony czas dostępu do szeregowego EEPROM	- Wyłączyć zasilanie sterownika i go wymienić. - Włączyć ponownie zasilanie.
14	Przekroczona maksymalna liczba bram lub modułów mailbox	- Wyłączyć zasilanie sterownika. - Zredukować liczbę bram lub modułów mailbox. - Włączyć ponownie zasilanie.
16	Przekroczona maksymalna liczba modułów I/O	- Wyłączyć zasilanie sterownika. - Zredukować liczbę modułów I/O. - Włączyć ponownie zasilanie.

Tabela 112: Kod błędu 2, znaczenie kodu migania i sposoby usuwania błędu

Argument błędu	Przyczyna	Środek zaradczy
2	Przekroczona maksymalna wielkość obrazu procesu	- Wyłączyć zasilanie sterownika. - Zredukować liczbę modułów I/O. - Włączyć z powrotem zasilanie.

Tabela 113: Kod błędu 3, znaczenie kodu migania i sposoby usuwania błędu

Argument błędu	Przyczyna	Środek zaradczy
-	Zakłócenie komunikacji w magistrali systemowej; nie można wykryć uszkodzonego modułu I/O	Jeśli do sterownika podłączony jest moduł zasilający (np. 750-602), należy sprawdzić jego prawidłowe działanie (patrz rozdział „Sygnalizacja LED“). Jeśli moduł zasilający nie jest wadliwy, przyczyna zakłócenia może leżeć w module I/O. Moduł I/O można wykryć w następujący sposób: - Wyłączyć zasilanie. - Umieścić moduł końcowy w środku, między podłączonymi modułami I/O. - Włączyć z powrotem zasilanie. - Jeśli LED I/O miga nadal na czerwono, wyłączyć ponownie zasilanie, włożyć moduł końcowy w środek pierwszej połowy wężła (patrząc od strony sterownika sieciowego). Gdy pozostał tylko jeden moduł I/O, a LED nadal miga, oznacza to, że uszkodzony jest ten moduł lub złącze magistrali systemowej sterownika. Wymienić uszkodzony moduł I/O lub sterownik. - Jeśli LED przestała migać, wyłączyć zasilanie i włożyć moduł końcowy w środek drugiej połowy wężła (patrząc od strony sterownika sieciowego). - Włączyć z powrotem zasilanie. - Powtarzać procedurę do momentu, aż uszkodzony moduł I/O zostanie zlokalizowany. Wymienić uszkodzony moduł.

Tabela 114: Kod błędu 4, znaczenie kodu migania i sposoby usuwania błędu

Argument błędu	Przyczyna	Środek zaradczy
-	Przekroczona dopuszczalna liczba modułów I/O	- Wyłączyć zasilanie sterownika. - Zredukować liczbę modułów I/O do dopuszczalnej wartości. - Włączyć z powrotem zasilanie.
n*	Przerwanie magistrali systemowej po n-tym module udostępniającym dane procesowe	- Wyłączyć zasilanie sterownika. - Wymienić moduł I/O (n+1) udostępniający dane procesowe. - Włączyć z powrotem zasilanie. Moduły I/O, które nie dostarczają danych, nie są liczone (np. moduł zasilający bez diagnostyki)

Tabela 115: Kod błędu 5, znaczenie kodu migania i sposoby usuwania błędu

Argument błędu	Przyczyna	Środek zaradczy
n*	Błąd przy komunikacji rejestrowej w czasie inicjalizacji magistrali systemowej	- Wyłączyć zasilanie sterownika. - Wymienić moduł I/O (n+1) udostępniający dane procesowe. - Włączyć z powrotem zasilanie. Moduły I/O, które nie dostarczają danych, nie są liczone (np. moduł zasilający bez diagnostyki)

Tabela 116: Kod błędu 7, znaczenie kodu migania i sposoby usuwania błędu

Argument błędu	Przyczyna	Środek zaradczy
n	Pierwszy nieobsługiwany moduł I/O na pozycji n	- Wyłączyć zasilanie sterownika. - Wymienić n-ty moduł I/O udostępniający dane procesowe lub zredukuj liczbę modułów I/O na n-1. - Włączyć z powrotem zasilanie.

Tabela 117: Kod błędu 9, znaczenie kodu migania i sposoby usuwania błędu

Argument błędu	Przyczyna	Środek zaradczy
1	Niewłaściwe przydzielenie programu	Zakłócenie przebiegu programu. - Skontaktować się ze wsparciem WAGO.
2	Nadmiar stosu	Zakłócenie przebiegu programu. - Skontaktować się ze wsparciem WAGO.
3	Niedomiar stosu	Zakłócenie przebiegu programu. - Skontaktować się ze wsparciem WAGO.
4	Nieważne zdarzenie (NMI)	Zakłócenie przebiegu programu. - Skontaktować się ze wsparciem WAGO.
5	Zadziałał watchdog magistrali systemowej.	W przypadku aplikacji bazujących na CODESYS V2: - Skontaktować się ze wsparciem WAGO. W przypadku aplikacji bazujących na e!RUNTIME : - Sprawdzić obciążenie systemu przez zadania IEC o priorytetach 1 ... 14 w systemie runtime (patrz rozdział „Środowisko systemowe e!RUNTIME ” > „Priorytety CODESYS V3”). W przypadku aplikacji bazujących na C: - Sprawdzić ustawienia dla czasu monitorowania.

14.2.4 Kody migania LED „MS” i sposoby usuwania błędu

W tym rozdziale opisano diagnostykę wyświetlaną przez LED „MS” w postaci kodu migania.

Jeśli przedstawionych poniżej błędów nie da się usunąć opisanymi sposobami, należy skontaktować się ze wsparciem WAGO. Prosimy podać kod migania.

tel.: +48 71 360 29 33

e-mail: wsparcie.techniczne@wago.com

Tabela 118: Przegląd kodów błędu LED „MS”

Kod błędu	Znaczenie
1	Błąd konfiguracji

Tabela 119: Kod błędu 1, znaczenie kodu migania i sposoby usuwania błędu

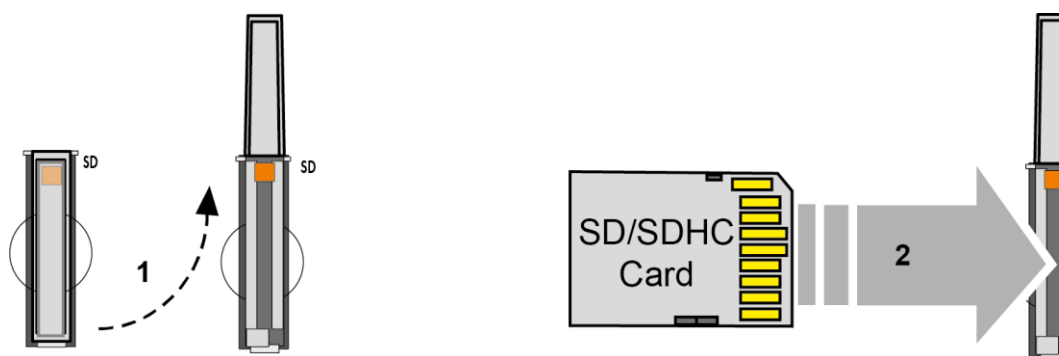
Argument błędu	Przyczyna	Środek zaradczy
5	Błąd zgodności konfiguracji sterownika z magistralą systemową	- Skontrolować dane o włożonych modułach I/O w konfiguracji sterowania CODESYS. - Dostosować je do faktycznie włożonych modułów I/O. - Skompilować ponownie projekt. - Załadować od nowa projekt do sterownika.

15 Serwis

15.1 Wkładanie i wyjmowanie karty pamięci

15.1.1 Wkładanie karty pamięci

1. Użyć przyrządu montażowego lub śrubokręta, aby otworzyć przezroczystą klapkę, odchylając ją do góry. Miejsce włożenia narzędzia zaznaczone jest strzałką.
2. Przytrzymać kartę pamięci w sposób przedstawiony na poniższym rysunku – ze stykami widocznymi po prawej stronie i ukośną krawędzią do góry
3. Trzymając kartę w tej pozycji, włożyć ją do odpowiedniego gniazda.
4. Wsunąć kartę pamięci do końca. Po puszczeniu karta pamięci nieco się odsunie, a następnie zatrzaśnie (mechanizm push-push).
5. Zamknąć osłonę przez jej ponowne opuszczenie w dół aż do zatrzaśnięcia.
6. Zamkniętą klapkę można uszczelnić przez otwór w obudowie obok klapki i w klapce.



Ilustracja 161: Wkładanie karty pamięci

15.1.2 Wyjmowanie karty pamięci

1. Zdjąć obecną uszczelkę.
2. Użyć przyrządu montażowego lub śrubokręta, aby otworzyć przezroczystą klapkę, odchylając ją do góry. Miejsce włożenia narzędzia zaznaczone jest strzałką.
3. W celu wyjęcia karty pamięci najpierw należy wcisnąć ją delikatnie do wnętrza gniazda (mechanizm push-push). Spowoduje to zwolnienie blokady mechanicznej.
4. Po puszczeniu karta wysunie pod wpływem nacisku sprężyny.
5. Wyjąć kartę pamięci.
6. Zamknąć osłonę przez jej ponowne opuszczenie w dół aż do zatrzaśnięcia.

15.2 Zmiany firmware

UWAGA



Nie wyłączać sterownika!

Przerwanie procedury aktualizacji standardowej / wstecznej może uszkodzić sterownik.

Dlatego podczas tej procedury nie należy wyłączać sterownika i odłączać zasilania!

Wskazówka



Uwzględnić dokumentację dla docelowej wersji firmware!

Dzięki aktualizacji firmware można zmieniać, usuwać lub rozszerzać właściwości i funkcje sterownika. Dlatego niektóre opisane właściwości i funkcje mogą nie być dostępne lub niektóre właściwości i funkcje sterownika mogą nie być opisane w dokumentacji.

Po aktualizacji firmware należy zawsze korzystać z dokumentacji odpowiadającej jego docelowej wersji.

W razie pytań skontaktować się ze wsparciem WAGO.

Wskazówka



Uwzględnić wersję firmware!

Przy urządzeniach z fabryczną instalacją firmware $\geq$ FW 05 nie jest możliwa aktualizacja wsteczna do wersji $\leq$ FW 04!

Należy zastosować specjalny obraz aktualizacji wstecznej.

Firmware można aktualizować na trzy różne sposoby:

- przy użyciu **e!COCKPIT**
- przy użyciu WAGOupload
- przy użyciu karty pamięci i WBM

15.2.1 Aktualizacja firmware standardowa / wsteczna przy użyciu **e!COCKPIT**

1. Otworzyć **e!COCKPIT**.
2. Założyć nowy projekt lub otworzyć już istniejący.
3. Do swojego projektu **e!COCKPIT** dodać co najmniej jeden sterownik – albo przez skanowanie sieci, albo otwarcie katalogu urządzenia i wpisanie w oknie dialogowym ustawień adresu IP sterownika.

Dodany sterownik wyświetli się w widoku urządzeń projektu.
4. Zaznaczyć wyświetlony sterownik i w zakładce „SCAN” kliknąć opcję „Apply Selection”.
5. W oknie dialogowym kliknąć **[Add]**.
6. Następnie w zakładce „DEVICE” kliknąć **[Replace Firmware]**.

Pojawi się okno „Replace Firmware”.
7. W oknie dialogowym „Replace Firmware” w punkcie „Available firmware on the PC” wybrać żądany firmware lub kliknąć „Select File” i wybrać plik *.wup żadanego firmware.
8. Kliknąć **[Replace Firmware]**, aby załadować do sterownika nowy firmware.
9. Poczekać, aż proces zostanie zakończony komunikatem o statusie i kliknąć przycisk **[OK]**, aby zamknąć okno.

Nowo zainstalowany firmware jest dostępny na sterowniku.

15.2.2 Aktualizacja firmware standardowa / wsteczna przy użyciu WAGOupload

1. Uruchomić WAGOupload.
2. Kliknąć **[Update Firmware]**.
3. W oknie dialogowym „Select Target Controllers“ przy opcji „Transfer via TCP/IP“ wpisać adres IP sterownika.
4. Kliknąć przycisk **[Find Controller]**.

Wybrany sterownik wyświetli się na liście.
5. Zaznaczyć wyświetlony sterownik i kliknąć przycisk **[Next]**.
6. W oknie dialogowym „Select Update File“ wybrać plik *.wup żadanego firmware.
7. Kliknąć **[Next]**.
8. Potwierdzić listę przyciskiem **[Next]**.
9. Poczekać, aż proces zostanie zakończony komunikatem o statusie i kliknąć przycisk **[Exit]**, aby zamknąć okno.

Nowo zainstalowany firmware jest dostępny na sterowniku.

15.2.3 Aktualizacja firmware standardowa / wsteczna przy użyciu karty pamięci i WBM

Aby wgrać do sterownika nowszą lub starszą wersję firmware, należy postępować w następujący sposób:

1. Najpierw skopiować obraz firmware (plik *.img) na kartę pamięci, np. narzędziem „Win32 Disk Imager“ lub „UNetbootin“.
2. Zapisać aplikację i ustawienia sterownika.
3. Wyłączyć sterownik.
4. Włożyć do gniazda kartę pamięci z nowym firmware. W razie potrzeby zastosować specjalny obraz aktualizacji wstecznej (patrz wyżej).
5. Włączyć sterownik.

Sterownik uruchamia się z obrazem firmware, który ma być zainstalowany z karty pamięci.

6. Po uruchomieniu sterownika otworzyć stronę WBM „Administration“ > „Create Boot Image“ (w tym celu należy zawsze zmienić tymczasowy adres IP).
7. Utworzyć obraz boot w wewnętrznej pamięci. W tym celu kliknąć przycisk **[Start Copy]**.
8. Po zakończeniu tej czynności wyłączyć sterownik.
9. Wyjąć kartę pamięci.
10. Włączyć ponownie sterownik.

Sterownik uruchomi się z nową wersją firmware.

15.3 Aktualizacja certyfikatów Root

Aby uaktualnić w sterowniku certyfikaty Root, należy postępować w następujący sposób:

1. Pobrać do sterownika aktualny plik Root CA bundle ze strony internetowej <https://curl.haxx.se/ca>.
2. Zmienić nazwę pliku na „ca-certificates.crt”.
3. Przesłać plik za pomocą SFTP lub FTP Client do folderu /etc/ssl/certs w sterowniku.
4. Zrestartować sterownik. W tym celu należy skorzystać z funkcji Reboot w WBM lub CBM.

16 Demontaż

OSTRZEŻENIE Ryzyko zranienia stykami nożowymi z ostrymi krawędziami!



Ponieważ styki nożowe mają bardzo ostre krawędzie, istnieje ryzyko zranienia w przypadku nieostrożnej obsługi modułów I/O. Nie należy dotykać styków nożowych.

16.1 Usuwanie urządzeń

NIEBEZPIECZEŃSTWO Nie pracować przy urządzeniach znajdujących się pod napięciem!

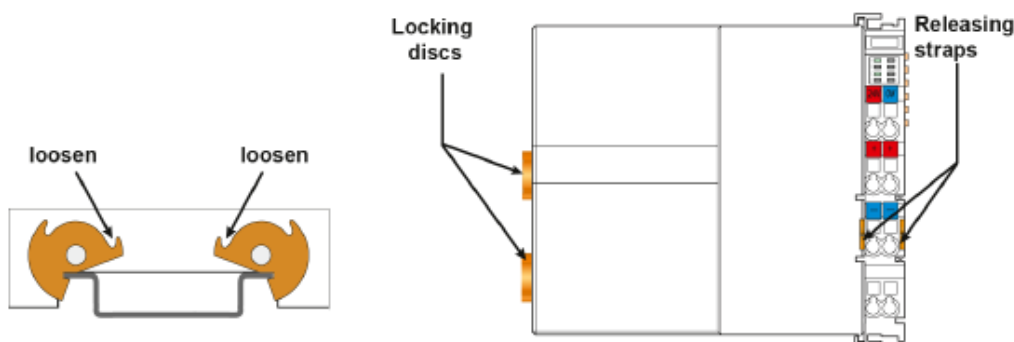


Niebezpieczne napięcie elektryczne może spowodować porażenie prądem elektrycznym i oparzenia. Przed rozpoczęciem montażu, instalacji, usuwania usterek lub prac konserwacyjnych należy zawsze odłączyć urządzenie od zasilania.

16.1.1 Demontaż sterownika

1. Przekręcić obie blokady ryglujące ostrzem przyrządu montażowego do momentu, aż wyczepią się one z szyny montażowej.
2. Pociągając za oba uchwyty zwalniające blokadę, wyjąć sterownik z układu.

W momencie demontażu sterownika połączenia elektryczne styków magistrali systemowej i styków mocy z kolejnym modułem I/O zostają rozłączone.



Ilustracja 162: Zwolnienie zaczepu ryglującego

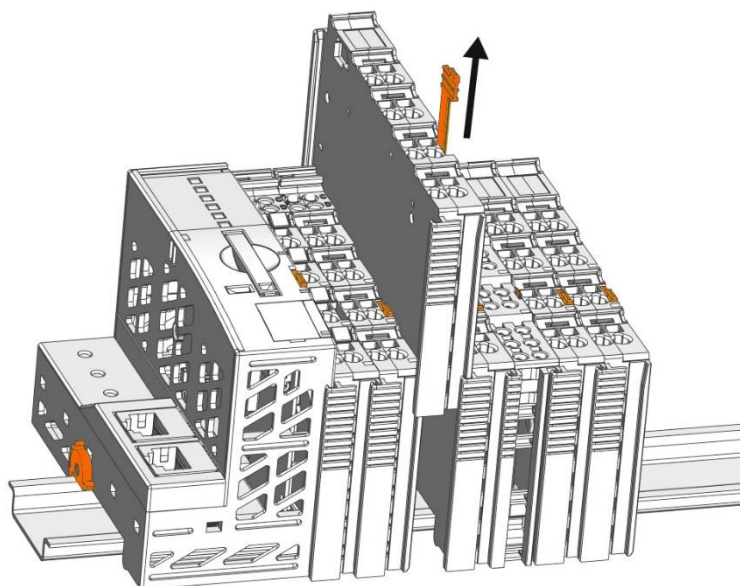
Wskazówka Nie rozłączać elementów obudowy sterownika!



Elementy obudowy sterownika są ze sobą połączone na stałe. Części zasilającej z zaciskami CAGE CLAMP® nie można oddzielać od pozostałej części obudowy.

16.1.2 Demontaż modułu I/O

1. Pociągnąć za uchwyt zwalniający blokadę i wyjąć moduł I/O z układu.



Ilustracja 163: Usuwanie modułu I/O (przykład)

Podczas demontażu modułu I/O połączenia elektryczne styków magistrali systemowej oraz styków mocy z kolejnym modułem I/O są rozłączane.

17 Utylizacja

17.1 Sprzęt elektryczny i elektroniczny



Nie utylizować sprzętu elektrycznego i elektronicznego razem z odpadami komunalnymi. Dotyczy to także produktów bez tego znaku.

Urządzenia elektryczne i elektroniczne zawierają surowce, materiały i substancje, które mogą być szkodliwe dla środowiska oraz zdrowia. Wycofane z eksploatacji urządzenia elektryczne i elektroniczne należy utylizować zgodnie z przepisami. Na terenie Europy obowiązuje dyrektywa WEEE 2012/19/EU. W poszczególnych krajach mogą obowiązywać osobne dyrektywy i ustawy.



Prawidłowa utylizacja służy zachowaniu zdrowia, chroni środowisko przed szkodliwymi substancjami pochodzącymi z urządzeń elektrycznych i elektronicznych.

- Należy przestrzegać krajowych i lokalnych przepisów dotyczących utylizacji sprzętu elektrycznego i elektronicznego.
- Przed utylizacją usunąć dane zapisane w urządzeniach elektrycznych i elektronicznych.
- Wyjąć zamontowane ewentualnie baterie, akumulatory i karty pamięci.
- Urządzenia elektryczne i elektroniczne należy oddać do lokalnych punktów zbiórki odpadów.

Nieprawidłowa utylizacja sprzętu elektrycznego i elektronicznego może mieć negatywny wpływ na zdrowie ludzi i środowisko.

17.2 Opakowanie

Opakowanie zawiera materiały, które mogą być użyte ponownie.

Na terenie Europy obowiązują dyrektywy dotyczące opakowań PPWD 94/62/EU i 2004/12/EU. W poszczególnych krajach mogą obowiązywać osobne dyrektywy i ustawy.

Prawidłowa utylizacja opakowań chroni środowisko oraz umożliwia zrównoważone i efektywne wykorzystanie zasobów.

- Należy przestrzegać krajowych i lokalnych przepisów dotyczących utylizacji opakowań.
- Wszystkie opakowania należy zutylizować w sposób, zapewniający odpowiednio wysoki poziom recyklingu, odzysku oraz ponownego użycia surowców.

Nieprawidłowa utylizacja opakowań może mieć szkodliwy wpływ na środowisko i przyczyniać się do marnotrawstwa surowców.

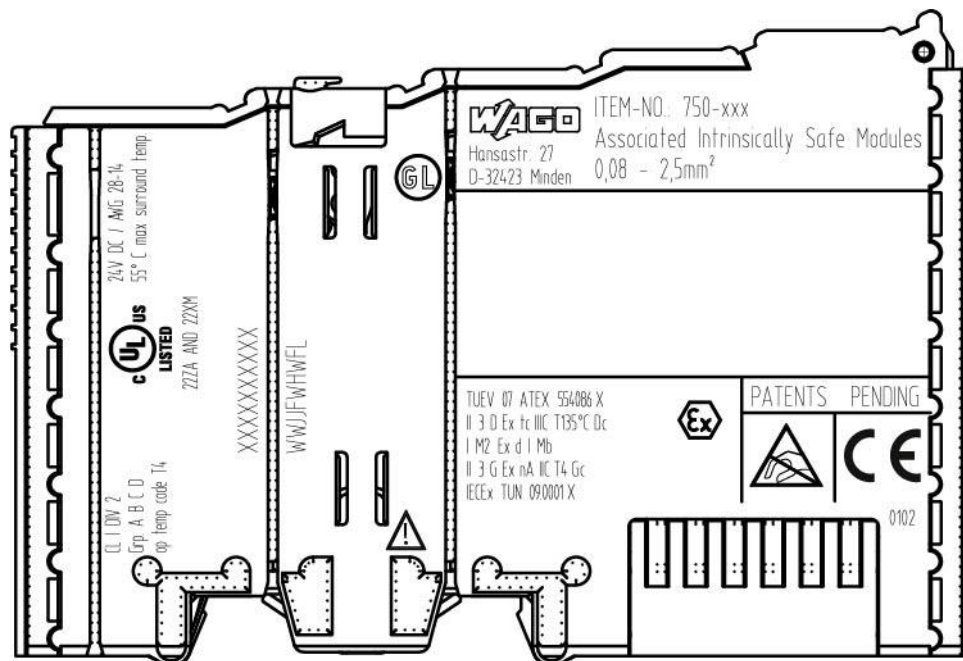
18 **Użytkowanie w przestrzeniach zagrożonych wybuchem**

WAGO I/O System 750 (urządzenie elektryczne) jest przeznaczony do stosowania w strefie 2 obszaru zagrożenia wybuchem i można go stosować zgodnie z oznaczeniem i przepisami instalacyjnymi odpowiednimi dla danego zastosowania.

Kolejne rozdziały podają ogólne oznaczenie komponentów oraz obowiązujące warunki eksploatacji. Przestrzegać informacji zawartych w rozdziale „Warunki stosowania”, jeżeli moduł I/O ma odpowiednią aprobatę lub podlega zakresowi zastosowania dyrektywy ATEX.

18.1 Przykładowa konstrukcja i oznaczanie

18.1.1 Oznaczanie dla Europy zgodnie z ATEX i IECEx



Ilustracja 164: Przykład nadruku zgodnie z ATEX i IECEx

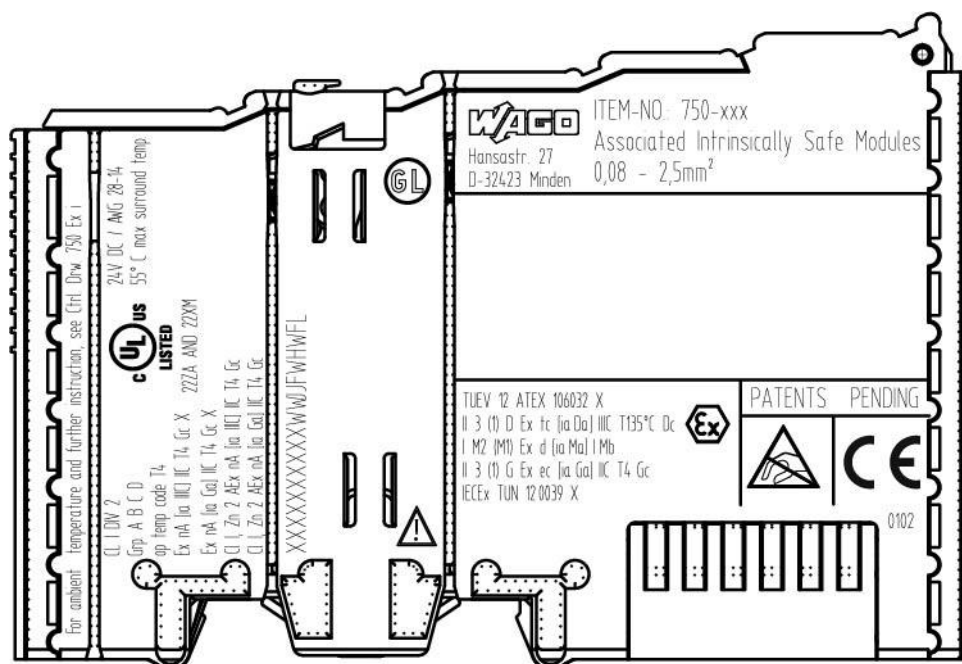
TÜV 07 ATEX 554086 X
II 3 D Ex tc III C T135°C Dc
I M2 Ex d I Mb
II 3 G Ex nA IIC T4 Gc
IECEx TUN 090001 X



Ilustracja 165: Szczegół – przykład nadruku zgodnie z ATEX i IECEx

Tabela 120: Opis przykładowego nadruku zgodnie z ATEX i IECEx

Tekst	Opis
TUEV 07 ATEX 554086 X IECEx TUN 09.0001 X	Jednostka aprobowująca lub numer zaświadczenia
Pyły	
II	Grupa urządzeń: wszystkie oprócz górnictwa
3 D	Kategoria urządzenia 3 (strefa 22)
Ex	Oznaczenie ochrony przeciwwybuchowej
tc	Rodzaj budowy przeciwwybuchowej: ochrona przez obudowę
IIIC	Grupa pyłów: wybuchowa atmosfera zawierająca pył
T135°C	Maks. temperatura powierzchni obudowy (bez warstwy pyłów)
Dc	Poziom zabezpieczenia urządzeń (EPL)
Górnictwo	
I	Grupa urządzeń: górnictwo
M2	Kategoria urządzeń: wysoki stopień bezpieczeństwa
Ex	Oznaczenie ochrony przeciwwybuchowej
d	Rodzaj budowy przeciwwybuchowej: osłona ognioszczelna
I	Urządzenia elektryczne pracujące w wybuchowej mieszaninie gazów kopalnianych
Mb	Poziom zabezpieczenia urządzeń (EPL)
Gazy	
II	Grupa urządzeń: wszystkie oprócz górnictwa
3 G	Kategoria urządzenia 3 (strefa 2)
Ex	Oznaczenie ochrony przeciwwybuchowej
nA	Rodzaj budowy przeciwwybuchowej: urządzenia nieiskrzące
IIC	Grupa gazów: obszary zagrożone wybuchem gazu
T4	Klasa temperaturowa: maks. temperatura powierzchni 135°C
Gc	Poziom zabezpieczenia urządzeń (EPL)



Ilustracja 166: Przykład nadruku na certyfikowanym module I/O Ex i z godnie z ATEX i IECEx

TUEV 12 ATEX 106032 X
II 3 (1) D Ex tc [ia Da] IIC T135°C Dc
I M2 (M1) Ex d [ia Ma] I Mb
II 3 (1) G Ex ec [ia Ga] IIC T4 Gc
IECEX TUN 12 0039 X



Ilustracja 167: Szczegół – przykład nadruku na certyfikowanym module I/O Ex i z godnie z ATEX i IECEx

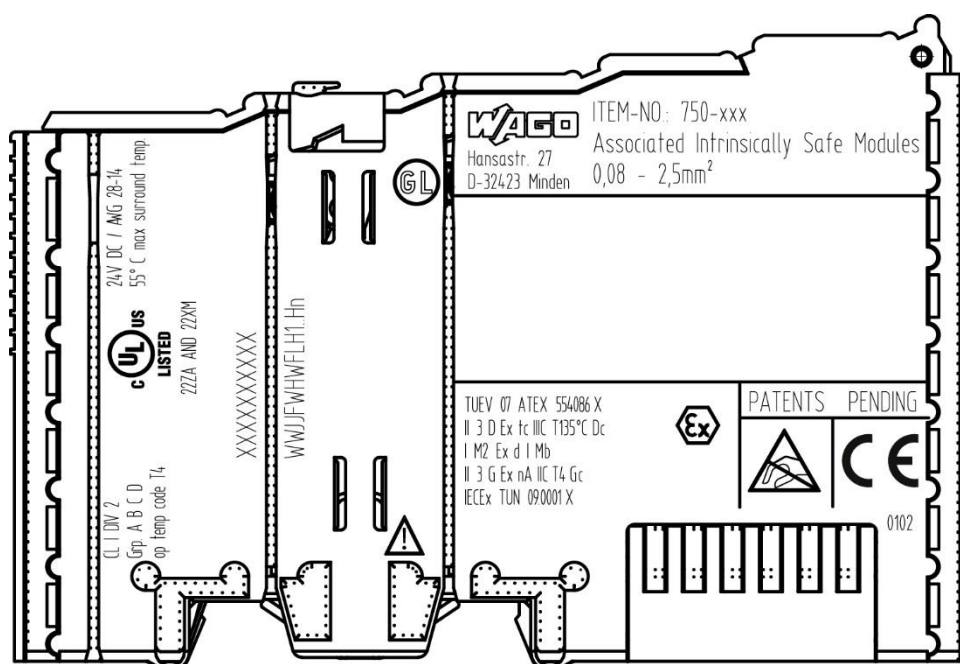
Tabela 121: Opis przykładowego nadruku na certyfikowanym module I/O Ex i zgodnie z ATEX i IECEx

Tekst	Opis
TUEV 12 ATEX 106032 X IECEx TUN 12 0039 X	Jednostka aprobowująca lub numer zaświadczenia
Pyły	
II	Grupa urządzeń: wszystkie oprócz górnictwa
3 (1) D	Kategoria urządzenia 3 (strefa 22) zachowane środki bezpieczeństwa dla urządzeń kategorii 1 (strefa 20)
Ex	Oznaczenie ochrony przeciwwybuchowej
tc	Rodzaj budowy przeciwwybuchowej: ochrona przez obudowę
[ia Da]	Rodzaj budowy przeciwwybuchowej i poziom zabezpieczenia urządzeń (EPL): przynależne urządzenie z iskrobezpiecznymi obwodami prądowymi do strefy 20
IIIC	Grupa pyłów: wybuchowa atmosfera zawierająca pył
T135°C	Maks. temperatura powierzchni obudowy (bez warstwy pyłów)
Dc	Poziom zabezpieczenia urządzeń (EPL)
Górnictwo	
I	Grupa urządzeń: górnictwo
M2 (M1)	Kategoria urządzeń: wysoki stopień bezpieczeństwa, z obwodami prądowymi o wysokim poziomie bezpieczeństwa
Ex	Oznaczenie ochrony przeciwwybuchowej
d	Rodzaj budowy przeciwwybuchowej: osłona ognioszczelna
[ia Ma]	Rodzaj budowy przeciwwybuchowej i poziom zabezpieczenia urządzeń (EPL): przynależne urządzenie z iskrobezpiecznymi obwodami prądowymi
I	Urządzenia elektryczne pracujące w wybuchowej mieszaninie gazów kopalnianych
Mb	Poziom zabezpieczenia urządzeń (EPL)
Gazy	
II	Grupa urządzeń: wszystkie oprócz górnictwa
3 (1) G	Kategoria urządzenia 3 (strefa 2) zachowane środki bezpieczeństwa dla urządzeń kategorii 1 (strefa 0)
Ex	Oznaczenie ochrony przeciwwybuchowej
ec	Rodzaj budowy przeciwwybuchowej: budowa wzmocniona
[ia Ga]	Rodzaj budowy przeciwwybuchowej i poziom zabezpieczenia urządzeń (EPL): przynależne urządzenie z iskrobezpiecznymi obwodami prądowymi do strefy 0

Tabela 121: Opis przykładowego nadruku na certyfikowanym module I/O Ex i zgodnie z ATEX i IECEx

IIC	Grupa gazów: obszary zagrożone wybuchem gazu
T4	Klasa temperaturowa: maks. temperatura powierzchni 135°C
Gc	Poziom zabezpieczenia urządzeń (EPL)

18.1.2 Oznaczanie na USA (NEC) i Kanadę (CEC)



Ilustracja 168: Przykład nadruku zgodnie z NEC

CL I DIV 2
Grp. A B C D
op temp code T4

Ilustracja 169: Szczegół – przykład nadruku zgodnie z NEC 500

Tabela 122: Opis przykładowego nadruku zgodnie z NEC 500

Tekst	Opis
CL I	Grupa gazów: obszary zagrożone wybuchem gazu
DIV 2	Obszar zastosowania
Grp. A B C D	Grupa wybuchowości atmosfery (gazy)
op temp code T4	Klasa temperaturowa

CI I, Zn 2 AEx nA [ia Ga] IIC T4 Gc

Ilustracja 170: Szczegół – przykład nadruku na certyfikowanym module I/O Ex i zgodnie z NEC 505

Tabela 123: Opis przykładowego nadruku na certyfikowanym module I/O Ex i zgodnie z NEC 505

Tekst	Opis
CI I,	Grupa gazów: obszary zagrożone wybuchem gazu
Zn 2	Strefa
AEx	Urządzenia elektryczne w obszarach zagrożonych wybuchem
nA	Rodzaj budowy przeciwwybuchowej
[ia Ga]	Rodzaj budowy przeciwwybuchowej i grupa lub poziom zabezpieczenia urządzeń (EPL): przynależne urządzenie z iskrobezpiecznymi obwodami prądowymi do strefy 20
IIC	Grupa
T4	Klasa temperaturowa
Gc	Poziom zabezpieczenia urządzeń (EPL)

CI I, Zn 2 AEx nA [ia IIIC] IIC T4 Gc

Ilustracja 171: Szczegół – przykład nadruku na certyfikowanym module I/O Ex i zgodnie z NEC 506

Tabela 124: Opis przykładowego nadruku na certyfikowanym module I/O Ex i zgodnie z NEC 506

Tekst	Opis
CI I,	Grupa gazów: obszary zagrożone wybuchem gazu
Zn 2	Strefa
AEx	Urządzenia elektryczne w obszarach zagrożonych wybuchem
nA	Rodzaj budowy przeciwwybuchowej
[ia IIIC]	Rodzaj budowy przeciwwybuchowej i grupa lub poziom zabezpieczenia urządzeń (EPL): przynależne urządzenie z iskrobezpiecznymi obwodami prądowymi do strefy 20
IIC	Grupa
T4	Klasa temperaturowa
Gc	Poziom zabezpieczenia urządzeń (EPL)

Ex nA [ia IIIC] IIC T4 Gc X

Ex nA [ia Ga] IIC T4 Gc X

Ilustracja 172: Szczegół – przykład nadruku na certyfikowanym module I/O Ex i zgodnie z CEC 18 załącznik J

Tabela 125: Opis przykładowego nadruku na certyfikowanym module I/O Ex i zgodnie z CEC 18 załącznik J

Tekst	Opis
Pyły	
Ex	Urządzenia elektryczne w obszarach zagrożonych wybuchem
nA	Rodzaj budowy przeciwwybuchowej
[ia IIIC]	Rodzaj budowy przeciwwybuchowej i grupa lub poziom zabezpieczenia urządzeń (EPL): przynależne urządzenie z iskrobezpiecznymi obwodami prądowymi do strefy 20
IIC	Grupa
T4	Klasa temperaturowa
Gc	Poziom zabezpieczenia urządzeń (EPL)
X	Informacje dotyczące warunków stosowania
Gaz	
Ex	Urządzenia elektryczne w obszarach zagrożonych wybuchem
nA	Rodzaj budowy przeciwwybuchowej
[ia Ga]	Rodzaj budowy przeciwwybuchowej i grupa lub poziom zabezpieczenia urządzeń (EPL): przynależne urządzenie z iskrobezpiecznymi obwodami prądowymi do strefy 0
IIC	Grupa
T4	Klasa temperaturowa
Gc	Poziom zabezpieczenia urządzeń (EPL)
X	Informacje dotyczące warunków stosowania

18.2 Warunki stosowania

Budowa i eksploatacja urządzeń elektrycznych w obszarach zagrożonych wybuchem powinna uwzględniać stosowne lokalne i międzynarodowe wymagania i zalecenia.

18.2.1 Szczególne wskazówki i ochrona przeciwwybuchowa

W bezpośredniej bliskości WAGO I/O System 750 (nazywanym poniżej produktem) należy umieścić następujące ostrzeżenia:

OSTRZEŻENIE – NIE WYJMOWAĆ ANI NIE WYMIENIAĆ BEZPIECZNIKA POD NAPIĘCIEM!

OSTRZEŻENIE – NIE ODŁĄCZAĆ URZĄDZENIA OD SIECI POD NAPIĘCIEM!

OSTRZEŻENIE – ODŁĄCZAĆ OD SIECI TYLKO W PRZESTRZENIACH NIEZAGROŻONYCH WYBUCHEM!

Przed zastosowaniem komponentów należy sprawdzić, czy ich użycie jest zgodne z nadrukiem. Także przy wymianie podzespołów należy zwrócić uwagę na ewentualną zmianę nadruku.

Produkt jest otwartym urządzeniem elektrycznym. Może być używany wyłącznie w obudowach lub rozdzielniach elektrycznych, spełniających następujące warunki:

- Otwieranie tylko narzędziem lub odpowiednim kluczem
- Wewnątrz stopień zanieczyszczenia 1 lub 2
- Temperatura powietrza wewnątrz podczas pracy w zakresie $0^{\circ}\text{C} \leq T_a \leq +55^{\circ}\text{C}$ lub $-20^{\circ}\text{C} \leq T_a \leq +60^{\circ}\text{C}$ dla komponentów z rozszerzeniem numeru .../025-xxx lub $-40^{\circ}\text{C} \leq T_a \leq +70^{\circ}\text{C}$ dla komponentów z rozszerzeniem numeru .../040-xxx
- Stopień ochrony co najmniej IP54 (zgodnie z IEC 60529)
- Przy zastosowaniu w strefie 2 (Gc) spełnienie odpowiednich wymagań zawartych w normach EN/IEC/ABNT NBR IEC 60079-0, -7, -11, -15
- Przy zastosowaniu w strefie 22 (Dc) spełnienie odpowiednich wymagań zawartych w normach EN/IEC/ABNT NBR IEC 60079-0, -7, -11, -15 i -31
- Przy zastosowaniu w górnictwie (Mb) co najmniej stopień ochrony IP64 (zgodnie z EN/IEC 60529) i dostateczna ochrona zgodnie z EN/IEC/ABNT NBR IEC 60079-0 i -1
- Prawidłowe zamontowanie i zgodność z wymogami przy konkretnym podziale na strefy i kategorie urządzeń muszą być przeanalizowane i poświadczone przez jednostkę notyfikowaną (ExNB)!

Należy wykluczyć możliwość przejściowego wystąpienia atmosfery wybuchowej w czasie prac instalacyjnych, konserwacyjnych i naprawczych. Chodzi tu między innymi o następujące czynności:

- Wtykowy montaż i demontaż komponentów
- Nawiązywanie lub rozłączanie połączeń poprzez złącza sieci obiektowej, antenowe, D-Sub, ETHERNET lub USB, porty DVI, karty pamięci, złącza konfiguracyjne i programowe ogólne lub serwisowe, a szczególnie:
 - Uruchamianie przełączników DIP, przełączników kodujących lub potencjometrów
- Wymiana bezpiecznika

Podłączanie i odłączanie obwodów prądowych nieiskrobezpiecznych jest dozwolone wyłącznie w następujących przypadkach:

- Obwód prądowy jest odłączony od napięcia.
- Istnieje pewność, że obszar nie jest zagrożony wybuchem.

Na zewnątrz urządzenia należy podjąć odpowiednie działania zmierzające do tego, aby z uwagi na przejściowe zakłócenia napięcie pomiarowe nie zostało przekroczone o więcej niż 40% (np. w wypadku powtórnego zasilania obiektowego).

Komponenty urządzenia, przeznaczone do zastosowań iskrobezpiecznych, mogą być zasilane wyłącznie przez moduły zasilające 750-606 lub 750-625/000-001.

Do tych komponentów można podłączać wyłącznie urządzenia obiektowe, których zasilanie odpowiada kategorii przepięć I lub II.

18.2.2 Szczególne informacje dotyczące UL Hazardous Location

Dla UL Hazardous Location, zgodnie z File E198726, istnieją dodatkowo następujące wymagania:

- Zastosowanie wyłącznie w Class I, Division 2, Group A, B, C, D lub w przestrzeniach niezagrożonych wybuchem
- Złącza ETHERNET służą wyłącznie połączeniu z sieciami komputerowymi (LANs) i nie mogą być wykorzystywane do podłączania sieci telefonicznych lub przewodów telekomunikacyjnych.
- OSTRZEŻENIE – Moduł I/O 750-642 wolno stosować wyłącznie w połączeniu z zewnętrzną anteną 758-910!
- OSTRZEŻENIE – Komponentów urządzenia wyposażonych w bezpieczniki nie wolno integrować z obwodami prądowymi, w których może nastąpić przeciążenie!
Należą do nich np. obwody silnika.
- OSTRZEŻENIE – Przy instalacji modułu wyjść dwustanowych 750-538 należy uwzględnić „Rysunek schematyczny nr 750538” zawarty w podręczniku!

Informacja



Dodatkowa informacja

Certyfikat można otrzymać na zapytanie. Należy przestrzegać również wskazówek na ulotce załączonej do modułu I/O. Podręcznik zawierający wymienione powyżej warunki bezpiecznego użytkowania musi być zawsze dostępny dla użytkownika.

19 Załącznik

19.1 Dialogi konfiguracyjne

19.1.1 Web Based Management (WBM)

19.1.1.1 Zakładka „Information“

19.1.1.1.1 Strona „Device Status“

Na stronie „Device Status“ wyświetlane są dane identyfikacyjne produktu i najważniejsze właściwości sieci.

Grupa „Device Details“

W tej grupie wyświetlane są dane identyfikacyjne produktu.

Tabela 126: Strona WBM „Device Status“ – grupa „Device Details“

Parametr	Znaczenie
Product Description	Nazwa produktu
Ordernumber	Numer katalogowy produktu
Serial	Unikatowy numer serii produktu
License Information	Informuje, że system runtime CODESYS jest zainstalowany.
Firmware Revision	Wersja firmware

Grupa „Network TCP/IP Details“

W tej grupie wyświetlane są właściwości sieci i interfejsów produktu.

Tabela 127: Strona WBM „Device Status” – grupa „Network TCP/IP Details”

Parametr	Znaczenie	
DIP Switch Status	Status przełącznika adresów; ten obszar widoczny jest tylko wtedy, gdy urządzenie ma przełącznik adresów.	
DIP Switch Mode	Nastawa przełącznika adresów	
	Off (0)	Przydzielanie adresów IP poprzez np. WBM
	static (1 ... 254)	Statyczne przydzielanie adresów IP poprzez przełącznik adresów
	dhcp (255)	Dynamiczne przydzielanie adresów IP poprzez DHCP
DIP Switch Value	Ustawiona wartość przełącznika adresów	
Bridge <n>	Aktualnie skonfigurowany bridge; dla każdego skonfigurowanego bridge'a właściwości są wyświetlane w osobnym obszarze.	
Mac Address	Adres MAC, służący do identyfikacji i adresowania produktu	
IP Source	Aktualne odniesienie adresu IP	
	none	Nie została wybrana metoda przydzielania adresów IP; ma to miejsce np. wtedy, gdy bridge został dodany przez zmiany w konfiguracji bridge'ów. W zakładce Configuration na stronie Networking > TCP/IP Configuration należy wybrać źródło.
	static IP	Statyczne przydzielanie adresów
	dhcp	Dynamiczne przydzielanie adresów IP poprzez DHCP
	bootp	Dynamiczne przydzielanie adresów IP poprzez BootP (gdy BootP jest obsługiwany)
	external	Adres IP przypisywany jest ewentualnie przez aplikację sieciową; ma to miejsce na przykład wtedy, gdy adres IP zarządzany jest przez aplikację PROFINET.
IP Address	Aktualny adres IP produktu	
Subnet Mask	Aktualna maska podsieci produktu	

19.1.1.1.2 Strona „Vendor Information“

Na stronie „Vendor Information“ wyświetla się nazwa i adres producenta.

19.1.1.1.3 Strona „PLC Runtime Information“

Na stronie „PLC Runtime Information“ znajdują się informacje o aktywowanym systemie runtime i programie PLC utworzonym w środowisku programistycznym. Ponadto jest tu link otwierający WebVisu.

Grupa „Runtime“

Tabela 128: Strona WBM „PLC Runtime Information” – grupa „Runtime“

Parametr	Znaczenie
Version	Tu wyświetlana jest wersja aktualnie aktywowanego systemu runtime. Przy wyłączonym systemie runtime wyświetlana jest informacja „None“, a dalsze pola tej grupy są wyłączone.
Webserver Version	Tu wyświetlany jest numer wersji serwera WWW. Pole to widoczne jest tylko wtedy, gdy sterownik obsługuje system runtime CODESYS V2 i jako system runtime ustawiony jest CODESYS V2.
State	Tu wyświetlany jest stan pracy PLC. Pole to widoczne jest tylko wtedy, gdy sterownik obsługuje system runtime CODESYS V2 i jako system runtime ustawiony jest CODESYS V2.
	STOP Program PLC nie jest wykonywany.
	RUN Program PLC jest wykonywany.
Number of Tasks	Tu wyświetlana jest liczba zadań w programie PLC. Pole to widoczne jest tylko wtedy, gdy sterownik obsługuje system runtime CODESYS V2 i jako system runtime ustawiony jest CODESYS V2.

Grupa „WebVisu“

Tu znajduje się link, którym można otworzyć WebVisu.

Grupa „Projekt Details“

Grupa ta widoczna jest tylko wtedy, gdy sterownik obsługuje system runtime CODESYS V2 i jako system runtime ustawiony jest CODESYS V2.

Tabela 129: Strona WBM „PLC Runtime Information” – grupa „Projekt Details“

Parametr	Znaczenie
Date	Tu wyświetlana jest data ostatniego zapisu projektu.
Title	Tu wyświetlane są informacje o projekcie, które programista wprowadził do programu PLC (w oprogramowaniu programistycznym pod Projekt > Informacje o projekcie ...).
Version	
Author	
Description	
Checksum	Tu wyświetlana jest wyliczona suma kontrolna projektu.

Grupa (grupy) „Task <n>“

Podczas wykonywania programu PLC dla każdego zadania wyświetlana jest osobna grupa. Standardowo wyświetlany jest tylko nagłówek grupy z numerem, nazwą i ID zadania.

Grupa ta widoczna jest (grupy te widoczne są) tylko wtedy, gdy sterownik obsługuje system runtime CODESYS V2 i jako system runtime ustawiony jest CODESYS V2.

Tabela 130: Strona WBM „PLC Runtime Information” – grupa (grupy) „Task n“

Parametr	Znaczenie
Cycle count	Liczba cykli zadania od startu systemu
Cycletime (µsec)	Aktualnie mierzony czas wykonywania zadania
Cycletime min (µsec)	Minimalny czas wykonywania zadania od startu systemu
Cycletime max (µsec)	Maksymalny czas wykonywania zadania od startu systemu
Cycletime avg (µsec)	Średni czas wykonywania zadania od startu systemu
Status	Status zadania (np. RUN, STOP)
Mode	Tryb wykonywania zadania (np. cykliczny)
Priority	Ustawiony priorytet zadania
Interval (msec)	Ustawiony interwał zadania

19.1.1.1.4 Strona „WAGO Software License Agreement“

Na stronie „WAGO Software License Agreement“ wyszczególnione są warunki licencji dla oprogramowania WAGO zastosowanego w produkcie.

19.1.1.1.5 Strona „Open Source Licenses“

Na stronie „Open Source Licenses“ wyszczególnione są (w kolejności alfabetycznej) warunki licencji dla oprogramowania Open Source zastosowanego w produkcie.

19.1.1.1.6 Strona „WBM Third Party License Information“

Na stronie „WBM Third Party License Information“ znajdują się teksty o licencji dla oprogramowania Open Source, dotyczące samego systemu WBM.

19.1.1.1.7 Strona „WBM Version“

Na stronie „WBM Version“ znajdują się informacje o wersji różnych obszarów („Plugins“), zawartych w WBM. Informacje te mogą być przydatne dla serwisanta w przypadku, gdy zostanie stwierdzony błąd w systemie WBM.

19.1.1.2 Zakładka „Configuration“

19.1.1.2.1 Strona „PLC Runtime Configuration“

Na stronie „PLC Runtime Configuration“ znajdują się ustawienia projektu boot utworzonego w środowisku programistycznym i ustawienia do wizualizacji sieciowej utworzonej w systemie runtime.

Grupa „General PLC Runtime Configuration“

Tabela 131: Strona WBM „PLC Runtime Configuration” – grupa „General PLC Runtime Configuration“

Parametr	Znaczenie	
PLC runtime version	Tu można wybrać, który system runtime PLC jest aktywowany.	
	None	Żaden system runtime nie jest aktywowany.
	CODESYS V2	System runtime CODESYS V2 jest aktywowany. Wartość ta widoczna jest tylko wtedy, gdy sterownik obsługuje system runtime CODESYS V2.
	<i>e!RUNTIME</i>	System runtime <i>e!RUNTIME</i> jest aktywowany. Wartość ta widoczna jest tylko wtedy, gdy sterownik obsługuje system runtime <i>e!RUNTIME</i> .
Home directory on memory card enabled	Tu ustawia się, czy katalog Home dla systemu runtime ma być zapisywany na karcie pamięci.	
	Disabled	Katalog Home dla systemu operacyjnego zapisywany jest w wewnętrznej pamięci sterownika.
	Enabled	Katalog Home dla systemu operacyjnego zapisywany jest na karcie pamięci.

Wskazówka Przy przełączeniu systemu runtime usuwane są wszystkie dane!



Przy przełączeniu systemu runtime katalog Home dla systemu operacyjnego zostaje całkowicie usunięty.

Wskazówka Tylko pierwsza partycja może być wykorzystana jako katalog Home!



Tylko pierwsza partycja karty pamięci dostępna jest pod /media/sd i może zostać wykorzystana jako katalog Home.

Aby zastosować zmiany, kliknąć odpowiedni przycisk **[Submit]**. Zmiana systemu runtime jest realizowana natychmiast.

Zmiana katalogu Home zostanie zrealizowana dopiero po następnym restarcie

produktu. W tym celu należy skorzystać z funkcji Reboot WBM. Nie należy wyłączać urządzenia zbyt wcześnie!

Grupa „Webserver Configuration“

Tabela 132: Strona WBM „PLC Runtime Configuration” – grupa „Webserver Configuration“

Parametr	Znaczenie	
CODESYS 2 Webserver State	Tu wyświetlany jest status (enabled/disabled) serwera WWW CODESYS V2. Pole to widoczne jest tylko wtedy, gdy sterownik obsługuje system runtime CODESYS V2.	
e!RUNTIME Webserver State	Tu wyświetlany jest status (enabled/disabled) serwera WWW e!RUNTIME . Pole to widoczne jest tylko wtedy, gdy sterownik obsługuje system runtime e!RUNTIME .	
Default Webserver	Tu można wybrać, czy przy wpisaniu adresu IP sterownika ma być wyświetlany Web-Based-Management, czy wizualizacja sieciowa systemu runtime.	
	Zarządzanie przez stronę WWW	Wyświetla się Web-Based-Management.
	WebVisu	Wyświetla się wizualizacja sieciowa systemu runtime.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

W ustawieniu fabrycznym przy wpisaniu adresu IP otwiera się WBM.

W celu aktualizacji widoku po zmianie opcji należy jeszcze raz wpisać adres IP w pasku adresu przeglądarki internetowej.

Warunkiem wyświetlenia wizualizacji sieciowej jest włączony serwer WWW (w WBM pod „Ports and Services” -> „PLC Runtime Services”) oraz zainstalowana i odpowiednio skonfigurowana aplikacja.

Niezależnie od ustawienia domyślnego serwera WWW w każdej chwili można wywołać WBM za pomocą adresu „https://<adres IP>/wbm” oraz wizualizację sieciową za pomocą adresu „https://<adres IP>/webvisu”.

Wskazówka



Możliwe komunikaty błędu przy otwieraniu wizualizacji sieciowej

Komunikat „500 – Internal Server Error” oznacza, że serwer WWW nie jest włączony.

Strona o tytule „WebVisu not available” wskazuje, że do produktu nie została załadowana aplikacja z wizualizacją sieciową.

19.1.1.2.2 Strona „TCP/IP Configuration“

Na stronie „TCP/IP Configuration“ znajdują się ustawienia TCP/IP dla interfejsów sieci ETHERNET.

Grupa „TCP/IP Configuration“

Dla każdego skonfigurowanego bridge'a właściwości są wyświetlane w osobnym obszarze.

Tabela 133: Strona WBM „TCP/IP Configuration“ – grupa „TCP/IP Configuration“

Parametr	Znaczenie
Network Details Bridge <n>	Ustawienia dla aktualnie skonfigurowanego bridge'a
Current IP Address	Tu wyświetlany jest aktualny adres IP.
Current Subnet Mask	Tu wyświetlana jest aktualna maska podsieci.
IP Source	Tu można zdecydować, czy ma być zastosowane statyczne czy dynamiczne adresowanie IP.
	Static IP Statyczne adresowanie IP
	DHCP Dynamiczne adresowanie IP przez DHCP
	BootP Dynamiczne adresowanie IP przez BootP
IP Address	Tu wpisuje się statyczny adres IP. Jest on aktywny, gdy w polu IP Source zaznaczony jest „Static IP“.
Subnet Mask	Tu należy wpisać maskę podsieci. Jest on aktywny, gdy w polu IP Source zaznaczony jest „Static IP“.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Grupa „DNS Server“

Tabela 134: Strona WBM „TCP/IP Configuration“ – grupa „DNS Server“

Parametr	Znaczenie
New Server IP	tu dodaje się kolejne adresy DNS; Można wpisać 10 adresów.
Manually Assigned	Tu wyświetlane są adresy wpisanych serwerów DNS. Jeśli nie został wpisany serwer DNS, wyświetlana jest informacja „no DNS Servers configured“.
Assigned by DHCP	Tu wyświetlane są serwery DNS przydzielone przez DHCP (lub BootP). Jeśli nie został przydzielony serwer DNS przez DHCP (lub BootP), wyświetlana jest informacja „no DNS Servers assigned by DHCP“.

Aby dodać wpisany serwer DNS, należy kliknąć przycisk **[Add]**. Zmiana jest realizowana natychmiast.

Aby usunąć wybrany serwer DNS, należy kliknąć przycisk **[Delete]**. Zmiana jest realizowana natychmiast.

19.1.1.2.3 Strona „Ethernet Configuration“

Na stronie „Ethernet Configuration“ znajdują się ustawienia dla sieci ETHERNET.

Grupa „Bridge Configuration“

Tabela 135: Strona WBM „Ethernet Configuration“ – grupa „Bridge Configuration“

Parametr	Znaczenie
Bridge 1 ... <n>	Tu przyporządkowuje się fizyczne porty X1 ... X<n> do bramy logicznej. W tym celu należy nacisnąć odpowiedni przycisk opcji. Przyporządkowanie zostaje zaznaczone kolorem. Jeden port może być przyporządkowany do tylko jednej bramy.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Grupa „Switch Configuration“

Grupa ta widoczna jest tylko wtedy, gdy obsługiwana jest konfiguracja parametrów.

Tabela 136: Strona WBM „Ethernet Configuration“ – grupa „Switch Configuration“

Parametr	Znaczenie	
Port Mirror	Tu włącza się i wyłącza mirroring między portami.	
	None	Oba porty ETHERNET pracują normalnie.
	X1	Wymiana danych między X1 i systemem PFC jest odzwierciedlana na porcie X2.
	X2	Wymiana danych między X2 i systemem PFC jest odzwierciedlana na porcie X1.
Fast Aging	Tu ustawia się czas unieważnienia niewykorzystanych pozycji na liście adresów MAC z przydzielonymi portami do zewnętrznych urządzeń sieciowych. To pole jest aktywne tylko w trybie „Switched”. Fast Aging działa tylko w tym trybie.	
	Disabled	Niewykorzystany adres przepada po 200 sekundach.
	Enabled	Niewykorzystany adres przepada po 800 mikrosekundach.
Broadcast Protection	Tu ustawia się ograniczenie broadcast jako zabezpieczenie przed przeciążeniem.	
	Disabled	Brak ograniczenia pakietów broadcast
	1 % ... 5 %	Limitowanie przychodzących pakietów broadcast do wybranej wartości procentowej ogólnej możliwej przepustowości (10/100Mbit).
Rate Limit	Tu ustawia się podstawowe ograniczenie przychodzącej transmisji danych.	
	Disabled	Brak limitu dla przychodzącej transmisji danych.
	64 kbps ... 99 mbps	Limit do podanej wielkości dla przychodzącej transmisji danych.

Aby zastosować zmiany, kliknąć odpowiedni przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Grupa „Ethernet Interface Configuration“

Tabela 137: Strona WBM „Ethernet Configuration“ – grupa „Ethernet Interface Configuration“

Parametr	Znaczenie	
Interface X<n>	Dla każdego interfejsu zintegrowanego w sterowniku wyświetlany jest osobny obszar.	
Enabled	Tu można aktywować lub dezaktywować interfejs.	
Autonegotiation on	Przy aktywowanej autonegociacji tryby łączeniowe negocjowane są automatycznie z urządzeniem przeciwnym.	
Speed/Duplex	Tu można wybrać prędkość transmisji oraz typ duplex:	
	10 MBit half duplex	Informacje mogą być tylko wysyłane lub odbierane.
	100 MBit half duplex	
	10 MBit full duplex	Informacje mogą być równocześnie wysyłane i odbierane.
	100 Mbit full duplex	

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiany są realizowane natychmiast.

19.1.1.2.4 Strona „Configuration of Host and Domain Name“

Na stronie „Configuration of Host and Domain Name“ znajdują się ustawienia nazwy hosta i domeny.

Grupa „Hostname“

Tabela 138: Strona WBM „Configuration of Host and Domain Name“ – grupa „Hostname“

Parametr	Znaczenie
Currently used	Jeśli została wybrana opcja dynamicznego przydzielania adresu IP przez DHCP, w tym miejscu wyświetla się nazwa aktualnie zastosowanego hosta.
Configured	Tu wpisuje się nazwę hosta produktu, która ma być potem stosowana, gdy interfejs sieciowy zostanie zmieniony na statyczny adres IP lub gdy przez odpowiedź DHCP nie jest podawana nazwa hosta.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**.

Aby zresetować pole edycji, należy kliknąć przycisk **[Clear]**.

Zmiana jest realizowana natychmiast.

Jeśli nazwa hosta zostanie dostarczona za pośrednictwem odpowiedzi DHCP, stanie się ona aktywna w systemie. Przy kilku interfejsach sieciowych z DHCP zawsze obowiązuje ostatnia otrzymana nazwa hosta.

Jeśli ma obowiązywać tylko skonfigurowana tu nazwa hosta, konfiguracja serwera DHCP musi być tak dostosowana, aby w odpowiedzi DHCP nie były wysyłane nazwy hosta.

Grupa „Domain Name“

Tabela 139: Strona WBM „Configuration of Host and Domain Name“ – grupa „Domain Name“

Parametr	Znaczenie
Currently used	Jeśli została wybrana opcja dynamicznego przydzielania adresu IP przez DHCP, w tym miejscu zostaje wyświetlona nazwa aktualnie zastosowanej domeny.
Configured	Tu wpisuje się nazwę domeny produktu, która ma być potem stosowana, gdy interfejs sieciowy zostanie zmieniony na statyczny adres IP lub gdy przez odpowiedź DHCP nie jest podawana nazwa hosta.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**.

Aby zresetować pole edycji, należy kliknąć przycisk **[Clear]**.

Zmiana jest realizowana natychmiast.

Jeśli nazwa domeny zostanie dostarczona za pośrednictwem odpowiedzi DHCP, stanie się ona aktywna w systemie. Przy kilku interfejsach sieciowych z DHCP zawsze obowiązuje ostatnia otrzymana nazwa domeny.

Jeśli ma obowiązywać tylko skonfigurowana tu nazwa domeny, konfiguracja serwera DHCP musi być tak dostosowana, aby w odpowiedzi DHCP nie były wysyłane nazwy domeny.

19.1.1.2.5 Strona „Routing“

Na stronie „Routing“ znajdują się ustawienia i informacje dotyczące routingu między interfejsami sieciowymi.

Grupa „IP Forwarding through multiple interfaces“

Tabela 140: Strona WBM „Routing“ – grupa „IP Forwarding through multiple interfaces“

Parametr	Znaczenie
Enabled	Tu definiuje się, czy dozwolone jest przesyłanie dalej pakietów danych między różnymi interfejsami sieciowymi. Jeśli pole wyboru nie jest zaznaczone, zastosowane zostają ustawienia „Static Routes“, a wtedy pakiety danych IP, docierające do sterownika na jednym interfejsie sieciowym, nie mogą opuścić sterownika na innym interfejsie sieciowym. Jeśli pole wyboru jest zaznaczone, pakiety IP mogą być przesyłane dalej między interfejsami. Wymagane jest wtedy wprowadzenie dalszych ustawień na stronie WBM.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiany są realizowane natychmiast.

Grupa „Default Static Routes“

Dla każdej skonfigurowanej trasy statycznej wyświetlany jest osobny obszar.

Aby zachować kompatybilność z wcześniejszymi wersjami firmware, istnieją zawsze co najmniej dwie możliwości edycji routingu. Nie można ich usunąć; można tylko dezaktywować. Zarówno usunięcie, jak i dezaktywacja powoduje, że trasa nie jest wprowadzona do systemu.

Tabela 141: Strona WBM „Routing“ – grupa „Default Static Routes“

Parametr	Znaczenie	
Enabled	Tu można zdecydować, czy wybrana trasa ma być zastosowana.	
	Disabled	Trasa nie jest zastosowana.
	Enabled	Trasa jest zastosowana.
Destination Address	Tu definiuje się, czy dostępni mają być dowolni uczestnicy komunikacji sieciowej, czy też tylko określone urządzenie lub urządzenie z danej puli adresów.	
	Default	Dostępni są dowolni uczestnicy komunikacji sieciowej.
	Network address	Dostępne jest tylko określone urządzenie lub urządzenie z danej puli adresów.
Destination Mask	Tu wpisuje się maskę podsieci urządzenia. Jeśli Destination Address jest zdefiniowany jako „default“, należy tu wpisać wartość „0.0.0.0“.	
Gateway Address	Tu ustawia się adres bramy.	
Gateway Metric	Tu ustawia się liczbę, będącą metryką. Przy kilku trasach o tym samym adresie docelowym (Destination Address) i masce (Destination Mask) to metryka decyduje, do której bramy w pierwszej kolejności wysyłane są pakiety danych. Preferowane są trasy z niższą metryką. Standardowa wartość metryki wynosi 20. Najmniejsza wartość wynosi 0. Największa wartość to $2^{32}-1 = 4.294.967.295$.	

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiany są realizowane natychmiast.

Aby dodać nową trasę, należy kliknąć przycisk **[Add]**. Zmiana jest realizowana natychmiast.

Aby usunąć istniejącą trasę, należy kliknąć przycisk **[Delete]**. Zmiana jest realizowana natychmiast.

Grupa „Dynamic Routes“

Tu wyświetlane są wszystkie domyślne bramy otrzymane przez DHCP. Bramy domyślne, konfigurowane przez DHCP, otrzymują metrykę 10, dzięki czemu są zazwyczaj wykorzystywane przed domyślnymi bramami skonfigurowanymi statycznie.

Dla każdej trasy dynamicznej wyświetlany jest osobny obszar. Jeśli poprzez DHCP nie została odebrana żadna trasa dynamiczna, wyświetlany jest komunikat „(no dynamic route)”.

Grupa „IP-Masquerading“

Dla każdego parametru wyświetlany jest osobny obszar.

Tabela 142: Strona WBM „Routing“ – grupa „IP-Masquerading“

Parametr	Znaczenie	
Enabled	Tu można zdecydować, czy ma być zastosowany IP-Masquerading	
	Disabled	IP-Masquerading nie jest zastosowany.
	Enabled	IP-Masquerading jest zastosowany.
Interface	Tu można wybrać jedną z proponowanych nazw dla interfejsu sieciowego. Wybierając „other“ można alternatywnie wpisać dowolną nazwę interfejsu sieciowego.	

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiany są realizowane natychmiast.

Aby dodać nową pozycję, należy kliknąć przycisk **[Add]**. Zmiana jest realizowana natychmiast.

Aby usunąć daną pozycję, kliknąć przycisk **[Delete]**. Zmiana jest realizowana natychmiast.

Pozycja zostaje wprowadzona do systemu tylko wtedy, gdy zaznaczona jest opcja „Enable“ w grupie „General Routing Configuration“. W ten sposób można wprowadzić wstępnie dane ustawienie, które zostanie przejęte dopiero w momencie generalnego załączenia.

Grupa „Port Forwarding“

Dla każdego parametru wyświetlany jest osobny obszar.

Tabela 143: Strona WBM „Routing“ – grupa „Port Forwarding“

Parametr	Znaczenie	
Enabled	Tu można zdecydować, czy ma być zastosowany Port Forwarding.	
	Disabled	Port Forwarding nie jest zastosowany.
	Enabled	Port Forwarding jest zastosowany.
Interface	Tu można wybrać jedną z proponowanych nazw dla interfejsu sieciowego. Wybierając „other“ można alternatywnie wpisać dowolną nazwę interfejsu sieciowego.	
Port	Tu wpisuje się port, po którym przesyłane pakiety danych mają dotrzeć do produktu.	
Protocol	Tu można wybrać protokół, który ma być uwzględniony dla Port Forwarding. Do wyboru są protokoły TCP, UDP lub oba.	
Destination Address	Tu ustawia się adres sieciowy urządzenia docelowego. Adres ten zastępuje pierwotny adres docelowy pakietu danych.	
Destination Port	Tu ustawia się numer portu urządzenia docelowego. Wartość ta zastępuje pierwotny port docelowy pakietu danych.	

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiany są realizowane natychmiast.

Aby dodać nową pozycję, należy kliknąć przycisk **[Add]**. Zmiana jest realizowana natychmiast.

Aby usunąć daną pozycję, kliknąć przycisk **[Delete]**. Zmiana jest realizowana natychmiast.

Pozycja zostaje wprowadzona do systemu tylko wtedy, gdy zaznaczona jest opcja „Enable“ w grupie „General Routing Configuration“. W ten sposób można wprowadzić wstępnie dane ustawienie, które zostanie przejęte dopiero w momencie generalnego załączenia.

19.1.1.2.6 Strona „Clock Settings“

Na stronie „Clock Setting“ znajdują się ustawienia daty i godziny.

Grupa „Timezone and Format“

Tabela 144: Strona „Clock Setting“ – grupa „Timezone and Format“

Parametr	Znaczenie
Timezone	Tu wybiera się strefę czasową odpowiednią dla danego kraju. Ustawienie podstawowe:
	AST/ADT „Atlantic Standard Time“, Halifax
	EST/EDT „Eastern Standard Time“, New York, Toronto
	CST/CDT „Central Standard Time“, Chicago, Winnipeg
	MST/MDT „Mountain Standard Time“, Denver, Edmonton
	PST/PDT „Pacific Standard Time“, Los Angeles, Whitehouse
	GMT/BST „Greenwich Mean Time“, GB, P, IRL, IS, ...
	CET/CEST „Central European Time“, B, DK, D, F, I, CRO, NL, ...
	EET/EEST „East European Time“, BUL, FI, GR, TR, ...
	CST „China Standard Time“
	JST „Japan/Korea Standard Time“
TZ String	W przypadku strefy czasowej, która nie została uwzględniona w parametrach „Time Zone“ wpisuje się nazwę danej strefy czasowej lub kraj i miasto, które się w niej znajdują. Oficjalną nazwę strefy czasowej można znaleźć na stronie: http://www.timeanddate.com/time/map/
Time Format	Przełączanie między zegarem 12- i 24-godzinnym

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Grupa „UTC Time and Date“

Tabela 145: Strona WBM „Clock Settings“ – grupa „UTC Time and Date“

Parametr	Znaczenie
UTC Date	Tu ustawia się datę.
UTC Time	Tu ustawia się czas uniwersalny (GMT).

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Grupa „Local Time and Date“

Tabela 146: Strona WBM „Clock Settings“ – grupa „Local Time and Date“

Parametr	Znaczenie
Local Date	Tu ustawia się datę.
Local Time	Tu ustawia się lokalny czas.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

19.1.1.2.7 Strona „Configuration of Service Interface“

Na stronie „Configuration of Service Interface“ znajdują się ustawienia dla złącza serwisowego.

Grupa „Service Interface assigned to“

Wyświetlana jest tu aplikacja, do której przypisane jest aktualnie złącze serwisowe.

Grupa „Assign Owner of Service Interface“

Tu można wybrać aplikację, której przypisane zostało złącze serwisowe po kolejnym restarcie sterownika.

Tabela 147: Strona WBM „Configuration of Service Interface” – grupa „Assign Owner of Service Interface“

Parametr	Znaczenie
WAGO Service Communication	Tu deklaruje się, że złącze serwisowe wykorzystywane jest do komunikacji serwisowej WAGO lub komunikacji z systemem runtime.
Linux Console	Tu przypisuje się złącze serwisowe do konsoli Linux®.
Unassigned (usage by Applications, Libraries, CODESYS)	Tu deklaruje się, że złącze serwisowe nie jest przypisane do żadnej aplikacji i jest wolne, a więc można na przykład wykorzystać je w celu umożliwienia dostępu dla programu CODESYS przez bloki funkcyjne.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana zostanie zrealizowana dopiero po następnym restarcie sterownika. W tym celu należy skorzystać z funkcji Reboot WBM. Nie wyłączać sterownika zbyt wcześnie!

19.1.1.2.8 Strona „Create bootable Image“

Na stronie „Create bootable Image“ można tworzyć obraz dla projektów bootowalnych.

Grupa „Create bootable image from boot device“

Po ustaleniu i określeniu możliwego celu, jest on najpierw sprawdzany, a wynik zostaje wyświetlony pod ustawieniami.

Tabela 148: Strona WBM „Create bootable Image” – grupa „Create bootable image from boot device“

Parametr	Znaczenie		
Boot Device	Tu wyświetlany jest nośnik, z którego przeprowadzony był rozruch.		
Destination	W zależności od tego, z którego nośnika przeprowadzony był rozruch, po procesie bootowania można wybrać następujący cel dla utworzonego obrazu:		
	System bootowany z		docelowa partycja dla „bootable Image“
	karta pamięci	→	Internal Flash
	Pamięć wewnętrzna	→	Memory Card

- Wolna pamięć na urządzeniu docelowym:
Jeśli wolne miejsce w pamięci wynosi mniej niż 5%, wysyłane jest odpowiednie ostrzeżenie. Mimo to można rozpocząć kopiowanie. Jeśli wolnego miejsca jest zdecydowanie za mało, wysyłany jest odpowiedni komunikat, a proces kopiowania nie może się rozpocząć.
- Device w użyciu przez CODESYS:
Jeśli urządzenie jest używane przez CODESYS, wysyłany jest odpowiedni komunikat. Mimo to można rozpocząć kopiowanie, jednak nie jest to zalecane!

Aby rozpocząć kopiowanie, należy kliknąć przycisk **[Start Copy]**. Po pozytywnym wyniku testu proces rozpoczyna się od razu. Jeśli zostały wykryte błędy, wyświetlany jest odpowiedni komunikat i proces nie jest realizowany. W przypadku wystąpienia jakiegokolwiek ostrzeżenia zostaną one wyświetlone ponownie i wymagane będzie potwierdzenie, że można kontynuować proces.

19.1.1.2.9 Strona „Firmware Backup“

Na stronie „Firmware Backup“ znajdują się ustawienia dotyczące zabezpieczenia danych sterownika.

Grupa „Firmware Backup“

Tabela 149: Strona WBM „Firmware Backup“ – grupa „Firmware Backup“

Parametr	Znaczenie	
Boot Device	Tu wyświetlany jest nośnik pamięci, z którego przeprowadzony był rozruch.	
Destination	Tu wybiera się miejsce zapisu dla backupu.	
	Memory Card	Dane zostają zapisane na karcie pamięci. Ta możliwość wyboru widoczna jest tylko po włożeniu karty pamięci, z której nie był przeprowadzony rozruch.
	Network	Dane zapisywane są w systemie plików i udostępniane na PC do pobrania.
PLC Runtime Project	To pole wyboru należy zaznaczyć, gdy chce się zapisać projekt runtime PLC.	
Settings	To pole wyboru należy zaznaczyć, gdy chce się zapisać ustawienia urządzenia.	
System	To pole wyboru należy zaznaczyć, gdy chce się zapisać system operacyjny urządzenia.	
Encryption	To pole należy zaznaczyć, gdy chce się zapisać zaszyfrowane dane.	
Encryption passphrase	Tu wpisuje się hasło szyfrowania. Pole edycji widoczne jest tylko wtedy, gdy zaznaczone jest pole wyboru Encryption.	
Confirm passphrase	Tu ponownie wpisuje się hasło szyfrowania w celu potwierdzenia. Pole edycji widoczne jest tylko wtedy, gdy zaznaczone jest pole wyboru Encryption.	

Wskazówka Uwzględnić wersję firmware!



Przywrócenie systemu operacyjnego sterownika (opcja „System”) jest dopuszczalne i możliwe tylko wtedy, gdy wersje firmware w czasie tworzenia kopii zapasowej i przywracania są identyczne.
W razie potrzeby należy pominąć przywracanie systemu operacyjnego sterownika lub dopasować wcześniej uprzednio wersję firmware sterownika do wersji firmware w momencie tworzenia kopii zapasowej.

-
Wskazówka	Do sieci można skopiować tylko jeden package!
	Jeśli jako miejsce docelowe ustawiona jest opcja „Network“, dla każdego procesu zapisu można wybrać tylko jeden package.
-
Wskazówka	Brak funkcji „Backup“ dla karty pamięci!
	Nie ma możliwości utworzenia kopii zapasowej karty pamięci w wewnętrznej pamięci flash.
-
Wskazówka	Uwzględnić czas backupu
	Tworzenie plików backup może potrwać kilka minut. Aby skrócić ten czas, należy przed rozpoczęciem tworzenia kopii zapasowych zatrzymać program CODESYS.
-

Aby rozpocząć proces backupu, należy kliknąć przycisk **[Create Backup]**.

19.1.1.2.10 Strona „Firmware Restore“

Na stronie „Firmware Restore“ znajdują się ustawienia do przywracania firmware.

Grupa „Firmware Restore“

Tabela 150: Strona WBM „Firmware Restore“ – grupa „Firmware Restore“

Parametr	Znaczenie
Source	W tym miejscu należy wybrać źródło danych do przywrócenia.
	Memory Card Dane zostają odczytane z karty pamięci. Ta możliwość wyboru widoczna jest tylko po włożeniu karty pamięci, z której nie był przeprowadzony rozruch.
	Network Dane do przywrócenia zostaną pobrane z PC.
Boot Device	Tu wyświetlany jest nośnik pamięci, z którego przeprowadzony był rozruch.
PLC Runtime Project	Tu wpisuje się nazwę pliku archiwalnego projektu CODESYS. Pole edycji jest aktywne tylko wtedy, gdy jako źródło danych wybrana jest sieć.
Settings	Tu wpisuje się nazwę pliku archiwalnego dla ustawień. Pole edycji jest aktywne tylko wtedy, gdy jako źródło danych wybrana jest sieć.
System	Tu wpisuje się nazwę pliku archiwalnego dla danych systemowych. Pole edycji jest aktywne tylko wtedy, gdy jako źródło danych wybrana jest sieć.
Decryption	To pole wyboru należy zaznaczyć, gdy chce się zapisać zaszyfrowane dane.
Decryption passphrase	Tu wpisuje się hasło szyfrowania. Pole edycji widoczne jest tylko wtedy, gdy zaznaczone zostało pole wyboru Decryption.

Wskazówka Uwzględnić wersję firmware!



Przywrócenie systemu operacyjnego sterownika (opcja „System”) jest dopuszczalne i możliwe tylko wtedy, gdy wersje firmware w czasie tworzenia kopii zapasowej i przywracania są identyczne.
W razie potrzeby należy pominąć przywracanie systemu operacyjnego sterownika lub dopasować wcześniej uprzednio wersję firmware sterownika do wersji firmware w momencie tworzenia kopii zapasowej.

Wskazówka	Przywracanie możliwe tylko z wewnętrznej pamięci! Jeśli urządzenie było bootowane z karty pamięci, przywrócenie firmware nie jest możliwe.
	
Wskazówka	Reset przez przywracanie Reset można wykonać przez przywrócenie systemu, ustawień lub CODESYS!
	
Wskazówka	Utrata połączenia w wyniku przywracania Jeśli przy przywracaniu zmieniają się parametry połączenia ETHERNET, WBM nie będzie mógł nawiązać połączenia z urządzeniem. Trzeba wtedy ponownie otworzyć WBM, wpisując w pasku adresu poprawny adres IP urządzenia.
	

Aby rozpocząć proces przywracania, należy kliknąć przycisk **[Restore]**.

19.1.1.2.11 Strona „Active System“

Na stronie „Active System“ znajdują się ustawienia do wyboru partycji, z której ma być uruchamiany system.

Grupa „Boot Device“

Tabela 151: Strona WBM „Active System“ – grupa "Boot Device"

Parametr	Znaczenie
Boot Device	Tu wyświetlany jest nośnik pamięci, z którego przeprowadzony był rozruch.

Grupy „System <n> (Internal Flash)“

Tabela 152: Strona WBM „Active System“ – grupa „System <n> (Internal Flash)“

Parametr	Znaczenie	
Active	Tu wyświetlana jest informacja, czy system jest aktywny.	
Configured	Tu wyświetlana jest informacja, czy po następnym procesie Reboot system ma być aktywny.	
State	Tu wyświetlany jest status systemu.	
	good	System jest aktualny i może zostać użyty.
	bad	System nie jest aktualny i nie może być użyty.

Aby przy następnym procesie Reboot ponownie uruchomić żądany system, należy kliknąć odpowiedni przycisk **[Activate]**.

Wskazówka



Przygotować system bootowalny!

W systemie bootowalnym musi istnieć backup firmware!

19.1.1.2.12 Strona „Mass Storage“

Na stronie „Mass Storage“ znajdują się ustawienia i informacje dotyczące nośników pamięci.

Nagłówek grupy zawiera nazwę nośnika pamięci („Memory Card“ lub „Internal Flash“), a jeśli ta pamięć jest aktywną partycją, także tekst „Active Partition“.

Grupa „Devices“

Dla każdego znalezionej nośnika pamięci wyświetlany jest obszar z informacjami o tym nośniku.

Tabela 153: Strona WBM „Mass Storage“ – grupa „Devices“

Parametr	Znaczenie
<Device>	Tu wyświetlany jest nośnik pamięci.
Boot device	Tu wyświetlana jest informacja, czy z tego nośnika pamięci przeprowadzony był rozruch.
Volume name	Tu wyświetlana jest nazwa pamięci.

Grupa „Create new Filesystem on Memory Card“

Tabela 154: Strona WBM „Mass Storage“ – grupa „Create new Filesystem on Memory Card“

Parametr	Znaczenie
Filesystem type	Tu wybiera się format, w którym tworzy się nowy system danych na karcie pamięci.
	Ext4 System danych tworzony jest w formacie Ext4. Danych nie można odczytać w systemie Windows!
	FAT System danych tworzony jest w formacie FAT.
Etykieta	Tu wpisuje się nazwę, jaką ma otrzymać nośnik pamięci przy formatowaniu.

Wskazówka Dane zostaną usunięte!



Przy formatowaniu dane zapisane na nośniku pamięci są usuwane!

Aby sformatować dany nośnik pamięci, należy kliknąć **[Start Formatting]**.

19.1.1.2.13 Strona „Software Uploads“

Na stronie „Software Uploads“ można zainstalować na produkcie pakiety oprogramowania pobrane z komputera.

Tabela 155: Strona WBM „Software Uploads“ – grupa „Upload new Software“

Parametr	Znaczenie
Software file	Tu pojawia się nazwa pliku wybranego pakietu oprogramowania, dopóki nie zostanie on przesłany do produktu. Jeśli pakiet nie został jeszcze wybrany, pojawia się tekst „Choose ipk file...“. W tym celu należy kliknąć pole edycji i wybrać na komputerze plik z pakietem.

Aby zainstalować pakiet, należy kliknąć przycisk **[Install]**.

Po zainstalowaniu plik z pakietem oprogramowania zostaje usunięty z urządzenia. Jeśli nie jest to możliwe na skutek błędu w trakcie przetwarzania, usunięcie nastąpi najpóźniej przy kolejnym restarcie produktu.

19.1.1.2.14 Strona „Configuration of Network Services“

Na stronie „Configuration of Network Services“ znajdują się ustawienia dla różnego typu usług.

Wskazówka



Zamknąć nieużywane porty i usługi!

Przez otwarte porty i usługi osoby nieuprawnione mogą uzyskać dostęp do systemu automatyki.

Aby zredukować niebezpieczeństwo cyberataku, należy zamykać wszystkie porty i usługi w komponentach systemu sterowania, które nie są wykorzystywane przez aplikację (np. port 6626 dla WAGO-I/O-CHECK, port 2455 dla CODESYS V2 i port 11740 dla **e!COCKPIT**).

Porty i usługi dobrze jest otwierać tylko na czas uruchamiania lub konfiguracji.

Grupa „Telnet“

Tabela 156: Strona WBM „Configuration of Network Services“ – grupa „Telnet“

Parametr	Znaczenie
Telnet	Tu można aktywować/dezaktywować serwis Telnet. W ustawieniach fabrycznych ta usługa nie jest aktywna.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Grupa „FTP“

Tabela 157: Strona WBM „Configuration of Network Services“ – grupa „FTP“

Parametr	Znaczenie
FTP	Tu można aktywować/dezaktywować serwis FTP. W ustawieniach fabrycznych ta usługa nie jest aktywna.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Grupa „FTPS“

Tabela 158: Strona WBM „Configuration of Network Services“ – grupa „FTPS“

Parametr	Znaczenie
FTPS	Tu można aktywować/dezaktywować serwis FTPS. W ustawieniach fabrycznych ta usługa nie jest aktywna.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Grupa „HTTP“

Tabela 159: Strona WBM „Configuration of Network Services“ – grupa „HTTP“

Parametr	Znaczenie
HTTP	Tu można aktywować/dezaktywować serwis HTTP. W ustawieniach fabrycznych ta usługa nie jest aktywna.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Wskazówka**Utrata połączenia w wyniku dezaktywacji**

Przy dezaktywacji serwisu HTTP połączenie z produktem może zostać przerwane. Należy wtedy ponownie otworzyć stronę.

Grupa „HTTPS“

Tabela 160: Strona WBM „Configuration of Network Services“ – grupa „HTTPS“

Parametr	Znaczenie
HTTPS	Tu można aktywować/dezaktywować serwis HTTPS.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Wskazówka**Utrata połączenia w wyniku dezaktywacji**

Przy dezaktywacji serwisu HTTPS połączenie z produktem może zostać przerwane. Należy wtedy ponownie otworzyć stronę.

Grupa „I/O-CHECK“

Tabela 161: Strona WBM „Configuration of Network Services“ – grupa „I/O-CHECK“

Parametr	Znaczenie
Service active	Tu można aktywować/dezaktywować serwis WAGO-I/O-CHECK.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

19.1.1.2.15 Strona „Configuration of NTP Client“

Na stronie „Configuration of NTP Client“ znajdują się ustawienia dla usługi NTP.

Grupa „NTP Client Configuration“

Tabela 162: Strona WBM „Configuration of NTP Client“ – grupa „NTP Client Configuration“

Parametr	Znaczenie
Service enabled	Tu można aktywować/dezaktywować aktualizację godziny.
Update Interval (sec)	Tu definiuje się interwał czasowy aktualizacji serwera czasu.
Time Server <n>	Tu wpisuje się adresy IP maksymalnie 4 serwerów czasu. Serwer czasu nr 1 odpytywany jest jako pierwszy. Jeśli nie można pobrać z niego danych, odpytywany jest serwer nr 2.
Additionally assigned (DHCP)	Tu wyświetlane są serwery NTP przydzielone przez DHCP (lub BootP). Jeśli nie został przydzielony serwer NTP przez DHCP (lub BootP), wyświetlana jest informacja („no additional servers assigned“).

Aby aktualizować czas niezależnie od interwału, należy kliknąć przycisk **[Update Time]**.

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiany są realizowane natychmiast.

19.1.1.2.16 Strona „PLC Runtime Services“

Na stronie „PLC Runtime Services“ znajdują się ustawienia dla różnego typu usług aktywnego systemu operacyjnego.

Grupa „General Configuration“

Tabela 163: Strona WBM „PLC Runtime Services“ – grupa „General Configuration“

Parametr	Znaczenie
Port Authentication Password	Tu należy podać nowe hasło dla uwierzytelnienia portu.
Confirm Password	Tu należy jeszcze raz podać nowe hasło w celu sprawdzenia.

Aby zastosować zmianę, kliknąć przycisk **[Set Password]**.

Zmiana jest realizowana natychmiast.

Grupa „CODESYS 2“

Grupa ta widoczna jest tylko wtedy, gdy sterownik obsługuje system runtime CODESYS V2.

Tabela 164: Strona WBM „PLC Runtime Services“ – grupa „CODESYS 2“

Parametr	Znaczenie
CODESYS 2 State	Tu wyświetlany jest status systemu runtime CODESYS V2 (enabled/disabled).
Webserver enabled	Tu aktywuje się i dezaktywuje serwer WWW CODESYS V2 dla wizualizacji sieciowej CODESYS.
Communication enabled	Tu aktywuje się i dezaktywuje komunikację między systemem runtime CODESYS V2 i środowiskiem programistycznym CODESYS V2.
Communication Port Number	Tu wpisuje się numer portu do komunikacji ze środowiskiem programistycznym CODESYS V2. Standardowa wartość wynosi 2455.
Port authentication enabled	Tu definiuje się, czy dla portu włączone jest uwierzytelnienie. Jeśli jest włączone (enabled), przy zalogowaniu przez CODESYS V2 należy wpisać hasło podane w „General Configuration“.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**.

Zmiana uwierzytelnienia zostanie zrealizowana po następnym restarcie.

Wszystkie inne zmiany są realizowane natychmiast.

Grupa „*e!RUNTIME*“

Grupa ta widoczna jest tylko wtedy, gdy sterownik obsługuje system runtime *e!RUNTIME*.

Tabela 165: Strona WBM „PLC Runtime Services“ – grupa „*e!RUNTIME*“

Parametr	Znaczenie
<i>e!RUNTIME</i> State	Tu wyświetlany jest status systemu runtime <i>e!RUNTIME</i> (enabled/disabled).
Webserver enabled	Tu aktywuje się i dezaktywuje serwer WWW <i>e!RUNTIME</i> dla wizualizacji sieciowej.
Port authentication enabled	Tu definiuje się, czy dla połączenia z urządzeniem wymagany jest Log-in. Nazwa użytkownika to admin, a hasłem jest hasło podane w „General Configuration“.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**.

Zmiana uwierzytelnienia zostanie zrealizowana po następnym restarcie.

Wszystkie inne zmiany są realizowane natychmiast.

19.1.1.2.17 Strona „SSH Server Settings“

Na stronie „SSH Server Settings“ znajdują się ustawienia dla usługi SSH.

Grupa „SSH Server“

Tabela 166: Strona WBM „SSH Server Settings“ – grupa „SSH Server“

Parametr	Znaczenie
Service active	Tu włączą się i wyłączą serwer SSH.
Port Number	Tu wpisuje się numer portu.
Allow root login	Tu blokuje się lub zezwala na dostęp do katalogu głównego.
Allow password login	Tu aktywuje się i dezaktywuje pytanie o hasło.

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiany są realizowane natychmiast.

19.1.1.2.18 Strona „TFTP Server“

Na stronie „TFTP Server“ znajdują się ustawienia dla usługi TFTP.

Grupa „TFTP Server“

Tabela 167: Strona WBM „TFTP Server“ – grupa „TFTP Server“

Parametr	Znaczenie
Service active	Tu aktywuje się i dezaktywuje serwer TFTP.
Download directory	Tu wpisuje się ścieżkę do katalogu download serwera.

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiany są realizowane natychmiast.

19.1.1.2.19 Strona „DHCP Server Configuration“

Na stronie „DHCP Server Configuration“ znajdują się ustawienia dla usługi DHCP.

Grupa „DHCP Server Configuration Bridge <n>“

Tabela 168: Strona WBM „DHCP Server Configuration“ – grupa „DHCP Configuration Bridge <n>“

Parametr	Znaczenie
Service active	Tu włączą się i wyłączą usługę DHCP dla interfejsu X<n>.
Start IP for Range	Tu należy wpisać wartość początkową dostępnego zakresu adresów IP.
End IP for Range	Tu należy wpisać wartość końcową dostępnego zakresu adresów IP.
Lease time (min)	Tu wpisuje się czas dzierżawy w minutach. Jako wartość standardowa wpisane jest 120 minut.
Static Hosts	Tu wyświetlane są statyczne przyporządkowania adresów MAC do adresów IP. Jeśli przyporządkowanie nie zostało zdefiniowane, wyświetlana jest informacja „No static hosts configured“.
Add Static Host	Następnie można dodać statyczne adresy MAC lub nazwy hosta i adresy IP.
MAC Address or Hostname	Tu wpisuje się nowe przyporządkowanie statyczne, np. „01:02:03:04:05:06=192.168.1.20“ lub „hostname=192.168.1.20“. Można wpisać 10 przyporządkowań lub nazw hosta.
addIp Address	Tu wpisuje się adresy IP, Można wpisać 10 adresów IP.

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiany są realizowane natychmiast.

Aby zastosować nowe przyporządkowanie, kliknąć przycisk **[Add]**. Zmiana jest realizowana natychmiast.

Aby usunąć istniejące przyporządkowanie, należy kliknąć przycisk **[Delete]**. Zmiana jest realizowana natychmiast.

19.1.1.2.20 Strona „Configuration of DNS Server“

Na stronie „Configuration of DNS Server“ znajdują się ustawienia dla usługi DNS.

Grupa „DNS Server“

Tabela 169: Strona WBM „Configuration of DNS Server“ – grupa „DNS Server“

Parametr	Znaczenie	
Service active	Tu włączają się i wyłączają usługę serwera DNS.	
Mode	Tu wybiera się typ pracy serwera DNS.	
	Proxy	Zapytania buforowane są w celu optymalizacji przepustowości komunikacji.
	Relay	Wszystkie zapytania są przesyłane bezpośrednio dalej.
Static Hosts	Tu wyświetlane są statyczne przyporządkowania nazw do adresów IP. Jeśli przyporządkowanie nie zostało zdefiniowane, wyświetlana jest informacja „No static hosts configured“.	
Add Static Host	Następnie można dodać statyczne adresy IP i nazwy hosta.	
IP Address	Tu wpisuje się nowe stałe przyporządkowanie, np. „192.168.1.20:hostname“. Można wpisać 10 przyporządkowań.	
Host name	Tu wpisuje się nazwę hosta.	

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiany są realizowane natychmiast.

Aby zastosować nowe przyporządkowanie, kliknąć przycisk **[Add]**. Zmiana jest realizowana natychmiast.

Aby usunąć istniejące przyporządkowanie, należy kliknąć przycisk **[Delete]**. Zmiana jest realizowana natychmiast.

19.1.1.2.21 Strona „Status overview“

Na stronie „Status overview“ znajdują się informacje dotyczące dostępu do chmury.

Grupa „Service“

Tabela 170: Strona WBM „Overview“ – grupa „Service“

Parametr	Znaczenie
Version	Tu wyświetlana jest wersja wtyczki Cloud.

Grupa „Connection <n>“

Dla każdego dostępu do chmury wyświetlana jest osobna grupa.

Tabela 171: Strona WBM „Overview“ – grupa „Connection <n>“

Parametr	Znaczenie
Operation	Tu wyświetlany jest status aplikacji z połączeniem z chmurą.
Data from PLC Runtime	Tu wyświetlana jest informacja, ile kolekcji danych (Data-Collections) ze strony aplikacji IEC zostało zarejestrowanych do transmisji do chmury.
Cloud Connection	Tu wyświetlany jest status połączenia z chmurą.
Heartbeat	Tu wyświetlany jest aktualnie skonfigurowany interwał heartbeat mierzony w sekundach.
Telemetry data transmission	Tu wyświetlana jest informacja, czy transmisja danych jest aktywna, czy nieaktywna.
Cache fill level (QoS 1 and 2)	Tu wyświetlany jest stan zapełnienia pamięci dla wiadomości wychodzących, wyrażony w procentach.

19.1.1.2.22 Strona „Configuration of Connection <n>“

Na stronie „Configuration of Connection <n>“ znajdują się ustawienia i informacje dotyczące dostępu do chmury.

Dla każdego dostępu do chmury wyświetlana jest osobna strona.

Grupa „Configuration“

Wyświetlone parametry są zależne od ustawionej platformy chmury i ewentualnie od innych ustawień w tej grupie.

Te zależności są przedstawione w osobnej tabeli.

Tabela 172: Strona WBM „Configuration of Connection <n>“ – grupa „Configuration“

Parametr	Znaczenie
Enabled	Tu aktywuje się i dezaktywuje funkcję Cloud Connectivity.
Cloud platform	Tu wybiera się platformę chmury.
Host name	Tu wpisuje się nazwę hosta lub adres IP dla wybranej platformy chmury.
Port number	Tu wpisuje się port, do którego ma być utworzone połączenie. Typowe wartości to 8883 dla połączeń szyfrowanych i 1883 dla połączeń nieszyfrowanych.
Device ID	Tu wpisuje się Device ID dla wybranej platformy chmury.
Client ID	Tu wpisuje się Client ID dla wybranej platformy chmury.
Authentication	Tu wybiera się metodę uwierzytelnienia. Możliwe ustawienia to „Shared Key Acces“ lub „X.509 Certificate“.
Activation Key	Tu wpisuje się kod aktywacji dla wybranej platformy chmury.
Clean Session	Tu deklaruje się, czy Clean Session ma być aktywna przy połączeniu z usługą chmury. Jeśli Clean Session jest aktywna, informacje i wiadomości dotyczące tego połączenia z usługą chmury nie są zapisywane.
TLS	Tu można zdecydować, czy dla połączenia z platformą chmury ma być zastosowane kodowanie TLS. Amazon Web Services (AWS) stosuje zawsze TLS.
CA file	Tu podaje się ścieżkę do pliku zakodowanego w formacie PEM, który zawiera stosowny i wiarygodny certyfikat CA potwierdzający tworzenie zakodowanych połączeń. Standardowo jest nim zainstalowany już w sterowniku certyfikat CA /etc/ssl/certs/ca-certificates.crt.

Tabela 172: Strona WBM „Configuration of Connection <n>” – grupa „Configuration”

Parametr	Znaczenie
User	Tu wpisuje się nazwę użytkownika dla uwierzytelnienia usługi chmury.
Password	Tu wpisuje się hasło dla uwierzytelnienia usługi chmury.
Certification file	Tu wpisuje się ścieżkę do pliku zakodowanego w formacie PEM, wykorzystywanego do uwierzytelnienia usługi chmury.
Key file	Tu wpisuje się ścieżkę do pliku zakodowanego w formacie PEM, który zawiera prywatny kod do uwierzytelnienia usługi chmury.
Use websockets	Tu można zdecydować, czy połączenie z platformą chmury ma być nawiązane poprzez protokół WebSocket przez port 443. Gdy pole wyboru nie jest zaznaczone, połączenie z platformą chmury zostaje nawiązane poprzez protokół MQTT przez port 8883.
Use compression	Tu można zdecydować, czy dane mają być skompresowane za pomocą programu GZIP.
Data Protocol	Tu wybiera się protokół danych.
Cache mode	Tu definiuje się, w której pamięci ma być założona pamięć podręczna (cache) dla telegramów danych. To pole wyboru jest aktywne tylko wtedy, gdy wetknięta jest prawidłowo sformatowana karta SD. (Więcej informacji można znaleźć w instrukcji A500920.)
Last Will	Tu definiuje się, czy wiadomość Last Will ma być aktywowana/dezaktywowana.
(Last Will) Topic	Tu wpisuje się temat dla wysyłanej wiadomości Last Will.
(Last Will) Message	Tu wpisuje się treść, która ma być wysłana jako wiadomość Last Will.
(Last Will) QoS	Tu podaje się „Quality of Service” (QoS) wiadomości Last Will.
(Last Will) Retain	Tu definiuje się, czy ostatnia wysłana z danym tematem wiadomość Last Will ma być potraktowana przez brokera jako wiadomość zapisana (Retained Message).
Device info	Tu definiuje się, czy generowana jest wiadomość Device Info, informująca usługę chmury o podstawowej konfiguracji sterownika. (Więcej informacji można znaleźć w instrukcji A500920.)

Tabela 172: Strona WBM „Configuration of Connection <n>” – grupa „Configuration“

Parametr	Znaczenie
Device status	Tu definiuje się, czy ma być generowana wiadomość Device State, informująca usługę chmury o zmianach przełącznika trybu pracy i wskaźników LED. (Więcej informacji można znaleźć w instrukcji A500920.)
Standard commands	W tym miejscu można ustawić, czy mają być obsługiwane zintegrowane standardowe polecenia. (Listę standardowych poleceń można znaleźć w instrukcji A500920.) Jeśli pole wyboru nie jest zaznaczone, obsługiwane są tylko polecenia zdefiniowane w programie IEC.
Application property template	Tu można utworzyć własność dla poszczególnych wiadomości MQTT do chmury Azure. Ten parametr jest opcjonalny, tzn. gdy pole pozostawione jest puste, ta własność nie jest wysyłana. Przy tworzeniu tej własności są do dyspozycji następujące komponenty: • <m>: Message type • <p>: Protocol version • <d>: Device ID Przykłady: • MyKey=HelloWorld_<m> • TestKey=<m>/<p>/<d> • DeviceId=<d>

Aby zastosować zmianę, kliknąć przycisk **[Submit]**.

Zmiany zostaną zrealizowane dopiero po następnym restarcie sterownika.
W tym celu należy skorzystać z funkcji Reboot WBM. Nie wyłączać sterownika zbyt wcześnie!

Poniższa tabela pokazuje zależność pól wyboru i edycji dla wybranej platformy chmury.

Tabela 173: Zależność pól wyboru i edycji dla platformy chmury

Selection or Input Field	Cloud Platform						Authen- tication		Data Protocol				Last Will
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services	Shared Access Key	X.509 Certificate	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B	
Enabled	X	X	X	X	X	X							
Cloud platform	X	X	X	X	X	X							
Host name	X	X	X	X	X	X							
Port number			X	X	(X)	X							
Device ID	X	X											
Client ID			>	>	>	X			X	X	X		
Authentication		X											
Activation Key	X	>					X						
Clean Session			X	(X)	(X)	X							
TLS			X	X	(X)	X							
CA file			X	X	X	X							
User			X	X									
Password			X	X									
Certification file		>	X		X	X		X					
Key file		>	X		X	X		X					
Use websockets	X	X											
Use compression	X	X	>						X	X	X		
Data Protocol			X	X	X	(X)							
• WAGO Protocol			X	X	X								
• WAGO Protocol 1.5			X	X	X								
• Native MQTT			X	X	X	(X)							
• Sparkplug payload B			X		X								
Cache mode	X	X	X	X	X	X							
Last Will			X	X	X	X							
• Last Will Topic			>	>	>	>							X
• Last Will Message			>	>	>	>							X
• Last Will QoS			>	>	>	>							X
• Last Will Retain			>	>	(>)	>							X

Tabela 173: Zależność pól wyboru i edycji dla platformy chmury

Selection or Input Field	Cloud Platform						Authen- tication		Data Protocol				Last Will
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services	Shared Access Key	X.509 Certificate	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B	
Device info		X	>	>	>				X	X			
Device status		X	>	>	>				X	X			
Standard commands		X	>		>				X	X			
Application property template		X											

X: Widoczne i aktywne

(X): Widoczne, ale nieaktywne

>: Widoczne i aktywne, zależnie od innych ustawień

(>): Widoczne, ale nieaktywne, zależnie od innych ustawień

19.1.1.2.23 Strona „Configuration of general SNMP parameters“

Na stronie „Configuration of general SNMP parameters“ znajdują się ogólne ustawienia dla SNMP.

Grupa „General SNMP Configuration“

Tabela 174: Strona WBM „Configuration of general SNMP parameter“ – grupa „General SNMP Configuration“

Parametr	Znaczenie
Service active	Tu można aktywować/dezaktywować serwis SNMP.
Name of device	Tu wpisuje się nazwę urządzenia (sysName).
Description	Tu wpisuje się opis urządzenia (sysDescription).
Physical location	Tu wpisuje się lokalizację urządzenia (sysLocation).
Contact	Tu wpisuje się adres kontaktowy e-mail (sysContact).
ObjectID	Tu wpisuje się Object-ID.

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiany zostaną zrealizowane dopiero po następnym restarcie sterownika. W tym celu należy skorzystać z funkcji Reboot WBM. Nie wyłączać sterownika zbyt wcześnie!

19.1.1.2.24 Strona „Configuration of SNMP v1/v2c parameters“

Na stronie „Configuration of SNMP v1/v2c parameters“ znajdują się ustawienia dla SNMP v1/v2c.

Grupa „SNMP v1/v2c Manager Configuration“

Tabela 175: Strona WBM „Configuration of SNMP v1/v2c parameters“ – grupa „SNMP v1/v2c Manager Configuration“

Parametr	Znaczenie
Protocol enabled	Tu wyświetlana jest informacja, czy jest aktywowany protokół SNMP dla v1/v2c. Przy nieaktywnym protokole również Local Community Name zostaje usunięta.
Local Community Name	Tu wpisuje się nazwę Community do konfiguracji managera SNMP. Przez nazwę Community można tworzyć powiązania między managerami i agentami SNMP, którzy określani są jako Community i sterują identyfikacją oraz dostępem między urządzeniami SNMP. Nazwa Community może liczyć maksymalnie 32 znaki i nie może zawierać spacji. Aby móc zastosować protokół SNMP, musi być podana aktualna nazwa Community. Standardem jest „public“.

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiany zostaną zrealizowane dopiero po następnym restarcie sterownika. W tym celu należy skorzystać z funkcji Reboot WBM. Nie wyłączać sterownika zbyt wcześnie!

Grupa „Actually configured Trap Receivers“

Tabela 176: Strona WBM „Configuration of SNMP v1/v2c parameters“ – grupa „Actually configured Trap Receivers“

Parametr	Znaczenie
	Dla każdego skonfigurowanego odbiorcy komunikatów trap wyświetlany jest osobny obszar. Jeśli odbiorca komunikatów trap nie został skonfigurowany, wyświetlana jest informacja „(no trap receivers configured)“.
IP Address	Tu wyświetlany jest adres IP odbiorcy komunikatów trap (Managementstation).
Community Name	Tu wyświetlana jest nazwa Community do konfiguracji odbiorcy komunikatów trap. Nazwa Community może być weryfikowana przez odbiorcę komunikatów trap.
Version	Tu wyświetlana jest wersja SNMP, przez którą powinny być wysyłane komunikaty trap: v1 lub v2c (komunikaty trap przez v3 wyświetlane są w osobnym formularzu).
Add new Trap Receiver	W tym obszarze można wpisać nowego odbiorcę komunikatów trap.
IP Address	Tu wpisuje się adres IP nowego odbiorcy komunikatów trap (Managementstation).
Community Name	Tu wpisuje się nazwę Community do nowej konfiguracji odbiorcy komunikatów trap. Nazwa Community może być weryfikowana przez odbiorcę komunikatów trap. Nazwa Community może liczyć maksymalnie 32 znaki i nie może zawierać spacji.
Version	Tu wybiera się wersję SNMP, przez którą powinny być wysyłane komunikaty trap: v1 lub v2c (komunikaty trap przez v3 konfigurowane są w osobnym formularzu).

Aby usunąć istniejącego odbiorcę komunikatów trap, należy kliknąć odpowiedni przycisk **[Delete]**.

Aby dodać nowego odbiorcę komunikatów trap, należy kliknąć przycisk **[Add]**.

Zmiany zostaną zrealizowane dopiero po następnym restarcie sterownika. W tym celu należy skorzystać z funkcji Reboot WBM. Nie wyłączać sterownika zbyt wcześnie!

19.1.1.2.25 Strona „Configuration of SNMP v3 Users“

Na stronie „Configuration of SNMP v3 Users“ znajdują się ustawienia dla SNMP v3.

Grupa „Actually configured v3 Users“

Tabela 177: Strona WBM „Configuration of SNMP v3 Users“ – grupa „Actually configured v3 Users“

Parametr	Znaczenie
User <n>	Dla każdego skonfigurowanego użytkownika v3 wyświetlany jest osobny obszar. Jeśli użytkownik v3 nie został skonfigurowany, wyświetlana jest informacja „(no users configured)“.
Security Authentication Name	Tu wyświetlana jest nazwa użytkownika.
Authentication Type	Tu wyświetlany jest typ uwierzytelnienia dla pakietów SNMP v3. Możliwe wartości to: - Brak uwierzytelnienia („None“) - Message Digest 5 („MD5“) - Secure Hash Algorithm („SHA“)
Authentication Key	Tu wyświetlany jest klucz dla uwierzytelniania.
Privacy	Tu wyświetlany jest algorytm kodowania dla wiadomości SNMP. Możliwe wartości to: - Brak kodowania („None“) - Data Encryption Standard („DES“) - Advanced Encryption Standard („AES“)
Privacy Key	Tu wyświetlany jest klucz do kodowania wiadomości SNMP. Jeśli brak jakiegokolwiek wyświetlenia, automatycznie zastosowany zostaje „Authentication Key“.
Notification Receiver IP	Tu wyświetlany jest adres IP odbiorcy komunikatów trap dla v3. Jeśli dla tego użytkownika nie są wysyłane komunikaty trap w v3, pole jest puste.
Add new v3 User	W tym obszarze można wpisać nowego użytkownika v3. Można wpisać 10 użytkowników.
Security Authentication Name	Tu wpisuje się nazwę użytkownika. Musi ona być unikatowa; już istniejąca nazwa użytkownika nie zostanie zaakceptowana. Nazwa może zawierać min. 8 i maks. 32 znaków, w tym małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9), znaki specjalne !()*~'-._, ale nie może zawierać spacji.
Authentication Type	Tu wpisuje się typ uwierzytelnienia dla pakietów SNMP v3. Możliwe wartości to: - Brak uwierzytelnienia („None“) - Message Digest 5 („MD5“) - Secure Hash Algorithm („SHA“)

Authentication Key (min. 8 char.)	Tu należy podać klucz dla uwierzytelnienia. Klucz może zawierać min. 8 i maks. 32 znaków, w tym małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9), znaki specjalne !()*~'._-, ale nie może zawierać spacji.
Privacy	Tu wpisuje się algorytm kodowania dla wiadomości SNMP. Możliwe wartości to: - Brak kodowania („None“) - Data Encryption Standard („DES“) - Advanced Encryption Standard („AES“)
Privacy Key (min. 8 char.)	Tu wpisuje się klucz do kodowania wiadomości SNMP. Jeśli nic nie zostanie wpisane, automatycznie zastosowany zostaje „Authentication Key“. Klucz może zawierać min. 8 i maks. 32 znaków, w tym małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9), znaki specjalne !()*~'._-, ale nie może zawierać spacji.
Notification Receiver IP	Tu wpisuje się adres IP odbiorcy komunikatów trap dla v3. Jeśli dla tego użytkownika nie mają być wysyłane komunikaty trap w v3, pole zostaje puste.

Aby usunąć użytkownika, należy kliknąć odpowiedni przycisk **[Delete]**.

Aby dodać nowego użytkownika, należy kliknąć przycisk **[Add]**.

Zmiany zostaną zrealizowane dopiero po następnym restarcie sterownika.
W tym celu należy skorzystać z funkcji Reboot WBM. Nie wyłączać sterownika zbyt wcześnie!

19.1.1.2.26 Strona „WBM User Configuration“

Na stronie „WBM User Configuration“ można znaleźć ustawienia dla User-Aministration.

Grupa „Change Passwords“

Wskazówka Zmiana haseł



Ustawione fabrycznie hasła inicjalne podane są w niniejszej instrukcji obsługi i dlatego nie stanowią wystarczającego zabezpieczenia! Hasła należy zmieniać stosownie do potrzeb!

Tabela 178: Strona WMB „Users Configuration” – grupa „Change Passwords“

Parametr	Znaczenie
Select User	Tu wybiera się użytkownika („User“ lub „Admin“), dla którego ma być nadane nowe hasło.
Old Password	Tu należy podać stosowane aktualnie hasło.
New Password	Tu wpisuje się nowe hasło dla użytkownika wybranego w „Select User”. W hasło dopuszczalne są następujące znaki ASCII: a ... z, A ... Z, 0 ... 9, spacje i znaki specjalne: ! ? % + = () _ # " - / ` < > * ; , .
Confirm Password	Tu wpisuje się jeszcze raz nowe hasło w celu sprawdzenia.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Wskazówka W hasłach WBM używać dopuszczalnych znaków!



Jeśli poza WBM (np. przez klawiaturę USB) tworzone są hasła zawierające znaki niedopuszczalne w WBM, dostęp do stron WBM bezpośrednio na wyświetlaczu nie będzie możliwy, ponieważ na wirtualnej klawiaturze znajdują się tylko dopuszczalne znaki!

Wskazówka Rozszerzone uprawnienia użytkowników WBM



Użytkownicy WBM „admin“ i „user“ posiadają uprawnienia wykraczające poza WBM, aby mieć możliwość konfigurowania systemu i instalacji oprogramowania.

Zarządzanie użytkownikami dla aplikacji sterowania ustalane i realizowane jest osobno.

19.1.1.3 Zakładka „Fieldbus“

19.1.1.3.1 Strona „OPC UA Status“

Strona „OPC UA Status“ zawiera informacje o statusie usługi OPC UA.

Grupa „OPC UA Server“

Tabela 179: Strona WBM „OPC UA Configuration“ – grupa „OPC UA Server“

Parametr	Znaczenie
State	Tu wyświetlany jest aktualny status (enabled/disabled) serwera OPC UA WAGO.
Version	Tu wyświetlana jest zainstalowana wersja serwera OPC UA WAGO.
License	Tu wyświetlana jest aktualna licencja serwera OPC UA. Niektóre wersje serwera OPC UA WAGO zakładają konieczność wykupienia licencji.

19.1.1.3.2 Strona „OPC UA Configuration“

Na stronie „OPC UA Configuration“ znajdują się ustawienia dla usługi OPA UA.

Grupa „General OPC UA Server Configuration“

Tabela 180: Strona WBM „OPC UA Configuration“ – grupa „General OPC UA Server Configuration“

Parametr	Znaczenie	
Service enabled	Tu aktywuje się i dezaktywuje serwer OPC UA WAGO.	
Ctrl Configuration name	Tu podaje się nazwę konfiguracji, którą otrzymuje sterownik wewnątrz PLC Open Device Set.	
Log level	Tu wybiera się poziom dziennika. Można ustawić następujące wartości: Info / Debug / Warning / Error. Przy poziomie dziennika „Error” odczytywane są tylko komunikaty o błędach; przy poziomie dziennika „Info” odczytywane są również komunikaty o stanie. Wybór określonego poziomu dziennika wpływa na czas reakcji serwera. Dlatego należy wybrać najniższy niezbędny poziom, np. „Debug” dla dogłębnych analiz.	
Unlimited anonymous access	Tu ustawia się uprawnienia dostępu do danych udostępnianych przez serwer.	
	Enabled	Niezałogowany użytkownik może widzieć, odczytywać i zapisywać wszystkie zmienne.
	Disabled	Pełny dostęp do danych możliwy jest tylko dla zalogowanego użytkownika o odpowiednich uprawnieniach.

Aby zastosować zmiany, kliknąć przycisk **[Submit]**.

Grupa „OPC UA Endpoints“

Tabela 181: Strona WBM „OPC UA Configuration“ – grupa „OPC UA Endpoints“

Parametr	Znaczenie
Security Policy – None	Tu aktywuje się i dezaktywuje OPC UA Endpoint „None“. Umożliwia on nawiązanie niezabezpieczonego połączenia z serwerem OPC UA.
Security Policy – Basic128Rsa15	Tu aktywuje się lub dezaktywuje politykę bezpieczeństwa „Basic128Rsa15“. Wskazówka: Ta polityka nie jest już klasyfikowana jako bezpieczna.
Security Policy – Basic256Sha256	Polityka bezpieczeństwa „Basic256Sha256“ umożliwia nawiązanie bezpiecznego połączenia z serwerem OPC UA.

Aby zastosować zmiany, kliknąć przycisk **[Submit]**.

Grupa „OPC UA Security Settings“

Tabela 182: Strona WBM „OPC UA Configuration“ – grupa „OPC UA Security Settings“

Parametr	Znaczenie
Trust all clients	Tu aktywuje się lub dezaktywuje weryfikację.
	Enabled Dozwolone jest połączenie ze wszystkimi klientami. → Brak bezpieczeństwa!
	Disabled Dozwolone jest tylko połączenie z klientami z certyfikatami bezpieczeństwa.
Application URI Check	Tu aktywuje się lub dezaktywuje sprawdzenie URI. Dezaktywowany test URI umożliwia nawiązanie połączenia z serwerem OPC, nawet gdy jego URI różni się od URI zapisanego w certyfikatach.
Error Certificate Time	Tu aktywuje się lub dezaktywuje sprawdzenie czasu. Certyfikaty mogą mieć datę upływu. Ta data sprawdzana jest z aktualnym czasem urządzenia. Gdy w urządzeniu jest nieprawidłowo ustawiony czas, test nie może być przeprowadzony pomyślnie.
Certificate Issuer Time Invalid	Tu aktywuje się lub dezaktywuje sprawdzenie stempla czasowego. Certyfikaty CA zawierają ważność stempla czasu od wystawcy. Jest on używany, gdy sprawdzany jest czas na sprzecie serwera. Jeśli na serwerze nie został ustawiony czas lub jest on niepoprawny, certyfikat może zostać uznany za nieważny.
Certificate Revocation Unknown	Tu aktywuje się lub dezaktywuje sprawdzenie dostępności miejsca zapisu wycofanych certyfikatów. Każdy certyfikat może mieć miejsce na wycofane certyfikaty. Jeśli podane miejsce nie jest dostępne, np. na skutek problemów w pracy sieci, certyfikat nie zostaje zaakceptowany.
Certificate Issuer Revocation Unknown	Tu aktywuje się lub dezaktywuje sprawdzenie dostępności lokalizacji dla wycofanych certyfikatów. Każdy certyfikat (certyfikat CA) może zawierać wpis o lokalizacji dla wycofanych certyfikatów. Jeśli podane miejsce nie jest dostępne, certyfikat nie zostaje zaakceptowany przez serwer.

Aby zastosować zmiany, kliknąć przycisk **[Submit]**.

19.1.1.3.3 Strona „OPC UA Information Model“

Na stronie „OPC UA Information Model“ znajdują się ustawienia dla modelu informacyjnego OPA UA.

Strona ta widoczna jest tylko dla sterowników 2. generacji (750-821x/xxx-xxx), które obsługują komponenty programowe, podlegające kontroli licencji (licencje runtime).

Grupa „OPC UA Server Information Model“

Tabela 183: Strona WBM „OPC UA Information Model“ – grupa „OPC UA Server Information Model“

Parametr	Znaczenie
Feature enabled	Tu aktywuje się i dezaktywuje model informacyjny serwera OPC UA.
informationmodel.xml	Tu wybiera się plik XML dla modelu informacyjnego, który ma być zastosowany. Zastosowanie specyficznego modelu informacyjnego wymaga rozszerzonej („extended“) licencji OPC UA!

Aby zastosować zmianę, kliknąć przycisk **[Submit]**.

Aby przesłać wybrany plik do sterownika, należy kliknąć przycisk **[Upload]**.

Aby usunąć zainstalowany plik ze sterownika, należy kliknąć przycisk **[Delete]**.
Po usunięciu ponownie używany jest domyślnie zainstalowany model informacyjny PLC Open.

19.1.1.3.4 Strona „Modbus Services Configuration“

Na stronie „Modbus Services Configuration“ znajdują się ustawienia dla różnego typu usług Modbus. Grupy widoczne są tylko wtedy, gdy aktywowany jest system runtime *e!RUNTIME*. W przeciwnym razie zostaje wyświetlona wskazówka.

Grupa „Modbus TCP Slave“

Tabela 184: Strona WBM „Modbus Services Configuration“ – grupa „Modbus TCP“

Parametr	Znaczenie
Service active	Tu można aktywować/dezaktywować usługę Modbus/TCP.

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Grupa „Modbus UDP Slave“

Tabela 185: Strona WBM „Modbus Services Configuration“ – grupa „Modbus UDP“

Parametr	Znaczenie
Service active	Tu można aktywować/dezaktywować usługę Modbus UDP.

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

19.1.1.3.5 Strony „BACnet ...“

Strony WBM „BACnet Status“, „BACnet Configuration“, „BACnet Storage Location“, „BACnet Files“ i „BACnet Diagnostic“ wykazują pełną funkcjonalność tylko do celów testowych lub przy zainstalowanej licencji.

Funkcjonalność BACnet jest dostępna tylko wtedy, gdy sterownik obsługuje system *e!RUNTIME* i *e!RUNTIME* ustawiony jest jako system runtime.

Użycie funkcjonalności BACnet tylko do celów testowych sygnalizowane jest LED „SYS“ (patrz rozdział „Diagnostyka“ > „Elementy sygnalizacyjne“ > „LED dla systemu/sieci obiektowej“).

Opis stron WBM można znaleźć w informacjach technicznych dotyczących funkcjonalności udostępnianej na bazie licencji „*e!RUNTIME* BACnet/IP 300 (M)/600 (M)“.

19.1.1.4 Zakładka „Security“

19.1.1.4.1 Strona „OpenVPN / IPsec Configuration“

Na stronie „OpenVPN / IPsec Configuration“ znajdują się ustawienia OpenVPN i IPsec.

Grupa „OpenVPN“

Tabela 186: Strona WBM „OpenVPN / IPsec Configuration“ – grupa „OpenVPN“

Parametr	Znaczenie	
Current State	Tu wyświetlany jest aktualny status usługi OpenVPN.	
	stopped	Usługa nie jest aktywna.
	running	Usługa jest aktywna.
OpenVPN enabled	Tu można aktywować lub dezaktywować usługę OpenVPN.	
openvpn.config	Tu wybiera się plik konfiguracyjny OpenVPN, który należy przesłać z PC do produktu lub na odwrót.	

Aby zastosować zmianę, kliknąć przycisk **[Submit]**.

Aby wybrać plik na komputerze, należy kliknąć pole wyboru **Choose file**

Aby przesłać wybrany plik z PC do produktu, należy kliknąć przycisk **[Upload]**.

Aby przesłać plik z produktu do PC, należy kliknąć przycisk **[Download]**.

Zmiany zostaną zrealizowane dopiero po następnym restarcie produktu. W tym celu należy skorzystać z funkcji Reboot WBM. Nie należy wyłączać urządzenia zbyt wcześnie!

Grupa „IPsec“

Tabela 187: Strona WBM „OpenVPN / IPsec Configuration“ – grupa „IPsec“

Parametr	Znaczenie	
Current State	Tu wyświetlany jest aktualny status usługi IPsec.	
	stopped	Usługa nie jest aktywna.
	running	Usługa jest aktywna.
IPsec enabled	Tu można aktywować lub dezaktywować usługę IPsec.	
ipsec.conf	Tu wybiera się plik konfiguracyjny IPsec, który należy przesłać z PC do produktu lub na odwrót.	
ipsec.secrets	Tu wybiera się plik konfiguracyjny IPsec, który należy przesłać z PC do produktu.	

Aby zastosować zmianę, kliknąć przycisk **[Submit]**.

Aby wybrać plik na komputerze, należy kliknąć pole wyboru **Choose file**

Aby przesłać wybrany plik z PC do produktu, należy kliknąć przycisk **[Upload]**.

Aby przesłać plik z produktu do PC, należy kliknąć przycisk **[Download]**.

Zmiany zostaną zrealizowane dopiero po następnym restarcie produktu.
W tym celu należy skorzystać z funkcji Reboot WBM. Nie należy wyłączać urządzenia zbyt wcześnie!

19.1.1.4.2 Strona „General Firewall Configuration“

Na stronie „General Firewall Configuration“ można znaleźć globalne ustawienia dla funkcji Firewall.

Grupa „Global Firewall Parameter“

Tabela 188: Strona WBM „General Firewall Configuration“ – grupa „Global Firewall Parameter“

Parametr	Znaczenie
Firewall enabled entirely	Tu aktywuje się i dezaktywuje wszystkie funkcje firewall. To ustawienie ma najwyższy priorytet. Gdy firewall jest wyłączony, wszystkie inne ustawienia nie mają bezpośredniego znaczenia. Mimo to konfiguracja pozostałych parametrów jest możliwa, w celu odpowiedniego ich ustawienia przed włączeniem funkcji firewall.
ICMP echo broadcast protection	Tu aktywuje się i dezaktywuje zabezpieczenie „ICMP echo broadcast“.
Max. UDP connections per second	Tu wpisuje się maksymalną liczbę połączeń UDP na sekundę.
Max. TCP connections per second	Tu wpisuje się maksymalną liczbę połączeń ICP na sekundę.

Aby zastosować zmiany, kliknąć odpowiedni przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

19.1.1.4.3 Strona „Interface Configuration“

Na stronie „Interface Configuration“ znajdują się ustawienia funkcji firewall dla poszczególnych interfejsów.

Grupa „Firewall Configuration Bridge <n> / VPN“

Dla każdego skonfigurowanego bridge'a wyświetlana jest osobna grupa. Ustawienia w tej grupie dotyczą konfiguracji funkcji firewall na poziomie IP.

Tabela 189: Strona WBM „Interface Configuration“ – grupa „Firewall Configuration Bridge <n> / VPN“

Parametr	Znaczenie
Firewall enabled for Interface	Tu aktywuje się i dezaktywuje funkcję firewall dla poszczególnych bridge'ów.
ICMP echo protection	Tu aktywuje się i dezaktywuje zabezpieczenie „ICMP echo“ dla poszczególnych bridge'ów.
ICMP echo limit per second	Tu wpisuje się maksymalną liczbę „ICMP pings“ na sekundę. „0“ = „Disabled“
ICMP burst limit (0 = disabled)	Tu wpisuje się maksymalną liczbę „ICMP echo burst“ na sekundę. „0“ = „Disabled“
Service enabled	Telnet; ten przycisk wyświetlany jest tylko wtedy, gdy obsługiwana jest usługa Telnet.
	FTP
	FTPS
	HTTP
	HTTPS
	I/O-CHECK
	PLC Runtime
	PLC WebVisu – direct link (port 8080)
	SSH
	TFTP
	BootP/DHCP
	DNS
	Modbus TCP
	Modbus UDP
	SNMP
	OPC UA
	PROFINET IO
Tu aktywuje się i dezaktywuje funkcję firewall dla poszczególnych usług. Same usługi muszą być włączane i wyłączane osobno przez stronę „Ports and Services“.	

Aby zastosować zmiany, kliknąć odpowiedni przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

19.1.1.4.4 Strona „Configuration of MAC address filter“

Na stronie „Configuration of MAC address filter“ ustawia się konfigurację funkcji firewall na poziomie sieci ETHERNET.

„MAC Address Filter Whitelist“ otrzymuje domyślny wpis o następujących wartościach:

Adres MAC: 00:30:DE:00:00:00

Maska MAC: ff:ff:ff:00:00:00

Włączenie domyślnego wpisu umożliwi komunikację między różnymi urządzeniami WAGO w sieci.

Wskazówka



Przed aktywowaniem filtra aktywować adresy MAC!

Zanim aktywuje się filtr adresów MAC, należy wpisać i aktywować własne adresy MAC na „MAC Address Filter Whitelist“.

W przeciwnym razie nie będzie można uzyskać dostępu do urządzenia przez sieć ETHERNET. Dotyczy to także innych usług, wykorzystywanych przez urządzenie, np. konfiguracji IP przez DHCP.

Jeśli na „MAC Address Filter Whitelist“ nie ma adresu MAC serwera DHCP, urządzenie po następnej aktualizacji straci swoje ustawienia IP i nie będzie już dostępne.

Dopóki „MAC Address Filter Whitelist“ będzie pusta, nie będzie można włączyć filtra.

Jeśli będzie na niej co najmniej jeden włączony adres, przed włączeniem zostanie jeszcze raz wysłane odpowiednie ostrzeżenie, które należy potwierdzić.

Opisany powyżej test przeprowadzany jest tylko w WBM, ale nie w CBM!

Grupa „Global MAC address filter state“

Tabela 190: Strona WBM „Configuration of MAC address filter“ – grupa „Global MAC address filter state“

Parametr	Znaczenie
Filter enabled	Tu aktywuje się i dezaktywuje globalny filtr adresów MAC.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Grupa „MAC address filter state Bridge <n>“

Dla każdego skonfigurowanego bridge'a wyświetlana jest osobna grupa.

Tabela 191: Strona WBM „Configuration of MAC address filter“ – grupa „MAC address filter state Bridge <n>“

Parametr	Znaczenie
Filter enabled	Tu aktywuje się i dezaktywuje filtr adresów MAC dla poszczególnych bridge'ów.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Grupa „MAC address filter whitelist“

Dla każdej pozycji na liście wyświetlany jest osobny obszar.

Tabela 192: Strona WBM „Configuration of MAC address filter“ – grupa „MAC address filter whitelist“

Parametr	Znaczenie
MAC address	Tu wyświetlany jest adres MAC danej pozycji na liście.
MAC mask	Tu wyświetlana jest maska MAC każdej danej na liście.
Filter enabled	Tu aktywuje się i dezaktywuje filtr dla danej pozycji na liście.
Add filter to whitelist	Tu tworzy się nową pozycję na liście.
MAC address	Tu wpisuje się adres MAC dla nowej pozycji na liście. Można wpisać 10 filtrów.
MAC mask	Tu wpisuje się maskę MAC dla nowej pozycji na liście.
Filter enabled	Tu aktywuje się i dezaktywuje filtr dla nowej pozycji na liście.

Aby zastosować zmiany, kliknąć odpowiedni przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Aby usunąć pozycję na liście, należy kliknąć odpowiedni przycisk **[Delete]**. Zmiana jest realizowana natychmiast.

Aby zastosować nową pozycję na liście, kliknąć przycisk **[Add]**. Można wpisać 10 filtrów. Zmiana jest realizowana natychmiast.

19.1.1.4.5 Strona „Configuration of User Filter“

Na stronie „Configuration of User Filter“ znajdują się ustawienia specyficznych dla użytkownika filtrów funkcji firewall.

Grupa „User filter“

Dla każdego skonfigurowanego filtra wyświetlany jest osobny obszar.

Tabela 193: Strona WBM „Configuration of User Filter” – grupa „User filter”

Parametr	Znaczenie	
Policy	Tu wyświetlana jest informacja, czy dane urządzenie sieciowe jest przez filtr dopuszczone czy wykluczone.	
Source IP address	Tu wyświetlany jest źródłowy adres IP dla danego filtra.	
Source Netmask	Tu wyświetlana jest maska sieci źródłowej dla danego filtra.	
Source Port	Tu wyświetlany jest numer portu źródłowego dla danego filtra.	
Destination IP address	Tu wyświetlany jest docelowy adres IP dla danego filtra.	
Destination Netmask	Tu wyświetlana jest maska sieci docelowej dla danego filtra.	
Destination Port	Tu wyświetlany jest numer portu docelowego dla danego filtra.	
Protocol	Tu wyświetlane są dopuszczalne protokoły dla danego filtra.	
Input interface	Tu wyświetlane są dopuszczalne interfejsy dla danego filtra.	
Add new user filter	Maksymalnie można utworzyć 10 filtrów. W polach należy wpisać wartości, które mają być użyte dla filtra. Należy wpisać co najmniej 1 wartość, pozostałe pola mogą zostać puste.	
Policy	Tu definiuje się, czy dane urządzenie sieciowe ma być przez filtr dopuszczone czy wykluczone.	
	Allow	Urządzenie sieciowe jest dopuszczone.
	Drop	Urządzenie sieciowe jest wykluczone.
Source IP address	Tu wpisuje się źródłowy adres IP dla nowego filtra.	
Source netmask	Tu wpisuje się maskę sieci źródłowej dla nowego filtra.	
Source port	Tu wpisuje się numer portu źródłowego dla nowego filtra.	
Destination IP address	Tu wpisuje się docelowy adres IP dla nowego filtra.	
Destination subnet mask	Tu wpisuje się maskę sieci docelowej dla nowego filtra.	
Destination port	Tu wpisuje się numer portu docelowego dla nowego filtra.	
Protocol	Tu wpisuje się protokoły dla nowego filtra.	
	TCP/UDP	Serwisy TCP i UDP są filtrowane.
	TCP	Serwis TCP jest filtrowany.
	UDP	Serwis UDP jest filtrowany.
Input interface	Tu wpisuje się interfejsy dla nowego filtra.	
	Any	Wszystkie interfejsy są filtrowane.

Tabela 193: Strona WBM „Configuration of User Filter“ – grupa „User filter“

Parametr	Znaczenie	
	Bridge <n>	Filtrowane są interfejsy przypisane do bridge'a <n>. Wyświetlane są tylko skonfigurowane bridge.
	VPN	Interfejs VPN jest filtrowany.

Aby zastosować nowy filtr, kliknąć przycisk **[Add]**. Zmiana jest realizowana natychmiast.

Aby usunąć istniejący filtr, kliknąć przycisk **[Delete]**. Zmiana jest realizowana natychmiast.

19.1.1.4.6 Strona „Certificates“

Na stronie „Certificates“ można dokonać wyboru, czy dane certyfikaty i klucze zainstalować, czy usunąć.

Grupa „Installed Certificates“

Tabela 194: Strona WBM „Configuration of OpenVPN and IPsec“ – grupa „Certificate List“

Parametr	Znaczenie
<certificate name>	Tu wyświetlane są załadowane certyfikaty. Jeśli brak załadowanych certyfikatów, wyświetlana jest informacja „No certificates existing“.

Aby wybrać plik na komputerze, należy kliknąć pole wyboru **Choose file**

Aby przesłać wybrany plik do produktu, należy kliknąć przycisk **[Upload]**. Zmiany są realizowane natychmiast.

Certyfikaty zapisywane są w katalogu „/etc/certificates/“, a klucze w katalogu „/etc/certificates/keys“.

Aby usunąć daną pozycję, należy kliknąć przycisk **[Delete]**. Zmiany są realizowane natychmiast.

Grupa „Installed Private Keys“

Tabela 195: Strona WBM „Configuration of OpenVPN and IPsec“ – grupa „Private Key List“

Parametr	Znaczenie
<private key name>	Tu wyświetlane są załadowane klucze. Jeśli brak załadowanych kluczy, wyświetlana jest informacja „No private keys existing“.

Aby wybrać plik na komputerze, należy kliknąć pole wyboru **Choose file**

Aby przesłać wybrany plik do produktu, należy kliknąć przycisk **[Upload]**. Zmiany są realizowane natychmiast.

Certyfikaty zapisywane są w katalogu „/etc/certificates/“, a klucze w katalogu „/etc/certificates/keys“.

Aby usunąć daną pozycję, należy kliknąć przycisk **[Delete]**. Zmiany są realizowane natychmiast.

19.1.1.4.7 Grupa „Security Settings“

Na stronie „Security Settings“ znajdują się ustawienia dotyczące bezpieczeństwa sieci.

Grupa „TLS Configuration“

Tabela 196: Strona WBM „Security Settings“ – grupa „TLS Configuration“

Parametr	Znaczenie	
TLS Configuration	Tu ustawia się dopuszczalne wersje TLS i procedur kryptograficznych dla HTTPS.	
	standard	Serwer WWW zezwala na wersje TLS 1.0, TLS 1.1, TLS 1.2, a także metody kryptograficzne, które obecnie nie są już uważane za bezpieczne.
	Strong	Serwer WWW zezwala tylko na wersję TLS 1.2 i na silne algorytmy. Starsze oprogramowanie i starsze systemy operacyjne mogą nie obsługiwać protokołu TLS 1.2.

Aby zastosować zmianę, kliknąć przycisk **[Submit]**. Zmiana jest realizowana natychmiast.

Informacja



Techniczna dyrektywa TR-02102 BSI

Zasady dotyczące ustawienia „Strong“ są oparte na wytycznej technicznej TR-02102 Federalnego Urzędu ds. Bezpieczeństwa Informacji.

Wytyczne można znaleźć na stronie: <https://www.bsi.bund.de> >

„Publikacje“ > „Wytyczne techniczne“.

19.1.1.4.8 Strona „Advanced Intrusion Detection Environment (AIDE)“

Na stronie „Advanced Intrusion Detection Environment (AIDE)“ znajdują się ustawienia dotyczące bezpieczeństwa sieci.

Grupa „Run AIDE check at startup“

Tabela 197: Strona WBM „Advanced Intrusion Detection Environment (AIDE)“ – grupa „Run AIDE check at startup“

Parametr	Znaczenie
Service active	Tu można aktywować/dezaktywować „AIDE check“ przy starcie sterownika.

Aby zastosować zmiany, kliknąć przycisk **[Submit]**. Zmiany zostaną zrealizowane przy następnym restarcie.

Grupa „Refresh Options“

Tabela 198: Strona WBM „Advanced Intrusion Detection Environment (AIDE)“ – grupa „Control AIDE and show log“

Parametr	Znaczenie
Select Action	Tu wybiera się działanie do wykonania.
	readlog Wyświetlane są dane logowania.
	init Instalowana jest baza danych, która uzupełniana jest aktualnymi wartościami.
	check Aktualne wartości zostają porównane z wartościami zapisanymi w bazie danych.
	update Aktualne wartości zostają porównane z wartościami zapisanymi w bazie danych, a następnie baza danych jest aktualizowana.
Read only the last n	Tu włącza się wyświetlanie ostatnich n komunikatów. Dodatkowo wpisuje się liczbę wyświetlonych komunikatów.
Automatic refresh interval (sec)	Aby włączyć cykliczną aktualizację, należy zaznaczyć odpowiednie pole. Wpisać odstęp czasowy (w sekundach) cyklicznych aktualizacji. W zależności od statusu zmienia się opis przycisku („Refresh“/„Start“/„Stop“).

Aby zaktualizować wyświetlenie, należy kliknąć przycisk **[Refresh]**.
Przycisk jest widoczny tylko wtedy, gdy cykliczna aktualizacja nie jest włączona.

Aby aktywować cykliczną aktualizację, należy kliknąć przycisk **[Start]**.
Przycisk ten jest widoczny tylko wtedy, gdy cykliczna aktualizacja jest włączona, ale jeszcze nie została uruchomiona.

Aby zakończyć cykliczną aktualizację, należy kliknąć przycisk **[Stop]**.
Przycisk ten jest widoczny tylko wtedy, gdy cykliczna aktualizacja jest aktywna.

Cykliczną aktualizację można przeprowadzić tylko wtedy, jeśli otwarta jest strona „Advanced Intrusion Detection Environment (AIDE)”. Przy zmianie strony WBM aktualizacja zostaje zatrzymana do momentu, aż strona „Advanced Intrusion Detection Environment (AIDE)” zostanie ponownie otwarta.

Komunikaty są wyświetlane pod ustawieniami.

19.1.1.5 Zakładka „Diagnostic“

19.1.1.5.1 Strona „Diagnostic Information“

Na stronie „Diagnostic Information“ znajdują się ustawienia do wyświetlania komunikatów diagnostycznych.

Tabela 199: Strona WBM „Diagnostic Information“

Parametr	Znaczenie
Read only the last	Tu włącza się wyświetlanie ostatnich n komunikatów. Dodatkowo wpisuje się liczbę wyświetlonych komunikatów.
Automatic refresh interval (sec)	Aby włączyć cykliczną aktualizację, należy zaznaczyć odpowiednie pole. Wpisać odstęp czasowy (w sekundach) cyklicznych aktualizacji. W zależności od statusu zmienia się opis przycisku („Refresh“/„Start“/„Stop“).

Aby zaktualizować wyświetlenie lub aktywować cykliczną aktualizację, należy kliknąć przycisk **[Refresh]**. Przycisk ten jest widoczny tylko wtedy, gdy cykliczna aktualizacja nie jest włączona.

Aby aktywować cykliczną aktualizację, należy kliknąć przycisk **[Start]**. Przycisk ten jest widoczny tylko wtedy, gdy cykliczna aktualizacja jest włączona, ale jeszcze nie została uruchomiona.

Aby zakończyć cykliczną aktualizację, należy kliknąć przycisk **[Stop]**. Przycisk ten jest widoczny tylko wtedy, gdy cykliczna aktualizacja jest aktywna.

Cykliczną aktualizację można przeprowadzić tylko wtedy, jeśli otwarta jest strona „Diagnostic Information“. Przy zmianie strony WBM aktualizacja jest zatrzymana do momentu, aż strona „Diagnostic Information“ zostanie ponownie otwarta.

Komunikaty są wyświetlane pod ustawieniami.

19.1.2 Console-Based-Management (CBM)

19.1.2.1 Menu „Information“

To menu zawiera dalsze podpunkty menu z informacjami na temat sterownika i sieci.

Tabela 200: Menu „Information“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Controller Details	Otwiera podmenu z właściwościami sterownika
2. Network Details	Otwiera podmenu z właściwościami sieci i interfejsów sterownika

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.1.1 Podmenu „Information“ > „Controller Details“

W tym podmenu wyświetlane są właściwości sterownika.

Tabela 201: Podmenu „Information“ > „Controller Details“

Parametr	Znaczenie
Product Description	Nazwa sterownika
Order Number	numer katalogowy sterownika
Licence Information	Informuje, że system runtime CODESYS jest zainstalowany.
Firmware Revision	Wersja firmware

Aby wrócić do menu nadrzędnego, należy nacisnąć **[Q]** lub **[Return]**.

19.1.2.1.2 Podmenu „Information“ > „Network Details“

W tym podmenu są wyświetlane właściwości sieci i interfejsów sterownika.

Jeśli interfejsy ETHERNET są używane w trybie „Switched“, to dla obu złącz wyświetlana jest jedna tabela („X1/X2“).

Jeśli interfejsy są używane w trybie „Separated“, to dla każdego złącza wyświetlana jest osobna tabela („X1“ / „X2“).

Tabela 202: Podmenu „Information“ > „Network Details“

Parametr	Znaczenie
State	Status interfejsu ETHERNET (aktywny/nieaktywny)
Mac Address	Adres MAC, służący do identyfikacji i adresowania sterownika
IP Address	Aktualny adres IP sterownika i (w nawiasach) rodzaj odniesienia (static/bootp/dhcp)
Subnet Mask	Aktualna maska podsieci sterownika

Aby wrócić do menu nadrzędnego, należy nacisnąć **[Q]** lub **[Return]**.

19.1.2.2 Menu „PLC Runtime“

To menu zawiera dalsze podpunkty menu z informacjami i ustawieniami systemu runtime.

Tabela 203: Menu „PLC Runtime“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Information	Otwiera podmenu z informacjami o systemie runtime.
2. General Configuration	Otwiera podmenu z ustawieniami systemu runtime.
3. WebVisu	Otwiera podmenu z ustawieniami wizualizacji sieciowej.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.2.1 Podmenu „PLC Runtime“ > „Information“

To podmenu zawiera dalsze podpunkty menu z informacjami o systemie runtime i programie PLC.

Punkty menu 2. ... 6. widoczne są tylko wtedy, gdy CODESYS V2 jest ustawiony jako system runtime.

Tabela 204: Podmenu „PLC Runtime“ > „Information“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Runtime Version	Otwiera podmenu umożliwiające wyświetlenie wersji systemu runtime.
2. Webserver Version	Otwiera podmenu umożliwiające wyświetlenie wersji serwera WWW.
3. State	Otwiera podmenu umożliwiające wyświetlenie stanu pracy PLC.
4. Number of Tasks	Otwiera podmenu umożliwiające wyświetlenie liczby zadań w programie PLC.
5. Project Details	Otwiera podmenu umożliwiające wyświetlenie informacji o projekcie do programu PLC.
6. Tasks	Otwiera podmenu umożliwiające wyświetlenie zadań w programie PLC.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.2.2 Podmenu „Information“ > „Runtime Version“

W tym podmenu wyświetlana jest wersja systemu runtime.

Tabela 205: Podmenu „PLC Runtime“ > „Information“ > „Runtime Version“

Parametr	Znaczenie
Version	Tu wyświetlana jest wersja aktualnie aktywowanego systemu runtime. Przy wyłączonym systemie runtime wyświetlana jest informacja „None“.

Aby wrócić do menu nadrzędnego, należy nacisnąć **[Q]** lub **[Return]**.

19.1.2.2.3 Podmenu „Information“ > „Webserver Version“

W tym podmenu wyświetlana jest wersja serwera WWW.

To podmenu jest widoczne tylko wtedy, gdy jako system runtime włączony jest CODESYS V2.

Tabela 206: Podmenu „PLC Runtime“ > „Information“ > „Webserver Version“

Parametr	Znaczenie
Version	Tu wyświetlana jest wersja serwera WWW.

Aby wrócić do menu nadrzędnego, należy nacisnąć **[Q]** lub **[Return]**.

19.1.2.2.4 Podmenu „Information“ > „State“

W tym podmenu wyświetlany jest stan pracy PLC.

To podmenu jest widoczne tylko wtedy, gdy jako system runtime włączony jest CODESYS V2.

Tabela 207: Podmenu „PLC Runtime“ > „Information“ > „State“

Parametr	Znaczenie	
State	Tu wyświetlany jest stan pracy PLC.	
	STOP	Program PLC nie jest wykonywany.
	RUN	Program PLC jest wykonywany.

Aby wrócić do menu nadrzędnego, należy nacisnąć **[Q]** lub **[Return]**.

19.1.2.2.5 Podmenu „Information“ > „Number of Tasks“

W tym podmenu wyświetlana jest liczba zadań w programie PLC.
To podmenu jest widoczne tylko wtedy, gdy jako system runtime włączony jest CODESYS V2.

Tabela 208: Podmenu „PLC Runtime“ > „Information“ > „Number of Tasks“

Parametr	Znaczenie
Number of Tasks	Tu wyświetlana jest liczba zadań w programie PLC.

Aby wrócić do menu nadrzędnego, należy nacisnąć **[Q]** lub **[Return]**.

19.1.2.2.6 Podmenu „Information“ > „Project Details“

W tym podmenu wyświetlane są informacje o projekcie z programu PLC.
To podmenu jest widoczne tylko wtedy, gdy jako system runtime włączony jest CODESYS V2 i program jest wykonywany.

Tabela 209: Podmenu „PLC Runtime“ > „Information“ > „Project Details“

Tabela 205: Podmenu „PLC Runtime” > „Information” > „Project Details	
Parametr	Znaczenie
Date	Wyświetla informacje o projekcie, które programista wprowadził do programu PLC (w środowisku programistycznym pod Project > Project Information ...)
Title	
Version	
Author	
Description	Pole „Description“ może zawierać tekst o długości maksymalnie 1024 znaki.

Aby wrócić do menu nadrzędnego, należy nacisnąć **[Q]** lub **[Return]**.

19.1.2.2.7 Podmenu „Information“ > „Tasks“

W tym podmenu wyświetlane są zadania z programu PLC. Dla każdego zadania tworzony jest osobny wpis.
To podmenu jest widoczne tylko wtedy, gdy jako system runtime włączony jest CODESYS V2.

Tabela 210: Podmenu „PLC Runtime“ > „Information“ > „Tasks“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
n. Task n	Otwiera podmenu z informacjami o wybranym zadaniu.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.2.8 Podmenu „Tasks“ > „Task n“

W tym podmenu wyświetlane są informacje o wybranym zadaniu. To podmenu jest widoczne tylko wtedy, gdy jako system runtime włączony jest CODESYS V2.

Tabela 211: Podmenu „PLC Runtime“ > „Information“ > „Tasks“ > „Task n“

Parametr	Znaczenie
Cycle count	Liczba cykli zadania od startu systemu
Cycletime (µsec)	Aktualnie mierzony czas wykonywania zadania
Cycletime min (µsec)	Minimalny czas wykonywania zadania od startu systemu
Cycletime max (µsec)	Maksymalny czas wykonywania zadania od startu systemu
Cycletime avg (µsec)	Średni czas wykonywania zadania od startu systemu
Status	Status zadania (np. RUN, STOP)
Mode	Tryb wykonywania zadania (np. cykliczny)
Priority	Ustawiony priorytet zadania
Interval (msec)	Ustawiony interwał zadania

Aby wrócić do menu nadrzędnego, należy nacisnąć **[Q]** lub **[Return]**.

19.1.2.2.9 Podmenu „PLC Runtime“ > „General Configuration“

To podmenu zawiera dalsze podpunkty menu z ogólnymi ustawieniami systemu runtime.

Tabela 212: Podmenu „PLC Runtime“ > „General Configuration“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. PLC Runtime Version	Otwiera podmenu z ustawieniami systemu runtime CODESYS.
2. Home Dir On SD Card	Otwiera podmenu z ustawieniami katalogu Home

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.2.10 Podmenu „General Configuration“ > „PLC Runtime Version“

W tym podmenu można wybrać, który system runtime PLC jest aktywowany.

Tabela 213: Podmenu „PLC Runtime“ > „General Configuration“ > „PLC Runtime Version“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. None	Żaden system runtime nie jest aktywowany.
2. CODESYS 2	System runtime CODESYS V2 jest aktywowany.
3. e!RUNTIME	System runtime e!RUNTIME jest aktywowany.

Wskazówka **Przy przełączeniu systemu runtime usuwane są wszystkie dane!**



Przy przełączeniu systemu runtime katalog Home dla systemu operacyjnego zostaje całkowicie usunięty.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.2.11 Podmenu „General Configuration“ > „Home Dir On SD Card“

W tym podmenu ustawia się, czy katalog Home dla systemu runtime ma być zapisywany na karcie pamięci.

Tabela 214: Podmenu „PLC Runtime“ > „General Configuration“ > „Home Dir On SD Card“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Enable	Katalog Home dla systemu operacyjnego zapisywany jest na karcie pamięci.
2. Disable	Katalog Home dla systemu operacyjnego zapisywany jest w wewnętrznej pamięci sterownika.

Wskazówka **Przed przeniesieniem katalogu Home włożyć kartę pamięci!**



Jeśli katalog Home ma być przeniesiony na kartę pamięci, należy najpierw włożyć do urządzenia kartę sformatowaną za pomocą obsługiwanego systemu plików. Tylko pierwsza partycja karty pamięci dostępna jest pod /media/sd i może zostać wykorzystana jako katalog Home.

Wskazówka **Przed przeniesieniem katalogu Home przeprowadzić reset!**



Przed przeniesieniem katalogu Home systemu runtime należy zatrzymać bieżącą aplikację IEC 61131. Urządzenie należy doprowadzić do stanu podstawowego przez zastosowanie funkcji „Reset“. Wszystkie obecne projekty bootowalne zostaną usunięte.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.2.12 Podmenu „PLC Runtime“ > „WebVisu“

To podmenu zawiera informacje i ustawienia wizualizacji sieciowej.

Tabela 215: Podmenu „PLC Runtime“ > „WebVisu“

Punkt menu	Podpunkt menu / znaczenie	
0. Back to ...	Powrót do menu nadrzędnego	
1. CODESYS 2 Webserver State	Tu wyświetlany jest status serwera WWW CODESYS V2.	
2. e!RUNTIME Webserver State	Tu wyświetlany jest status serwera WWW <i>e!RUNTIME</i> .	
3. Default Webserver	Tu można wybrać, czy przy wpisaniu adresu IP sterownika ma być wyświetlany Web-Based-Management, czy wizualizacja sieciowa systemu runtime.	
	0. Back to ...	Powrót do menu nadrzędnego
	1. Web-based Management	Wyświetla się Web-Based-Management.
	2. CODESYS WebVisu	Wyświetla się wizualizacja sieciowa systemu runtime.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.3 Menu „Networking“

To menu zawiera dalsze podpunkty menu z ustawieniami do konfiguracji sieci.

Tabela 216: Menu „Networking“

Parametr	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Host/Domainname	Otwiera podmenu z możliwościami ustawień ogólnych parametrów TCP/IP
2. TCP/IP	Otwiera podmenu z ustawieniami TCP/IP interfejsów sieci ETHERNET
3. Ethernet	Otwiera podmenu z ustawieniami do konfiguracji sieci ETHERNET.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.3.1 Podmenu „Networking“ > „Host-/Domain Name“

To podmenu zawiera dalsze podpunkty menu „Hostname“ i „Domain Name“ z możliwościami ustawień ogólnych parametrów TCP/IP.

Tabela 217: Podmenu „Networking“ > „Host-/Domain Name“

Parametr	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Hostname	Otwiera podmenu z ustawieniami nazwy hosta. Oprócz tego punktu wyświetlane są skonfigurowana i aktualnie używana nazwa hosta.
2. Domain Name	Otwiera podmenu z ustawieniami nazwy hosta. Oprócz tego punktu wyświetlane są skonfigurowana i aktualnie używana nazwa domeny.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.3.2 Podmenu „Host-/Domain Name“ > „Hostname“

W tym podmenu można ustawić nazwę hosta sterownika.

Tabela 218: Podmenu „Networking“ > „Host-/Domain Name“ > „Hostname“

Parametr	Znaczenie
Enter new Hostname	Tu wpisuje się nazwę hosta sterownika, która ma być potem stosowana, gdy interfejs sieciowy zostanie zmieniony na statyczny adres IP lub gdy nazwa hosta nie jest podawana przez odpowiedź DHCP.

Aby zastosować ustawienie, kliknąć przycisk [**<OK>**].

Aby odrzucić ustawienie, kliknąć przycisk [**<Abort>**].

19.1.2.3.3 Podmenu „Host-/Domain Name“ > „Domain Name“

W tym podmenu można ustawić nazwę domeny sterownika.

Tabela 219: Podmenu „Networking“ > „Host-/Domain Name“ > „Domain Name“

Parametr	Znaczenie
Enter new Domain Name	Tu wpisuje się nazwę domeny. Domyślny wpis brzmi: „localdomain.lan“.

Aby zastosować ustawienie, kliknąć przycisk [**<OK>**].

Aby odrzucić ustawienie, kliknąć przycisk [**<Abort>**].

19.1.2.3.4 Podmenu „Networking“ > „TCP/IP“

To podmenu zawiera dalsze podpunkty menu z ustawieniami TCP/IP interfejsów sieci ETHERNET.

Tabela 220: Podmenu „Networking“ > „TCP/IP“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. IP Address	Otwiera podmenu z ustawieniami adresu(-ów) IP.
2. Default Gateway	Otwiera podmenu z ustawieniami bram standardowych.
3. DNS Server	Otwiera podmenu z ustawieniami serwera(-ów) DNS.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [**Q**].

19.1.2.3.5 Podmenu „TCP/IP“ > „IP Address“

To podmenu zawiera dalsze podpunkty menu z ustawieniami interfejsów sieci ETHERNET.

Podmenu jest widoczne tylko wtedy, gdy sterownik pracuje w trybie „Separated“. Jeśli sterownik pracuje w trybie „Switched“, zostaje bezpośrednio wyświetlone podmenu „IP Address > X1“.

Tabela 221: Podmenu „Networking“ > „TCP/IP“ > „IP Address“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. X1	Otwiera podmenu z ustawieniami interfejsu X1.
2. X2	Otwiera podmenu z ustawieniami interfejsu X2.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.3.6 Podmenu „IP Address“ > „Xn“

To podmenu zawiera ustawienia wybranego interfejsu.

Tabela 222: Podmenu „Networking“ > „TCP/IP“ > „IP Address“ > „Xn“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Type of IP Address Configuration	Tu można zdecydować, czy ma być zastosowane statyczne czy dynamiczne adresowanie IP.
	0. Back to ... Powrót do menu nadrzędnego
	1. Static IP Statyczne adresowanie IP Przy wyborze statycznego adresowania odpytany jest od razu adres IP i maska podsieci.
	2. DHCP Dynamiczne adresowanie IP
	3. BootP Dynamiczne adresowanie IP
2. IP Address	Tu wpisuje się statyczny adres IP.
3. Subnet Mask	Tu należy wpisać maskę podsieci.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.
Aby zastosować ustawienie, kliknąć przycisk **[<OK>]**.
Aby odrzucić ustawienie, kliknąć przycisk **[<Abort>]**.

19.1.2.3.7 Podmenu „TCP/IP“ > „Default Gateway“

To podmenu zawiera dalsze podpunkty menu z ustawieniami bram standardowych.

Tabela 223: Podmenu „Networking“ > „TCP/IP“ > „Default Gateway“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Default Gateway 1	Otwiera podmenu z ustawieniami bramy standardowej 1 Oprócz tego punktu wyświetlany jest aktualny status bramy.
2. Default Gateway 2	Otwiera podmenu z ustawieniami bramy standardowej 2 Oprócz tego punktu wyświetlany jest aktualny status bramy.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć [Q].

19.1.2.3.8 Podmenu „Default Gateway“ > „Default Gateway n“

To podmenu zawiera ustawienia wybranej bramy.

Tabela 224: Podmenu „Networking“ > „TCP/IP“ > „Default Gateway“ > „Default Gateway n“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. State	Tu można zdecydować, czy wybrana brama standardowa ma być zastosowana.
	0. Back to ... Powrót do menu nadrzędnego
	1. Disabled Brama standardowa nie jest zastosowana.
	2. Enabled Brama standardowa jest zastosowana.
2. Gateway IP Address	Tu ustawia się adres bramy standardowej.
3. Gateway Metric	Tu ustawia się liczbę, będącą metryką. Standardowa wartość metryki wynosi 20, najmniejsza wartość to 0, a największa 4.294.967.295.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć [Q].
Aby zastosować ustawienie, kliknąć przycisk [<OK>].
Aby odrzucić ustawienie, kliknąć przycisk [<Abort>].

19.1.2.3.9 Podmenu „TCP/IP“ > „DNS Server“

To podmenu zawiera ustawienia serwera DNS.

Tabela 225: Podmenu „Networking“ > „TCP/IP“ > „DNS Server“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
n. DNS Server n	Tu wyświetlane są adresy wpisanych serwerów DNS. Dla wpisanego serwera dostępnych jest kilka podpunktów menu.
	0. Back to ... Powrót do menu nadrzędnego
	1. Edit Tu można zmienić wybrany adres serwera DNS.
	2. Delete Tu usuwa się wybrany adres serwera DNS.
(n+1). Add new DNS Server	Tu dodaje się kolejne adresy serwera DNS. Można wpisać 10 adresów.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

Aby zastosować ustawienie, kliknąć przycisk **[<OK>]**.

Aby odrzucić ustawienie, kliknąć przycisk **[<Abort>]**.

19.1.2.3.10 Podmenu „Networking“ > „Ethernet“

To podmenu zawiera dalsze podpunkty menu z ustawieniami do konfiguracji sieci ETHERNET

Tabela 226: Podmenu „Networking“ > „Ethernet“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Switch Configuration	Otwiera podmenu z ustawieniami do konfiguracji switcha.
2. Ethernet Ports	Otwiera podmenu z ustawieniami interfejsów sieci ETHERNET.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.3.11 Podmenu „Ethernet“ > „Switch Configuration“

To podmenu zawiera dalsze podpunkty menu z ustawieniami do konfiguracji switcha.

Tabela 227: Podmenu „Networking“ > „Ethernet“ > „Switch Configuration“

Podmenu	Podpunkt menu / znaczenie	
0. Back to ...	Powrót do menu nadrzędnego	
1. Network interfaces	Tu włączą się i wyłączą switch.	
	0. Back to ...	Powrót do menu nadrzędnego
	1. Separated	Każde złącze ma własny adres IP.
	2. Switched	Oba złącza mają jeden adres IP.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.3.12 Podmenu „Ethernet“ > „Ethernet Ports“

To podmenu zawiera dalsze podpunkty menu z ustawieniami interfejsów sieci ETHERNET.

Tabela 228: Podmenu „Networking“ > „Ethernet“ > „Ethernet Ports“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Interface X1	Otwiera podmenu z ustawieniami interfejsu X1.
2. Interface X2	Otwiera podmenu z ustawieniami interfejsu X2.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.3.13 Podmenu „Ethernet Ports“ > „Interface Xn“

To podmenu zawiera ustawienia wybranego interfejsu ETHERNET.

Tabela 229: Podmenu „Networking“ > „Ethernet“ > „Ethernet Ports“ > „Interface Xn“

Podmenu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Port	Tu można zdecydować, czy wybrany port ma być zastosowany.
	0. Back to ... Powrót do menu nadrzędnego
	1. Disabled Port nie jest zastosowany.
	2. Enabled Port jest zastosowany.
2. Autonegotiation	Tu można zdecydować, czy funkcja autonegotjacji dla wybranego portu ma być aktywna.
	0. Back to ... Powrót do menu nadrzędnego
	1. Disabled Autonegotjacja nie jest aktywna.
	2. Enabled Autonegotjacja jest aktywna.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.4 Podmenu „Firewall“

To menu zawiera dalsze podpunkty menu do ustawiania funkcji Firewall.

Tabela 230: Menu „Firewall“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. General Configuration	Otwiera podmenu z ogólnymi ustawieniami funkcji Firewall.
2. MAC Address Filter	Otwiera podmenu z ustawieniami filtra adresów MAC.
3. User Filter	Otwiera podmenu z ustawieniami filtra użytkowników.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.4.1 Podmenu „Firewall“ > „General Configuration“

To podmenu zawiera ogólne ustawienia funkcji Firewall.

Tabela 231: Podmenu „Firewall“ > „General Configuration“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Firewall enabled entirely	Tu aktywuje się i dezaktywuje wszystkie funkcje firewall.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Firewall jest aktywowany.
	2. Disable Firewall nie jest aktywowany.
2. ICMP echo broadcast protection	Tu aktywuje się i dezaktywuje zabezpieczenie „ICMP echo broadcast“.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Zabezpieczenie „ICMP echo broadcast“ jest aktywowane.
	2. Disable Zabezpieczenie „ICMP echo broadcast“ nie jest aktywowane.
3. Max UDP connections per second	Tu wpisuje się maksymalną liczbę połączeń UDP na sekundę. „0“ = „Disabled“
4. Max TCP connections per second	Tu wpisuje się maksymalną liczbę połączeń TCP na sekundę. „0“ = „Disabled“
5. Interface VPN	Otwiera podmenu z ustawieniami funkcji Firewall na poziomie IP dla wybranego interfejsu.
6. Interface WAN	
7. Interface X1	
8. Interface X2	

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

Aby zastosować ustawienie, kliknąć przycisk **[<OK>]**.

Aby odrzucić ustawienie, kliknąć przycisk **[<Abort>]**.

19.1.2.4.2 Podmenu „General Configuration“ > „Interface xxx“

To podmenu zawiera ustawienia funkcji firewall na poziomie IP dla wybranego interfejsu.

Tabela 232: Podmenu „Firewall“ > „General Configuration“ > „Interface xxx“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Interface state	Tu aktywuje się i dezaktywuje funkcję firewall dla wybranego interfejsu.
	0. Back to ... Powrót do menu nadrzędnego
	1. Open Funkcja firewall dla wybranego interfejsu nie jest aktywna.
	2. Filtered Funkcja firewall dla wybranego interfejsu jest aktywna.
2. ICMP Policy	Tu aktywuje się i dezaktywuje zabezpieczenie „ICMP echo“ dla poszczególnych interfejsów.
	0. Back to ... Powrót do menu nadrzędnego
	1. Accept Zabezpieczenie „ICMP echo“ nie jest aktywne.
	2. Drop Zabezpieczenie „ICMP echo“ jest aktywne.
3. ICMP Limit	Tu wpisuje się maksymalną liczbę „ICMP pings“ na sekundę. „0“ = „Disabled“
4. ICMP Burst	Tu wpisuje się maksymalną liczbę „ICMP echo burst“ na sekundę. „0“ = „Disabled“
5. Telnet	Tu aktywuje się i dezaktywuje funkcję firewall dla poszczególnych usług. Same usługi muszą być włączane i wyłączane osobno przez stronę „Ports and Services“.
6. FTP	
7. FTPS	
8. HTTP	
9. HTTPS	
10. I/O-CHECK	
11. PLC Runtime	
12. PLC WebVisu – direct link (port 8080)	
13. SSH	
14. TFTP	
15. BootP/DHCP	
16. DNS	
17. Modbus TCP	
18. Modbus UDP	
19. SNMP	

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.
Aby zastosować ustawienie, kliknąć przycisk **[<OK>]**.
Aby odrzucić ustawienie, kliknąć przycisk **[<Abort>]**.

19.1.2.4.3 Podmenu „Firewall“ > „MAC Address Filter“

To podmenu zawiera ustawienia filtra adresów MAC.

Tabela 233: Podmenu „Firewall“ > „MAC Address Filter“

Punkt menu	Podpunkt menu / znaczenie	
0. Back to ...	Powrót do menu nadrzędnego	
1. Global MAC address filter state	Tu aktywuje się i dezaktywuje globalny filtr adresu MAC.	
	0. Back to ...	Powrót do menu nadrzędnego
	1. Filtered	Globalny filtr adresu MAC jest aktywny.
	2. Open	Globalny filtr adresu MAC jest nieaktywny.
2. MAC address filter whitelist	Otwiera podmenu do edycji „białej listy“ filtrów adresów MAC.	
3. MAC address filter state X1	Tu aktywuje się i dezaktywuje filtr adresu MAC dla interfejsu X1.	
	0. Back to ...	Powrót do menu nadrzędnego
	1. Open	Filtr adresu MAC dla interfejsu X1 jest nieaktywny
	2. Filtered	Filtr adresu MAC dla interfejsu X1 jest aktywny
4. MAC address filter state X2	Tu aktywuje się i dezaktywuje filtr adresu MAC dla interfejsu X2.	
	0. Back to ...	Powrót do menu nadrzędnego
	1. Open	Filtr adresu MAC dla interfejsu X2 jest nieaktywny
	2. Filtered	Filtr adresu MAC dla interfejsu X2 jest aktywny

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.4.4 Podmenu „MAC Address Filter“ > „MAC address filter whitelist“

To podmenu wyświetla wszystkie istniejące filtry.

Tabela 234: Podmenu „Firewall“ > „MAC Address Filter“ > „MAC address filter whitelist“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Add new	Otwiera podmenu umożliwiające dodawanie nowego filtra. Można wpisać 10 filtrów.
2. Previous page	Wyświetla poprzednią stronę listy (jeśli wypełniona jest więcej niż jedna strona).
3. Next Page	Wyświetla następną stronę listy (jeśli wypełniona jest więcej niż jedna strona).
(n + 3.) No (n):	Otwiera podmenu umożliwiające edycję istniejącego filtra.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [**Q**].

19.1.2.4.5 Podmenu „MAC address filter whitelist“ > „Add new / No (n)“

W tym podmenu można tworzyć filtry, zmieniać je lub usuwać.

Tabela 235: Podmenu „Firewall“ > „MAC Address Filter“ > „MAC address filter whitelist“ > „Add new / No (n)“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. MAC address	Tu wpisuje się adres MAC.
2. MAC mask	Tu wpisuje się maskę MAC.
3. Filter state	Tu aktywuje się i dezaktywuje filtr.
	0. Back to ... Powrót do menu nadrzędnego
	1. on Filtr jest aktywny.
	2. off Filtr nie jest aktywny.
4. accept	Ten punkt menu należy wybrać, aby zastosować zmiany dla wybranego filtra.
5. delete	Ten punkt menu należy wybrać, aby usunąć wybrany filtr.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [**Q**].

Aby zastosować ustawienie, kliknąć przycisk [**<OK>**].

Aby odrzucić ustawienie, kliknąć przycisk [**<Abort>**].

19.1.2.4.6 Podmenu „Firewall“ > „User Filter“

To podmenu wyświetla wszystkie istniejące filtry.

Tabela 236: Podmenu „Firewall“ > „User Filter“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Add new	Otwiera podmenu umożliwiające dodawanie nowego filtra. Można wpisać 10 filtrów.
2. Previous page	Wyświetla poprzednią stronę listy (jeśli wypełniona jest więcej niż jedna strona).
3. Next Page	Wyświetla następną stronę listy (jeśli wypełniona jest więcej niż jedna strona).
(n + 3.) No (n):	Otwiera podmenu umożliwiające edycję istniejącego filtra.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.4.7 Podmenu „User Filter“ > „Add New / No (n)“

W tym podmenu można tworzyć filtry, zmieniać je lub usuwać.

Tabela 237: Podmenu „Firewall“ > „User Filter“ > „Add New / No (n)“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Policy	Tu definiuje się, czy dane urządzenie sieciowe ma być przez filtr dopuszczone czy wykluczone.
	0. Back to ... Powrót do menu nadrzędnego
	1. Allow Urządzenie sieciowe jest dopuszczone.
	2. Drop Urządzenie sieciowe jest wykluczone.
2. Source IP address	Tu wpisuje się źródłowy adres IP.
3. Source netmask	Tu wpisuje się maskę sieci źródłowej.
4. Source port	Tu wpisuje się numer portu źródłowego.
5. Destination IP address	Tu wpisuje się docelowy adres IP.
6. Destination netmask	Tu wpisuje się maskę sieci docelowej.
7. Destination port	Tu wpisuje się numer portu docelowego.
8. Protocol	Tu wybiera się dopuszczalne protokoły.
	0. Back to ... Powrót do menu nadrzędnego
	1. tcp Protokół TCP jest dozwolony.
	2. udp Protokół UDP jest dozwolony.
	3. tcp & udp Oba protokoły są dozwolone.
9. Interface	Tu wybiera się dopuszczalne interfejsy.
	0. Back to ... Powrót do menu nadrzędnego
	1. all Wszystkie interfejsy są dozwolone.
	2. VPN Interfejs VPN jest dozwolony.
	3. WAN Interfejs WAN jest dozwolony.
	4. X1 Interfejs X1 jest dozwolony.
	5. X2 Interfejs X2 jest dozwolony.
10. State	Tu aktywuje się i dezaktywuje filtr.
	0. Back to ... Powrót do menu nadrzędnego
	1. on Filtr jest aktywny.
	2. off Filtr nie jest aktywny.
11. Accept	Ten punkt menu należy wybrać, aby zastosować zmiany dla wybranego filtra.
12. Delete	Ten punkt menu należy wybrać, aby usunąć wybrany filtr.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

Aby zastosować ustawienie, kliknąć przycisk **[<OK>]**.

Aby odrzucić ustawienie, kliknąć przycisk **[<Abort>]**.

19.1.2.5 Menu „Clock“

To menu zawiera dalsze podpunkty menu do ustawiania daty i godziny.

Tabela 238: Menu „Clock“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Date on device (local)	Tu ustawia się datę.
2. Time on device (local)	Tu ustawia się lokalny czas.
3. Time on device (UTC)	Tu ustawia się czas uniwersalny (GMT).
4. Clock Display Mode	Tu wybiera się format zegara.
	0. Back to ... Powrót do menu nadrzędnego
	1. 24 hours Czas wyświetlany jest w formacie 24-godzinnym.
	2. 12 hours Czas wyświetlany jest w formacie 12-godzinnym.
5. Timezone	Tu wybiera się strefę czasową odpowiednią dla danego kraju. Ustawienie podstawowe:
	0. Back to ... Powrót do menu nadrzędnego
	1. AST/ADT „Atlantic Standard Time“, Halifax
	2. EST/EDT „Eastern Standard Time“, New York, Toronto
	3. CST/CDT „Central Standard Time“, Chicago, Winnipeg
	4. MST/MDT „Mountain Standard Time“, Denver, Edmonton
	5. PST/PDT „Pacific Standard Time“, Los Angeles, Whitehouse
	6. GMT/BST Greenwich Mean Time“, GB, P, IRL, IS, ...
	7. CET/CEST „Central European Time“, B, DK, D, F, I, CRO, NL, ...
	8. EET/EEST „East European Time“, BUL, FI, GR, TR, ...
	9. CST „China Standard Time“
	10. JST „Japan/Korea Standard Time“
6. TZ String	W przypadku strefy czasowej, która nie została uwzględniona w parametrach „Timezone“ wpisuje się nazwę danej strefy czasowej lub kraj i miasto, które się w niej znajdują.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [**Q**].

Aby zastosować ustawienie, kliknąć przycisk [**<OK>**].

Aby odrzucić ustawienie, kliknąć przycisk [**<Abort>**].

19.1.2.6 Menu „Administration“

To menu zawiera ustawienia do administracji sterownika.

Tabela 239: Menu „Administration“

Punkt menu	Podpunkt menu / znaczenie	
0. Back to ...	Powrót do menu nadrzędnego	
1. Users	Otwiera podmenu z ustawieniami haseł dla użytkowników.	
2. Create Image	Otwiera podmenu z ustawieniami obrazu bootowalnego.	
3. Reboot Controller	Tu restartuje się sterownik po zapytaniu o potwierdzenie.	
	0. Back to ...	Powrót do menu nadrzędnego
	1. Reboot	Powoduje restart sterownika.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.6.1 Podmenu „Administration“ > „Users“

To podmenu zawiera ustawienia haseł dla użytkowników.

Tabela 240: Podmenu „Administration“ > „Users“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. User	Tu wpisuje się nowe hasło dla użytkownika „user“.
2. Admin	Tu wpisuje się nowe hasło dla użytkownika „admin“.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

Aby zastosować ustawienie, kliknąć przycisk **[<OK>]**.

Aby odrzucić ustawienie, kliknąć przycisk **[<Abort>]**.

19.1.2.6.2 Podmenu „Administration“ > „Create Image“

To podmenu zawiera wybór ustawień obrazu.

Oprócz punktu menu dla aktywnego nośnika pamięci wyświetlany jest aktualny status.

Tabela 241: Podmenu „Administration“ > „Create Image“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. SD Card	Ten punkt menu należy wybrać, aby utworzyć obraz na karcie pamięci. W kolejnym kroku należy podać zarezerwowaną wielkość pamięci. Ten punkt menu widoczny jest tylko wtedy, gdy karta pamięci jest wetknięta.
2. Internal Flash	Ten punkt menu należy wybrać, aby utworzyć obraz w wewnętrznej pamięci.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

Aby zastosować ustawienie, kliknąć przycisk **[<OK>]**.

Aby odrzucić ustawienie, kliknąć przycisk **[<Abort>]**.

19.1.2.7 Menu „Package Server“

To menu zawiera dalsze podpunkty menu z funkcjami „Backup“ i „Restore“ dla firmware oraz informacjami i możliwymi ustawieniami dla aktualnej partycji systemu.

Tabela 242: Menu „Package Server“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Firmware Backup	Otwiera podmenu z funkcją tworzenia kopii zapasowej firmware.
2. Firmware Restore	Otwiera podmenu z funkcją przywracania firmware.
3. System Partition	Otwiera podmenu z informacjami i możliwymi ustawieniami dla aktualnej partycji systemu.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.7.1 Podmenu „Package Server“ > „Firmware Backup“

To podmenu zawiera możliwość wyboru danych do zabezpieczenia.

To podmenu widoczne jest tylko wtedy, gdy wetknięta jest karta pamięci, niezawierająca systemu bootowalnego. W przeciwnym razie wyświetlana jest wskazówka.

Tabela 243: Podmenu „Package Server“ > „Firmware Backup“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. All	Zostają zapisane wszystkie dane.
2. PLC Runtime project	Zostaje zapisany bieżący projekt PLC.
3. Settings	Zostają zapisane ustawienia sterownika.
4. System	Zostaje zapisany system operacyjny sterownika.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

Po dokonaniu wyboru przechodzi się do kolejnego podmenu.

19.1.2.7.2 Podmenu „Firmware Backup“ > „Auto Update Feature“

To podmenu zawiera możliwość ustawienia funkcji automatycznej aktualizacji.

To podmenu widoczne jest tylko wtedy, gdy zostały wybrane dane dla backupu firmware.

Tabela 244: Podmenu „Package Server“ > „Firmware Backup“ > „Auto Update Feature“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. No	Funkcja automatycznej aktualizacji jest wyłączona dla wybranych danych.
2. Yes	Funkcja automatycznej aktualizacji jest włączona dla wybranych danych.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [Q].

Po dokonaniu wyboru przechodzi się do kolejnego podmenu.

19.1.2.7.3 Podmenu „Firmware Backup“ > „Destination“

To podmenu zawiera możliwość wyboru backupu dysku docelowego.

Tabela 245: Podmenu „Package Server“ > „Firmware Backup“ > „Auto Update Feature“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. SD Card	Wybrane dane zostają skopiowane na kartę pamięci.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [Q].

Podczas kopiowania wyświetlany jest postęp tego procesu.

19.1.2.7.4 Podmenu „Package Server“ > „Firmware Restore“

To podmenu zawiera możliwość wyboru przywrócenia dysku źródłowego.

Oprócz aktywnej partycji wyświetlany jest aktualny status.

Tabela 246: Podmenu „Package Server“ > „Firmware Restore“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. SD Card	Dane zostają skopiowane z karty pamięci.
2. Internal Flash	Dane zostają skopiowane z wewnętrznej pamięci.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

Po dokonaniu wyboru przechodzi się do kolejnego podmenu.

19.1.2.7.5 Podmenu „Firmware Restore“ > „Select Package“

To podmenu zawiera możliwość wyboru danych do przywrócenia

Tabela 247: Podmenu „Package Server“ > „Firmware Restore“ > „Select Package“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. PLC Runtime project	Zostaje załadowany bieżący projekt PLC.
2. Settings	Zostają załadowane ustawienia sterownika.
3. System	Zostaje załadowany system operacyjny sterownika.
4. System + Setting	Zostają załadowane ustawienia systemu operacyjnego sterownika i samego sterownika.
5. All	Zostają załadowane wszystkie dane.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

Podczas procesu przywracania wyświetlany jest postęp kopiowania.

19.1.2.7.6 Podmenu „Package Server“ > „System Partition“

To podmenu zawiera informacje i możliwości ustawień dla aktualnej partycji systemu.

Tabela 248: Podmenu „Package Server“ > „System Partition“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Current active partition	Tu wyświetlana jest aktualnie używana partycja.
2. Set inactive NAND partition active	Ten punkt menu należy wybrać, aby przy następnym restarcie sterownika ponownie uruchomić system z innej partycji.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.8 Menu „Mass Storage“

To menu zawiera informacje na temat wewnętrznej pamięci flash oraz zewnętrznej karty pamięci, jeśli została włożona.

Oprócz tego punktu menu przy aktywnej partycji wyświetlany jest status.

Tabela 249: Menu „Mass Storage“

Parametr	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. SD Card	Otwiera podmenu z informacjami na temat karty pamięci i jej formatowania. Ten punkt menu widoczny jest tylko wtedy, gdy karta pamięci jest wetknięta do sterownika.
2. Internal Flash	Otwiera podmenu z informacjami o wewnętrznej pamięci flash.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.8.1 Podmenu „Mass Storage“ > „SD Card“

To podmenu zawiera informacje na temat zewnętrznej karty pamięci i jej formatowania.

To podmenu widoczne jest tylko wtedy, gdy karta pamięci jest wetknięta do sterownika.

Tabela 250: Podmenu „Mass Storage“ > „SD Card“

Parametr	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Show information	Wyświetla informacje na temat karty pamięci.
2. FAT format medium	Ten punkt menu należy wybrać, aby sformatować kartę pamięci w formacie FAT. Zaraz potem należy wpisać nazwę dysku.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

Aby zastosować ustawienie, kliknąć przycisk **[<OK>]**.

Aby odrzucić ustawienie, kliknąć przycisk **[<Abort>]**.

19.1.2.9 Menu „Software Uploads“

To menu zawiera opcje wyboru i ustawienia do aktualizacji urządzenia.

Tu wybiera się np. oprogramowanie do sterowania obiektowego, licencje programowe i skrypty aktualizacji do transmisji z PC do sterownika.

Można tu również aktywować przesłane pakiety lub usunąć je ze sterownika.

19.1.2.10 Menu „Ports and Services“

To menu zawiera dalsze podpunkty menu z ustawieniami poszczególnych usług.

Tabela 251: Menu „Ports and Services“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Telnet	Otwiera podmenu z ustawieniami usługi Telnet.
2. FTP	Otwiera podmenu z ustawieniami usługi FTP.
3. FTPS	Otwiera podmenu z ustawieniami usługi FTPS.
4. HTTP	Otwiera podmenu z ustawieniami usługi HTTP.
5. HTTPS	Otwiera podmenu z ustawieniami usługi HTTPS.
6. NTP	Otwiera podmenu z ustawieniami usługi NTP.
7. SSH	Otwiera podmenu z ustawieniami serwera SSH.
8. TFTP	Otwiera podmenu z ustawieniami serwera TFTP.
9. DHCPD	Otwiera podmenu z ustawieniami usługi DHCPD.
10. DNS	Otwiera podmenu z ustawieniami usługi DNS.
11. IOCHECK PORT	Otwiera podmenu z ustawieniami portu WAGO-I/O-CHECK.
12. Modbus TCP	Otwiera podmenu z ustawieniami usługi Modbus TCP.
13. Modbus UDP	Otwiera podmenu z ustawieniami usługi Modbus UDP.
14. OPC UA	Otwiera podmenu z ustawieniami usługi OPC UA.
15. PLC Runtime Services	Otwiera podmenu z ustawieniami usług systemu runtime PLC.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.10.1 Podmenu „Ports and Services“ > „Telnet“

To podmenu zawiera ustawienia usługi Telnet.

Tabela 252: Podmenu „Ports and Services“ > „Telnet“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. State	Tu można aktywować/dezaktywować usługę Telnet.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Usługa Telnet jest aktywna.
	2. Disable Usługa Telnet nie jest aktywna.
2. Firewall status	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.10.2 Podmenu „Ports and Services“ > „FTP“

To podmenu zawiera ustawienia usługi FTP.

Tabela 253: Podmenu „Ports and Services“ > „FTP“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. State	Tu można aktywować/dezaktywować usługę FTP.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Usługa FTP jest aktywna.
	2. Disable Usługa FTP nie jest aktywna.
2. Firewall status	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.10.3 Podmenu „Ports and Services“ > „FTPS“

To podmenu zawiera ustawienia usługi FTPS.

Tabela 254: Podmenu „Ports and Services“ > „FTPS“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. State	Tu można aktywować/dezaktywować usługę FTPS.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Usługa FTPS jest aktywna.
	2. Disable Usługa FTPS nie jest aktywna.
2. Firewall status	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć [Q].

19.1.2.10.4 Podmenu „Ports and Services“ > „HTTP“

To podmenu zawiera ustawienia usługi HTTP.

Tabela 255: Podmenu „Ports and Services“ > „HTTP“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. State	Tu można aktywować/dezaktywować usługę HTTP.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Usługa HTTP jest aktywna.
	2. Disable Usługa HTTP nie jest aktywna.
2. Firewall status	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć [Q].

19.1.2.10.5 Podmenu „Ports and Services“ > „HTTPS“

To podmenu zawiera ustawienia usługi HTTPS.

Tabela 256: Podmenu „Ports and Services“ > „HTTPS“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. State	Tu można aktywować/dezaktywować usługę HTTPS.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Usługa HTTPS jest aktywna.
	2. Disable Usługa HTTPS nie jest aktywna.
2. Firewall status	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.10.6 Podmenu „Ports and Services“ > „NTP“

To podmenu zawiera ustawienia usługi NTP.

Tabela 257: Podmenu „Ports and Services“ > „NTP“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. State	Tu można aktywować/dezaktywować usługę NTP.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Usługa NTP jest aktywna.
	2. Disable Usługa NTP nie jest aktywna.
2. Port	Tu wpisuje się numer portu serwera NTP.
3. Time Server 1	Tu wpisuje się adresy IP maksymalnie 4 serwerów czasu. Serwer czasowy nr 1 odpytywany jest jako pierwszy. Jeśli nie można pobrać danych z serwera czasowego nr 1, odpytywany jest serwer nr 2, itd.
4. Time Server 2	
5. Time Server 3	
6. Time Server 4	
7. Update Time	Tu definiuje się interwał czasowy aktualizacji serwera czasu.
8. Issue immediate update	Ten punkt menu należy wybrać, aby aktualizować godzinę od razu i niezależnie od interwału czasowego.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

Aby zastosować ustawienie, kliknąć przycisk **[<OK>]**.

Aby odrzucić ustawienie, kliknąć przycisk **[<Abort>]**.

19.1.2.10.7 Podmenu „Ports and Services“ > „SSH“

To podmenu zawiera ustawienia usługi SSH.

Tabela 258: Podmenu „Ports and Services“ > „SSH“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. State	Tu włączą się i wyłączą serwer SSH.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Serwer SSH jest aktywny.
	2. Disable Serwer SSH nie jest aktywny.
2. Port	Tu wpisuje się numer portu.
3. Allow root login	Tu blokuje się lub zezwala na dostęp do katalogu głównego.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Dostęp do katalogu głównego jest dozwolony.
	2. Disable Dostęp do katalogu głównego nie jest dozwolony.
4. Allow password login	Tu aktywuje się i dezaktywuje pytanie o hasło.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Zapytanie o hasło jest aktywne.
	2. Disable Zapytanie o hasło nie jest aktywne.
5. Status of firewalling	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.10.8 Podmenu „Ports and Services“ > „TFTP“

To podmenu zawiera ustawienia usługi TFTP.

Tabela 259: Podmenu „Ports and Services“ > „TFTP“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. State	Tu aktywuje się i dezaktywuje serwer TFTP.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Serwer TFTP jest aktywny.
	2. Disable Serwer TFTP nie jest aktywny.
2. Transfer Directory	Tu wpisuje się ścieżkę do katalogu download serwera.
3. Status of firewalling	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

Aby zastosować ustawienie, kliknąć przycisk [**<OK>**].

Aby odrzucić ustawienie, kliknąć przycisk [**<Abort>**].

19.1.2.10.9 Podmenu „Ports and Services“ > „DHCPD“

To podmenu zawiera ustawienia usługi DHCPD.

Tabela 260: Podmenu „Ports and Services“ > „DHCPD“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. DHCPD firewalling	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.
2. X1	Otwiera podmenu z ustawieniami DHCPD dla wybranego interfejsu.
3. X2	

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [**Q**].

19.1.2.10.10 Podmenu „DHCPD“ > „Xn“

To podmenu zawiera ustawienia usługi DHCPD dla wybranego interfejsu.

Tabela 261: Podmenu „Ports and Services“ > „DHCPD“ > „Xn“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. State	Tu można aktywować/dezaktywować usługę DHCPD dla interfejsu Xn.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Usługa DHCPD jest aktywna.
	2. Disable Usługa DHCPD nie jest aktywna.
2. Range	Tu należy wpisać zakres dostępnych adresów IP.
3. Lease Time (min)	Tu wpisuje się czas dzierżawy w sekundach. Jako wartość standardowa wpisane jest 120 sekund.
4. Add static hostname	Tu wpisuje się nowe przyporządkowanie statyczne MAC-ID do adresu IP, np. „01:02:03:04:05:06=192.168.1.20“ lub „hostname=192.168.1.20“. Można wpisać 10 przyporządkowań.
(5 + n). Static Host (n)	Tu wyświetlane są statyczne przyporządkowania.
	0. Back to ... Powrót do menu nadrzędnego
	1. Edit Otwiera podmenu umożliwiające zmianę wybranego przyporządkowania.
	2. Delete Usuwa wybrane przyporządkowanie

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [**Q**].

Aby zastosować ustawienie, kliknąć przycisk [**<OK>**].

Aby odrzucić ustawienie, kliknąć przycisk [**<Abort>**].

19.1.2.10.11 Podmenu „Ports and Services“ > „DNS“

To podmenu zawiera ustawienia usługi DNS.

Tabela 262: Podmenu „Ports and Services“ > „DNS“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. State	Tu można aktywować/dezaktywować usługę DNS.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Usługa DNS jest aktywna.
	2. Disable Usługa DNS nie jest aktywna.
2. Mode	Tu wybiera się typ pracy serwera DNS.
	0. Back to ... Powrót do menu nadrzędnego
	1. Proxy W celu optymalizacji przepustowości komunikacji zapytania są buforowane.
	2. Relay Wszystkie zapytania są przesyłane bezpośrednio dalej.
3. Firewall status	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.
4. Add static hostname	Tu wpisuje się nowe przyporządkowanie statyczne adresu IP do nazwy hosta, np. „192.168.1.20:hostname“. Można wpisać 10 przyporządkowań.
(5 + n). Static Host (n)	Tu wyświetlane są statyczne przyporządkowania.
	0. Back to ... Powrót do menu nadrzędnego
	1. Edit Otwiera podmenu umożliwiające zmianę wybranego przyporządkowania.
	2. Delete Usuwa wybrane przyporządkowanie

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

Aby zastosować ustawienie, kliknąć przycisk **[<OK>]**.

Aby odrzucić ustawienie, kliknąć przycisk **[<Abort>]**.

19.1.2.10.12 Podmenu „Ports and Services“ > „IOCHECK PORT“

To podmenu zawiera ustawienia portu WAGO-I/O-CHECK.

Tabela 263: Podmenu „Ports and Services“ > „IOCHECK PORT“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. State	Tu można aktywować/dezaktywować port WAGO-I/O-CHECK.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Port WAGO-I/O-CHECK jest aktywny.
	2. Disable Port WAGO-I/O-CHECK nie jest aktywny.
2. Firewall status	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.10.13 Podmenu „Ports and Services“ > „Modbus TCP“

To podmenu zawiera ustawienia usługi Modbus TCP.

Tabela 264: Podmenu „Ports and Services“ > „Modbus TCP“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. State	Tu można aktywować/dezaktywować usługę Modbus/TCP.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Usługa Modbus TCP jest aktywna.
	2. Disable Usługa Modbus TCP nie jest aktywna.
2. Firewall status	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.10.14 Podmenu „Ports and Services“ > „Modbus UDP“

To podmenu zawiera ustawienia usługi Modbus UDP.

Tabela 265: Podmenu „Ports and Services“ > „Modbus UDP“

Punkt menu	Podpunkt menu / znaczenie	
0. Back to ...	Powrót do menu nadrzędnego	
1. State	Tu można aktywować/dezaktywować usługę Modbus UDP.	
	0. Back to ...	Powrót do menu nadrzędnego
	1. Enable	Usługa Modbus UDP jest aktywna.
	2. Disable	Usługa Modbus UDP nie jest aktywna.
2. Firewall status	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.	

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.10.15 Podmenu „Ports and Services“ > „OPC UA“

To podmenu zawiera ustawienia usługi OPC UA.

Tabela 266: Podmenu „Ports and Services“ > „OPC UA“

Punkt menu	Podpunkt menu / znaczenie	
0. Back to ...	Powrót do menu nadrzędnego	
1. State	Tu można aktywować/dezaktywować usługę OPC UA.	
	0. Back to ...	Powrót do menu nadrzędnego
	1. Enable	Usługa OPC UA jest aktywna.
	2. Disable	Usługa OPC UA nie jest aktywna.
2. Firewall status	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.	

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.10.16 Podmenu „...” > „Firewall Status“

To podmenu zawiera ustawienia funkcji Firewall dla wybranej usługi.

Tabela 267: Podmenu „Ports and Services“ > „...” > „Firewall Status“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. VPN	Tu aktywuje się i dezaktywuje funkcję firewall dla interfejsu VPN i danej usługi.
	0. Back to ... Powrót do menu nadrzędnego
	1. open Wymiana danych przez interfejs VPN jest dozwolona.
	2. close Wymiana danych przez interfejs VPN jest wstrzymana.
2. WAN	Tu aktywuje się i dezaktywuje funkcję firewall dla interfejsu WAN i danej usługi.
	0. Back to ... Powrót do menu nadrzędnego
	1. open Wymiana danych przez interfejs WAN jest dozwolona.
	2. close Wymiana danych przez interfejs WAN jest wstrzymana.
3. X1	Tu aktywuje się i dezaktywuje funkcję firewall dla interfejsu X1 i danej usługi.
	0. Back to ... Powrót do menu nadrzędnego
	1. open Wymiana danych przez interfejs X1 jest dozwolona.
	2. close Wymiana danych przez interfejs X1 jest wstrzymana.
4. X2	Tu aktywuje się i dezaktywuje funkcję firewall dla interfejsu X2 i danej usługi.
	0. Back to ... Powrót do menu nadrzędnego
	1. open Wymiana danych przez interfejs X2 jest dozwolona.
	2. close Wymiana danych przez interfejs X2 jest wstrzymana.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.10.17 Podmenu „Ports and Services“ > „PLC Runtime Services“

To podmenu zawiera ustawienia usług systemu runtime PLC

Tabela 268: Podmenu „Ports and Services“ > „PLC Runtime Services“

Punkt menu	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. General Configuration	Tu należy podać hasło dla uwierzytelnienia portu.
2. CODESYS 2	Otwiera podmenu z ustawieniami usług dla CODESYS V2
3. e!RUNTIME	Otwiera podmenu z ustawieniami usług dla e!RUNTIME
4. Change CODESYS Runtime firewalling settings	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.
5. Change CODESYS WebVisu firewalling settings	Otwiera podmenu z ustawieniami funkcji firewall dla interfejsów.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [**Q**].

Aby zastosować ustawienie, kliknąć przycisk [**<OK>**].

Aby odrzucić ustawienie, kliknąć przycisk [**<Abort>**].

19.1.2.10.18 Podmenu „PLC Runtime Services“ > „CODESYS 2“

To podmenu zawiera ustawienia usługi CODESYS V2.

Tabela 269: Podmenu „Ports and Services“ > „PLC Runtime Services“ > „CODESYS 2“

Punkt menu	Podpunkt menu / znaczenie	
0. Back to ...	Powrót do menu nadrzędnego	
1. Webserver enable/disable	Tu aktywuje się i dezaktywuje serwer WWW dla wizualizacji WWW CODESYS V2.	
	0. Back to ...	Powrót do menu nadrzędnego
	1. Enable	Serwer WWW jest aktywny.
	2. Disable	Serwer WWW nie jest aktywny.
2. Communication enable/disable	Tu aktywuje się i dezaktywuje komunikację między systemem runtime CODESYS V2 i środowiskiem programistycznym CODESYS V2.	
	0. Back to ...	Powrót do menu nadrzędnego
	1. Enable	Komunikacja jest możliwa.
	2. Disable	Komunikacja jest zablokowana.
3. Communication Port Number	Tu wpisuje się numer portu do komunikacji ze środowiskiem programistycznym CODESYS V2. Standardowa wartość wynosi 2455.	
4. Port Authentication enable/disable	Tu definiuje się, czy dla połączenia z urządzeniem wymagany jest Log-in.	
	0. Back to ...	Powrót do menu nadrzędnego
	1. Enable	Wymagane jest uwierzytelnienie przez Log-in.
	2. Disable	Nie jest wymagane uwierzytelnienie przez Log-in.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

Aby zastosować ustawienie, kliknąć przycisk **[<OK>]**.

Aby odrzucić ustawienie, kliknąć przycisk **[<Abort>]**.

19.1.2.10.19 Podmenu „PLC Runtime Services“ > „e!RUNTIME“

To podmenu zawiera ustawienia usługi **e!RUNTIME**.

Tabela 270: Podmenu „Ports and Services“ > „PLC Runtime Services“ > „e!RUNTIME“

Punkt menu	Podpunkt menu / znaczenie	
0. Back to ...	Powrót do menu nadrzędnego	
1. Webserver enable/disable	Tu aktywuje się i dezaktywuje serwer WWW e!RUNTIME dla wizualizacji sieciowej.	
	0. Back to ...	Powrót do menu nadrzędnego
	1. Enable	Serwer WWW jest aktywny.
	2. Disable	Serwer WWW nie jest aktywny.
2. Port Authentication enable/disable	Tu definiuje się, czy dla połączenia z urządzeniem wymagany jest Log-in.	
	0. Back to ...	Powrót do menu nadrzędnego
	1. Enable	Wymagane jest uwierzytelnienie przez Log-in.
	2. Disable	Nie jest wymagane uwierzytelnienie przez Log-in.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.1.2.11 Menu „SNMP“

To menu zawiera dalsze podpunkty menu z ustawieniami SNMP.

Tabela 271: Menu „SNMP“

Parametr	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. General SNMP Configuration	Otwiera podmenu z ogólnymi ustawieniami SNMP.
2. SNMP v1/v2c Manager Configuration	Otwiera podmenu z ustawieniami managera SNMP v1/v2c.
3. SNMP v1/v2c Trap Receiver Configuration	Otwiera podmenu z ustawieniami odbiorców komunikatów trap SNMP v1/v2c
4. SNMP v3 Configuration	Otwiera podmenu z ustawieniami do konfiguracji SNMP v3.
5. SNMP firewalling	Otwiera podmenu z ustawieniami funkcji firewall dla SNMP.
6. Secure SNMP firewalling	

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [**Q**].

19.1.2.11.1 Podmenu „SNMP“ > „General SNMP Configuration“

To podmenu zawiera ogólne ustawienia SNMP.

Tabela 272: Podmenu „SNMP“ > „General SNMP Configuration“

Parametr	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. SNMP status	Tu można aktywować lub dezaktywować usługę SNMP.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Usługa SNMP jest aktywna.
	2. Disable Usługa SNMP nie jest aktywna.
2. Name of device	Tu wpisuje się nazwę urządzenia (sysName).
3. Description	Tu wpisuje się opis urządzenia (sysDescription).
4. Physical location	Tu wpisuje się lokalizację urządzenia (sysLocation).
5. Contact	Tu wpisuje się adres kontaktowy e-mail (sysContact).

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [**Q**].

Aby zastosować ustawienie, kliknąć przycisk [**<OK>**].

Aby odrzucić ustawienie, kliknąć przycisk [**<Abort>**].

19.1.2.11.2 Podmenu „SNMP“ > „SNMP v1/v2c Manager Configuration“

To podmenu zawiera ogólne ustawienia managera SNMP v1/v2c.

Tabela 273: Podmenu „SNMP“ > „SNMP v1/v2c Manager Configuration“

Parametr	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. Protocol state	Tu można aktywować lub dezaktywować usługę SNMP v1/v2c.
	0. Back to ... Powrót do menu nadrzędnego
	1. Enable Protokół SNMP v1/v2c jest aktywny.
	2. Disable Protokół SNMP v1/v2c nie jest aktywny.
2. Local community name	Tu wpisuje się nazwę Community do konfiguracji managera SNMP (maks. 32 znaki, bez spacji).

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [**Q**].

Aby zastosować ustawienie, kliknąć przycisk [**<OK>**].

Aby odrzucić ustawienie, kliknąć przycisk [**<Abort>**].

19.1.2.11.3 Podmenu „SNMP“ > „SNMP v1/v2c Trap Receiver Configuration“

To podmenu zawiera ustawienia odbiorców komunikatów trap SNMP v1/v2c.

Tabela 274: Podmenu „SNMP“ > „SNMP v1/v2c Trap Receiver Configuration“

Parametr	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
(n). Trap Receiver (n)	Otwiera podmenu z informacjami o wybranym odbiorcy komunikatów trap v1/v2c i możliwością usunięcia go.
(n + 1). Add new Trap Receiver	Otwiera szereg podpunktów menu do tworzenia nowego odbiorcy komunikatów trap v1/v2c Można wpisać 10 pozycji. Możliwe są następujące warianty: • adres IP nowego odbiorcy komunikatów trap (Managementstation), • nazwa Community do konfiguracji nowego odbiorcy komunikatów trap (maks. 32 znaki, bez spacji), • wersja SNMP, przez którą powinny być wysyłane komunikaty trap (v1 lub v2c).

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [**Q**].

Aby zastosować ustawienie, kliknąć przycisk [**<OK>**].

Aby odrzucić ustawienie, kliknąć przycisk [**<Abort>**].

19.1.2.11.4 Podmenu „SNMP“ > „SNMP v3 Configuration“

To podmenu zawiera ustawienia SNMP v3.

Tabela 275: Podmenu „SNMP“ > „SNMP v3 Configuration“

Parametr	Znaczenie
0. Back to ...	Powrót do menu nadrzędnego
(n). Username	Otwiera podmenu z informacjami o wybranym użytkowniku v3 i możliwości usunięcia go.
(n + 1). Add new v3 User	Otwiera szereg podpunktów menu do tworzenia nowego użytkownika v3 Można wpisać 10 użytkowników. Możliwe są następujące warianty: • nazwa uwierzytelnienia (nazwa może zawierać min. 8 i maks. 32 znaki, w tym małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9), znaki specjalne !()*~'._, ale nie może zawierać spacji), • typ uwierzytelnienia (None/MD5/SHA), • klucz uwierzytelnienia (klucz może zawierać min. 8 i maks. 32 znaki, w tym małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9), znaki specjalne !()*~'._, ale nie może zawierać spacji), • typ prywatności (None/DES/AES), • klucz prywatności (klucz może zawierać min. 8 i maks. 32 znaki, w tym małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9), znaki specjalne !()*~'._, ale nie może zawierać spacji), • adres IP odbiorcy komunikatów trap dla v3.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.

Aby wrócić do menu nadrzędnego, nacisnąć [**Q**].

Aby zastosować ustawienie, kliknąć przycisk [**<OK>**].

Aby odrzucić ustawienie, kliknąć przycisk [**<Abort>**].

19.1.2.11.5 Podmenu „SNMP“ > „(Secure)SNMP firewalling“

Te podpunkty menu zawierają ustawienia funkcji Firewall dla SNMP.

Tabela 276: Podmenu „SNMP“ > „(Secure)SNMP firewalling“

Punkt menu	Podpunkt menu / znaczenie
0. Back to ...	Powrót do menu nadrzędnego
1. VPN	Tu aktywuje się i dezaktywuje funkcję firewall dla interfejsu VPN i danej usługi.
	0. Back to ... Powrót do menu nadrzędnego
	1. open Wymiana danych przez interfejs VPN jest dozwolona.
	2. close Wymiana danych przez interfejs VPN jest wstrzymana.
2. WAN	Tu aktywuje się i dezaktywuje funkcję firewall dla interfejsu WAN i danej usługi.
	0. Back to ... Powrót do menu nadrzędnego
	1. open Wymiana danych przez interfejs WAN jest dozwolona.
	2. close Wymiana danych przez interfejs WAN jest wstrzymana.
3. X1	Tu aktywuje się i dezaktywuje funkcję firewall dla interfejsu X1 i danej usługi.
	0. Back to ... Powrót do menu nadrzędnego
	1. open Wymiana danych przez interfejs X1 jest dozwolona.
	2. close Wymiana danych przez interfejs X1 jest wstrzymana.
4. X2	Tu aktywuje się i dezaktywuje funkcję firewall dla interfejsu X2 i danej usługi.
	0. Back to ... Powrót do menu nadrzędnego
	1. open Wymiana danych przez interfejs X2 jest dozwolona.
	2. close Wymiana danych przez interfejs X2 jest wstrzymana.

Aby dokonać wyboru, zaznaczyć odpowiedni punkt menu.
Aby wrócić do menu nadrzędnego, nacisnąć **[Q]**.

19.2 Budowa danych procesowych

W przypadku sterownika obraz procesu dla modułów I/O w magistrali systemowej jest zbudowany ze słów (z wyrównaniem do pełnych słów). Wewnętrzne przedstawienie danych, większych niż jeden bajt, odbywa się w formacie Intel.

Poniżej opisano reprezentację modułów I/O WAGO I/O System 750 XTR w obrazie procesu, a także konfigurację wartości procesowych.

UWAGA



Uszkodzenie urządzenia w następstwie błędnego adresowania!

W celu uniknięcia uszkodzeń urządzenia na obiekcie, podczas adresowania modułu I/O w dowolnym miejscu w węźle, należy zawsze uwzględniać dane procesowe wszystkich poprzedzających modułów I/O, zorientowanych bajtowo lub bitowo.

Wskazówka



Brak bezpośredniego dostępu z sieci obiektowej do obrazu procesu modułów I/O!

Potrzebne dane z obrazu procesu magistrali systemowej muszą być wyraźnie zmapowane w programie sterującym na dane w obrazie procesu sieci obiektowej i na odwrót! Bezpośredni dostęp nie jest możliwy!

19.2.1 Moduły wejść dwustanowych

Moduły wejść dwustanowych dostarczają jako wartości w obrazie procesu po jednym bicie na kanał, który informuje o stanie sygnału tego kanału. Bity te są mapowane w obrazie procesu wejść.

Poszczególne moduły wejść dwustanowych składają się z dodatkowego bitu diagnostycznego na kanał w obrazie procesu wejść. Bit diagnostyczny służy do analizy błędu, który wystąpił, np. przerwania przewodu i/lub zwarcia.

Jeżeli w węzle podłączone są również moduły wejść analogowych, dane dwustanowe są zawsze zestawiane w bajty i umieszczane za analogowymi danymi wejściowymi w obrazie procesu wejść.

19.2.1.1 2-kanałowe moduły wejść dwustanowych

Tabela 277: 2-kanałowe moduły wejść dwustanowych

Obraz procesu wejść							
bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
						bit danych DI 2 kanał 2	bit danych DI 1 kanał 1

19.2.1.2 8-kanałowe moduły wejść dwustanowych

Tabela 278: 8-kanałowe moduły wejść dwustanowych

Obraz procesu wejść							
bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
bit danych DI 8 kanał 8	bit danych DI 7 kanał 7	bit danych DI 6 kanał 6	bit danych DI 5 kanał 5	bit danych DI 4 kanał 4	bit danych DI 3 kanał 3	bit danych DI 2 kanał 2	bit danych DI 1 kanał 1

19.2.1.3 16-kanałowe moduły wejść dwustanowych

Tabela 279: 16-kanałowe moduły wejść dwustanowych

Obraz procesu wejść															
bit 15	bit 14	bit 13	bit 12	bit 11	bit 10	bit 9	bit 8	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
bit danych DI 16 kanał 16	bit danych DI 15 kanał 15	bit danych DI 14 kanał 14	bit danych DI 13 kanał 13	bit danych DI 12 kanał 12	bit danych DI 11 kanał 11	bit danych DI 10 kanał 10	bit danych DI 9 kanał 9	bit danych DI 8 kanał 8	bit danych DI 7 kanał 7	bit danych DI 6 kanał 6	bit danych DI 5 kanał 5	bit danych DI 4 kanał 4	bit danych DI 3 kanał 3	bit danych DI 2 kanał 2	bit danych DI 1 kanał 1

19.2.2 Moduły wyjść dwustanowych

Moduły wyjść dwustanowych dostarczają jako wartości w obrazie procesu po jednym bicie na kanał, który informuje o statusie tego kanału. Bity te są mapowane w obrazie procesu wyjść.

Poszczególne moduły wyjść dwustanowych składają się z dodatkowego bitu diagnostycznego na kanał w obrazie procesu wejść. Bit diagnostyczny służy do analizy błędów, który wystąpił, np. przerwania przewodu i/lub zwarcia. W przypadku niektórych modułów I/O muszą zostać zanalizowane dodatkowo bity danych, przy ustawionym bicie diagnostycznym.

Jeżeli w węzle podłączone są również moduły wyjść analogowych, dane dwustanowe są zawsze zestawiane w bajty i umieszczane za analogowymi danymi wyjściowymi w obrazie procesu wyjść.

19.2.2.1 2-kanałowe moduły wyjść dwustanowych

Tabela 280: 2-kanałowe moduły wyjść dwustanowych

Obraz procesu wyjść							
bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
						steruje DO 2 kanał 2	steruje DO 1 kanał 1

19.2.2.2 2-kanałowe moduły wyjść dwustanowych z diagnostyką i danymi wejściowymi

Moduły wyjść dwustanowych, oprócz 2 bitów wartości w obrazie procesu wyjść, dostarczają 2 bity danych przedstawianych w obrazie procesu wejść. Są to przyporządkowane do kanałów bity diagnostyczne, pokazujące przeciążenie, zwarcie lub przerwanie przewodu.

Tabela 281: 2-kanałowe moduły wyjść dwustanowych z diagnostyką i danymi wejściowymi

Obraz procesu wejść							
bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
						bit diagnostyczny S 2 kanał 2	bit diagnostyczny S 1 kanał 1

Obraz procesu wyjść							
bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
						steruje DO 2 kanał 2	steruje DO 1 kanał 1

19.2.2.3 4-kanalowe moduły wyjść dwustanowych

Tabela 282: 4-kanalowe moduły wyjść dwustanowych

Obraz procesu wyjść							
bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
				steruje DO 4 kanał 4	steruje DO 3 kanał 3	steruje DO 2 kanał 2	steruje DO 1 kanał 1

19.2.2.4 4-kanalowe moduły wyjść dwustanowych z diagnostyką i danymi wejściowymi

Moduły wyjść dwustanowych, oprócz 4 bitów wartości w obrazie procesu wyjść, dostarczają 4 bity danych przedstawianych w obrazie procesu wejść. Są to przyporządkowane do kanałów bity diagnostyczne, pokazujące przeciążenie, zwarcie lub przerwanie przewodu.

Tabela 283: 4-kanalowe moduły wyjść dwustanowych z diagnostyką i danymi wejściowymi

Obraz procesu wejść							
bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
				bit diagnostyczny S 4 kanał 4	bit diagnostyczny S 3 kanał 3	bit diagnostyczny S 2 kanał 2	bit diagnostyczny S 1 kanał 1

Bit diagnostyczny S = '0' brak błędu

Bit diagnostyczny S = '1' przerwanie przewodu, zwarcie lub przeciążenie

Obraz procesu wyjść							
bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
				steruje DO 4 kanał 4	steruje DO 3 kanał 3	steruje DO 2 kanał 2	steruje DO 1 kanał 1

19.2.2.5 8-kanalowe moduły wyjść dwustanowych

Tabela 284: 8-kanalowe moduły wyjść dwustanowych

Obraz procesu wyjść							
bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
steruje DO 8 kanał 8	steruje DO 7 kanał 7	steruje DO 6 kanał 6	steruje DO 5 kanał 5	steruje DO 4 kanał 4	steruje DO 3 kanał 3	steruje DO 2 kanał 2	steruje DO 1 kanał 1

19.2.2.6 8-kanalowe moduły wyjść dwustanowych z diagnostyką i danymi wejściowymi

Moduły wyjść dwustanowych, oprócz 8 bitów wartości w obrazie procesu wyjść, dostarczają 8 bity danych przedstawianych w obrazie procesu wejść. Są to przyporządkowane do kanałów bity diagnostyczne, pokazujące przeciążenie, zwarcie lub przerwanie przewodu.

Tabela 285: 8-kanalowe moduły wyjść dwustanowych z diagnostyką i danymi wejściowymi

Obraz procesu wejść							
bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
bit diagnostyczny S 8	bit diagnostyczny S 7	bit diagnostyczny S 6	bit diagnostyczny S 5	bit diagnostyczny S 4	bit diagnostyczny S 3	bit diagnostyczny S 2	bit diagnostyczny S 1
kanal 8	kanal 7	kanal 6	kanal 5	kanal 4	kanal 3	kanal 2	kanal 1

Bit diagnostyczny S = '0' brak błędu

Bit diagnostyczny S = '1' przerwanie przewodu, zwarcie lub przeciążenie

Obraz procesu wyjść							
bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
steruje DO 8	steruje DO 7	steruje DO 6	steruje DO 5	steruje DO 4	steruje DO 3	steruje DO 2	steruje DO 1
kanal 8	kanal 7	kanal 6	kanal 5	kanal 4	kanal 3	kanal 2	kanal 1

19.2.2.7 16-kanalowe moduły wyjść dwustanowych

Tabela 286: 16-kanalowe moduły wyjść dwustanowych

Obraz procesu wyjść															
bit 15	bit 14	bit 13	bit 12	bit 11	bit 10	bit 9	bit 8	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
steruje DO 16	steruje DO 15	steruje DO 14	steruje DO 13	steruje DO 12	steruje DO 11	steruje DO 10	steruje DO 9	steruje DO 8	steruje DO 7	steruje DO 6	steruje DO 5	steruje DO 4	steruje DO 3	steruje DO 2	steruje DO 1
kanal 16	kanal 15	kanal 14	kanal 13	kanal 12	kanal 11	kanal 10	kanal 9	kanal 8	kanal 7	kanal 6	kanal 5	kanal 4	kanal 3	kanal 2	kanal 1

19.2.3 Moduły wejść analogowych

Moduły wejść analogowych dostarczają na kanał 16 bitów wartości pomiarowych oraz 8 bitów sterowania/statusu.

Sterownik wykorzystuje 8 bitów sterowania/statusu tylko wewnętrznie do konfiguracji/parametryzacji (np. przez WAGO-I/O-CHECK).

W obrazie procesu wejść są więc mapowane tylko 16-bitowe wartości pomiarowe na kanał jako słowa (word) w formacie Intel.

Jeżeli w węzle podłączone są również moduły wejść dwustanowych, analogowe dane wejściowe są zawsze umieszczane w obrazie procesu przed dwustanowymi danymi wejściowymi.

Informacja



Informacje na temat budowy bajtu sterowania/statusu

Informacje na temat specjalnej budowy bajtu sterowania/statusu znajdują się w opisie modułu I/O. Podręcznik z opisem każdego modułu I/O można znaleźć na stronie internetowej WAGO: www.wago.com.

19.2.3.1 2-kanałowe moduły wejść analogowych

Tabela 287: 2-kanałowe moduły wejść analogowych

Obraz procesu wejść			
Offset	Nazwa bajtu		Uwaga
	Starszy bajt	Młodszy bajt	
0	D1	D0	wartość pomiarowa kanału 1
1	D3	D2	wartość pomiarowa kanału 2

19.2.3.2 4-kanałowe moduły wejść analogowych

Tabela 288: 4-kanałowe moduły wejść analogowych

Obraz procesu wejść			
Offset	Nazwa bajtu		Uwaga
	Starszy bajt	Młodszy bajt	
0	D1	D0	wartość pomiarowa kanału 1
1	D3	D2	wartość pomiarowa kanału 2
2	D5	D4	wartość pomiarowa kanału 3
3	D7	D6	wartość pomiarowa kanału 4

19.2.3.3 Moduł pomiaru mocy 3-fazowy

Moduły wejść analogowych wykorzystują łącznie 9 bajtów danych użytkowych w obszarze wejść i wyjść obrazu procesu, 6 bajtów danych oraz trzy dodatkowe bajty sterowania/statusu. Przy tym zajętych jest zawsze 6 słów w obrazie procesu (z wyrównaniem do pełnych słów).

Tabela 289: Moduł pomiaru mocy 3-fazowej

Obraz procesu wejść			
Offset	Nazwa bajtu		Uwaga
	Starszy bajt	Młodszy bajt	
0	-	S0	bajt statusu 0
1	D1	D0	słowo danych wejściowych 1
2	-	S1	bajt statusu 1
3	D3	D2	słowo danych wejściowych 2
4	-	S2	bajt statusu 2
5	D5	D4	słowo danych wejściowych 3

Obraz procesu wyjść			
Offset	Nazwa bajtu		Uwaga
	Starszy bajt	Młodszy bajt	
0	-	C0	bajt sterowania 0
1	D1	D0	słowo danych wyjściowych 1
2	-	C1	bajt sterowania 1
3	D3	D2	słowo danych wyjściowych 2
4	-	C2	bajt sterowania 2
5	D5	D4	słowo danych wyjściowych 3

19.2.4 Moduły wyjść analogowych

Moduły wyjść analogowych dostarczają na kanał 16 bitów wartości wyjściowych oraz 8 bitów sterowania/statusu.

Sterownik wykorzystuje 8 bitów sterowania/statusu tylko wewnętrznie do konfiguracji / parametryzacji (np. przez WAGO-I/O-CHECK).

W obrazie procesu wyjść są więc mapowane tylko 16-bitowe wartości pomiarowe na kanał jako słowa (word) w formacie Intel.

Jeżeli w węzle podłączone są również moduły wyjść dwustanowych, dane analogowe są zawsze umieszczane w obrazie procesu wyjść przed danymi dwustanowymi.

Informacja



Informacje na temat budowy bajtu sterowania / statusu

Informacje na temat specjalnej budowy bajtu sterowania/statusu znajdują się w opisie modułu I/O. Podręcznik z opisem każdego modułu I/O można znaleźć na stronie internetowej WAGO: www.wago.com.

19.2.4.1 2-kanałowe moduły wyjść analogowych

Tabela 290: 2-kanałowe moduły wyjść analogowych

Obraz procesu wyjść			
Offset	Nazwa bajtu		Uwaga
	Starszy bajt	Młodszy bajt	
0	D1	D0	wartość wyjściowa kanału 1
1	D3	D2	wartość wyjściowa kanału 2

19.2.4.2 4-kanałowe moduły wyjść analogowych

Tabela 291: 4-kanałowe moduły wyjść analogowych

Obraz procesu wyjść			
Offset	Nazwa bajtu		Uwaga
	Starszy bajt	Młodszy bajt	
0	D1	D0	wartość wyjściowa kanału 1
1	D3	D2	wartość wyjściowa kanału 2
2	D5	D4	wartość wyjściowa kanału 3
3	D7	D6	wartość wyjściowa kanału 4

19.2.5 Funkcyjne moduły I/O

W niektórych modułach I/O oprócz bajtów danych pokazywany jest również bajt sterowania / statusu. Służy on do dwukierunkowej wymiany danych między modułem I/O a nadrzędnym układem sterowania.

Bajt sterowania zapisywany jest przez układ sterowania w module I/O i bajt statusu jest udostępniany przez moduł I/O do układu sterowania. W ten sposób możliwe jest na przykład ustawienie licznika za pomocą bajtu sterowania lub wyświetlanie przekroczenia zakresu w górę i w dół przez bajt statusu.

Bajt sterowania/statusu znajduje się w obrazie procesu zawsze w młodszych bajcie słowa.

Informacja



Informacje na temat budowy bajtu sterowania/statusu

Informacje na temat specjalnej budowy bajtu sterowania/statusu znajdują się w opisie modułu I/O. Podręcznik z opisem każdego modułu I/O znajduje Państwo na stronie internetowej WAGO <http://www.wago.com>.

19.2.5.1 Interfejsy szeregowo z alternatywnym formatem danych

Wskazówka



Obraz procesu zależy od sparametryzowanego trybu pracy!

W dowolnie parametryzowanych modułach I/O można ustawić żądany tryb pracy. W zależności od tego obraz procesu tych modułów I/O jest wówczas taki sam, jak dla odpowiedniego wariantu.

Moduły interfejsu szeregowego, ustawione na standardowy format danych, zajmują łącznie 4 bajty danych użytkowych w obszarze wejść i wyjść obrazu procesu: 3 bajty danych oraz jeden dodatkowy bajt sterowania/statusu. Przy tym zajęte są zawsze 2 słowa w obrazie procesu (z wyrównaniem do pełnych słów).

Tabela 292: Interfejsy szeregowo z alternatywnym formatem danych

Obraz procesu wejść i wyjść				
Offset	Nazwa bajtu		Uwaga	
	Starszy bajt	Młodszy bajt		
0	D0	C/S	bajt danych	bajt sterowania / statusu
1	D2	D1	bajty danych	

19.2.5.2 Moduł interfejsu SSI

Wskazówka



Obraz procesu zależy od sparametryzowanego trybu pracy!

W dowolnie parametryzowanych modułach I/O można ustawić żądany tryb pracy. W zależności od tego obraz procesu tych modułów I/O jest wówczas taki sam, jak dla odpowiedniego wariantu.

Moduły interfejsu SSI ze statusem zajmują łącznie 4 bajty danych użytkowych w obrazie procesu wejść. Przy tym zajęte są zawsze 2 słowa w obrazie procesu (z wyrównaniem do pełnych słów).

Tabela 293: Interfejsy SSI z alternatywnym formatem danych

Obraz procesu wejść			
Offset	Nazwa bajtu		Uwaga
	Starszy bajt	Młodszy bajt	
0	D1	D0	bajty danych
1	D3	D2	

19.2.5.3 Moduł pomiaru odległości i kąta

Moduł interfejsu enkodera przyrostowego zajmuje 6 bajtów danych użytkowych w obszarze wejść i wyjść obrazu procesu: 4 bajty danych i dwa dodatkowe bajty sterowania/statusu. Przy tym zajęte są zawsze 4 słowa w obrazie procesu (z wyrównaniem do pełnych słów).

Tabela 294: Moduł interfejsu enkodera przyrostowego

Obraz procesu wejść i wyjść			
Offset	Nazwa bajtu		Uwaga
	Starszy bajt	Młodszy bajt	
0	-	C0/S0	bajt sterowania/statusu kanału 1
1	D1	D0	wartości danych kanału 1
2	-	C1/S1	bajt sterowania/statusu kanału 2
3	D3	D2	wartości danych kanału 2

19.2.5.4 Liczniki

Tryby pracy:

- „licznik góra/dół / 100 kHz”,
- „licznik góra / wejście bramkujące”,
- „licznik bramkowany czasowo”,
- „pomiar częstotliwości”,
- „licznik góra/dół / wyjścia statusowe (DO)”

Liczniki te zajmują łącznie 5 bajtów danych użytkowych w obszarze wejść i wyjść obrazu procesu: 4 bajty danych oraz jeden dodatkowy bajt sterowania/statusu.

Moduły licznikowe dostarczają 32-bitowe stany licznika.

Przy tym zajęte są zawsze 3 słowa w obrazie procesu (z wyrównaniem do pełnych słów).

Tabela 295: Liczniki

Obraz procesu wejść			
Offset	Nazwa bajtu		Uwaga
	Starszy bajt	Młodszy bajt	
0	-	S	bajt statusu
1	D1	D0	wartość licznika
2	D3	D2	

Obraz procesu wyjść			
Offset	Nazwa bajtu		Uwaga
	Starszy bajt	Młodszy bajt	
0	-	C	bajt sterowania
1	D1	D0	nastawa licznika
2	D3	D2	

Przypadek szczególny: tryb pracy „2 licznik góra / 16 bitów / 5 kHz“

Liczniki te zajmują łącznie 5 bajtów danych użytkowych w obszarze wejść i wyjść obrazu procesu: 4 bajty danych oraz jeden dodatkowy bajt sterowania/statusu. Moduły licznikowe dostarczają na licznik stany 16-bitowe. Przy tym zajęte są zawsze 3 słowa w obrazie procesu (z wyrównaniem do pełnych słów).

Tabela 296: Licznik, tryb pracy „2 licznik góra/16 bitów/5 kHz“

Obraz procesu wejść			
Offset	Nazwa bajtu		Uwaga
	Starszy bajt	Młodszy bajt	
0	-	S	bajt statusu
1	D1	D0	wartość licznika – licznik 1
2	D3	D2	wartość licznika – licznik 2

Obraz procesu wyjść			
Offset	Nazwa bajtu		Uwaga
	Starszy bajt	Młodszy bajt	
0	-	C	bajt sterowania
1	D1	D0	wartość nastawy licznika – licznik 1
2	D3	D2	wartość nastawy licznika – licznik 2

19.2.5.5 Moduł gateway CAN

Rozmiar obrazu procesu bramy CAN można ustawiać w zakresie standardowych wielkości: 8, 12, 16, 20, 24, 32, 40 lub 48 bajtów.

Gateway CAN posiada niecykliczny kanał komunikacyjny (mailbox) w obrazie procesu. Transmitowane są przez niego dane konfiguracyjne, parametryzacyjne i diagnostyczne. Długość pierwszego niecyklicznego kanału można ustawić w zakresie od 2 do maksymalnie x bajtów (x = całkowity rozmiar obrazu procesu – 3). Za nimi znajduje się zakres danych użytkowych CAN. W trybach pracy „Sniffer Mode” i „Transparent Mode” transmitowane są tam telegramy CAN przez mechanizm komunikacyjny „Mailbox 2.0”, a w trybie pracy „Mapped Mode” mogą być tam odzwierciedlane przychodzące i wychodzące telegramy CAN.

Ustawienie trybu pracy, rozmiarów mailboxa i obrazu procesu wprowadza się za pomocą narzędzia do uruchamiania WAGO-I/O-CHECK.

Tabela 297: Gateway CAN

Obraz procesu wejść i wyjść					
Długość obrazu procesu	Offset	Nazwa bajtu		Uwaga	
		Starszy bajt	Młodszy bajt		
8 B	0	K/D_MBX	C0/S0	config/diag mailbox	bajt sterowania / statusu
	1	K/D_MBX / CAN_X	K/D_MBX	config/diag mailbox (1-44 bajty) oraz dane użytkowe CAN mailbox (5-45 bajtów **) lub bajt toggle + dane użytkowe CAN (4-44 bajty) ***	
	2	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
	3	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
12 B	4	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
	5	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
16 B	6	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
	7	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
20 B	8	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
	9	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
24 bajty*	10	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
	11	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
32 B	12	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
	...				
	15	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
40 B	16	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
	...				
	19	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
48 B	20	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
	21	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
	22	K/D_MBX / CAN_X	K/D_MBX / CAN_X		
	23	CAN_X	CAN_X		

*) Nastawa fabryczna

**) Tryb pracy „Sniffer Mode” i tryb pracy „Transparent Mode”

***) Tryb pracy „Mapped Mode”

19.3 Biblioteki CODESYS V2

Dodatkowe funkcje sterownika 750-8213/040-010 dostępne są w bibliotekach.

19.3.1 Biblioteki ogólne

W tym rozdziale omówiono ogólne biblioteki CODESYS, obsługiwane przez sterownik 750-8213/040-010.

19.3.1.1 Biblioteki systemowe CODESYS

Obsługiwane są wszystkie funkcje wymienionych w tabeli bibliotek systemowych CODESYS.

Tabela 298: Biblioteki systemowe CODESYS

Biblioteka	Funkcja	C/IEC61131
Analyzation.lib	Analiza wyrażeń boolowskich	C i IEC61131
AnalyzationNew.lib	Analiza wyrażeń boolowskich	C i IEC61131
lscsf.lib	Przygotowanie domyślnych zmiennych w AS	IEC 61131
NetVarUdp_LIB_V23.lib	Implementacja dla zmiennych sieciowych	IEC 61131
Standard.LIB	Oferuje różne funkcje standardowe	C
SysLibAlarmTrend.lib	Wsparcie dla alarmów i zadań trendu	IEC 61131
SysLibCallback.lib	Do instalacji działań Callback lub Event	C
SysLibDir.lib	Do dostępu do katalogów	C
SysLibDirect.lib	Dostęp do zmiennych przez indexy	C
SysLibEvent.lib	Reakcja na zdarzenia w systemie	C
SysLibFileStream.lib	Przetwarzanie danych za pomocą funkcji ANSI C	C
SysLibGetAddress.lib	Zwraca adresy i wielkości segmentów pamięci	C
SysLibIecTasks.lib	Zarządzanie zadaniami IEC	C
SysLibMem.lib	Zarządzanie pamięcią	C
SysLibPlcCtrl.lib	Kontrola PLC z programu PLC	C
SysLibProjectInfo.lib	Odczyt informacji o projekcie CODESYS	C
SysLibSem.lib	Działanie semaforów	C
SysLibSockets.lib	Działania Socket	C
SysLibSocketsAsync.lib	Działania Socket Asynchron	C
SysLibStr.lib	Funkcje String	C
SysLibTasks.lib	Zarządzanie zadaniami	C
SysLibTime.lib	Zarządzanie zegarem czasu rzeczywistego	C

Tabela 298: Biblioteki systemowe CODESYS

Biblioteka	Funkcja	C/IEC61131
SysLibVisu.lib	Dynamiczna wizualizacja	C
SysTaskInfo.lib	Weryfikacja informacji o zadaniach w trybie online	IEC 61131
Util.lib	Różne operacje logiczne	IEC 61131
Util_no_Real.lib	Różne operacje logiczne	IEC 61131

Więcej informacji o bibliotekach zamieszczono w pomocy online CODESYS IDE.

19.3.1.2 SysLibFile.lib

Sterownik 750-8213/040-010 obsługuje następujące bloki funkcyjne biblioteki „SysLibFile.lib“:

- SysFileClose
- SysFileCopy
- SysFileDelete
- SysFileEOF
- SysFileGetPos
- SysFileGetSize
- SysFileGetTime
- SysFileOpen
- SysFileRead
- SysFileRename
- SysFileSetPos
- SysFileWrite

Wskazówka



Upewnić się, że pliki na pewno zostaną zapisane!

Niezawodny zapis plików na nośniku danych jest możliwy dopiero po wywołaniu bloku funkcyjnego „SysFileClose“.

Więcej informacji zamieszczono w pomocy online CODESYS IDE.

Uwagi dotyczące parametrów bloków funkcyjnych

Przy nazwach plików i katalogów uwzględniana jest pisownia wielką i małą literą!

„test.txt“ ≠ „TEST.TXT“ ≠ „Test.txt“

Znakiem rozdzielającym dla katalogów jest: „/“.

System plików obsługuje:

- ścieżki absolutne, (np. „/media/sd/test.txt“)
- ścieżki względne, (np. „testpath/test.txt“)
- makra (np. „HOME://“, „CARD://“, „TMP://“)

Tabela 299: Możliwe makra dla dostępu do danych

Makro	Bootowanie wewnętrznej pamięci	Bootowanie karty pamięci
HOME://	„/home/codesys/“ (pamięć wewnętrzna NAND)	„/home/codesys/“ (karta pamięci)
CARD://	„/media/sd/“ (karta pamięci)	„/home/codesys/“ (karta pamięci)
TMP://	„/tmp/codesys/“ (pamięć wewnętrzna RAM)	„/tmp/codesys/“ (pamięć wewnętrzna RAM)

19.3.1.3 SysLibFileAsync.lib

Sterownik 750-8213/040-010 obsługuje następujące bloki funkcyjne biblioteki „SysLibFileAsync“:

- SysFileCloseAsync
- SysFileCopyAsync
- SysFileDeleteAsync
- SysFileEOFAsync
- SysFileGetPosAsync
- SysFileGetSizeAsync
- SysFileGetTimeAsync
- SysFileOpenAsync
- SysFileReadAsync
- SysFileRenameAsync
- SysFileSetPosAsync
- SysFileWriteAsync

Wskazówka



Upewnić się, że pliki na pewno zostaną zapisane!

Niezawodny zapis plików na nośniku danych jest możliwy dopiero po wywołaniu bloku funkcyjnego „SysLibFileAsync“.

Więcej informacji zamieszczono w pomocy online CODESYS IDE.

Uwagi dotyczące parametrów bloków funkcyjnych

Przy nazwach plików i katalogów uwzględniana jest pisownia wielką i małą literą!

„test.txt“ ≠ „TEST.TXT“ ≠ „Test.txt“

Znakiem rozdzielającym dla katalogów jest: „/“.

System plików obsługuje:

- ścieżki absolutne, (np. „/media/sd/test.txt“)
- ścieżki względne, (np. „testpath/test.txt“)
- makra (np. „HOME://“, „CARD://“, „TMP://“)

Tabela 300: Możliwe makra dla dostępu do danych

Makro	Bootowanie wewnętrznej pamięci	Bootowanie karty pamięci
HOME://	„/home/codesys/“ (pamięć wewnętrzna NAND)	„/home/codesys/“ (karta pamięci)
CARD://	„/media/sd/“ (karta pamięci)	„/home/codesys/“ (karta pamięci)
TMP://	„/tmp/codesys/“ (pamięć wewnętrzna RAM)	„/tmp/codesys/“ (pamięć wewnętrzna RAM)

19.3.1.4 SysLibRtc.lib

Sterownik 750-8213/040-010 obsługuje następujące bloki funkcyjne biblioteki „SysLibRtc.lib“:

- SysRtcGetHourMode
- SysRtcGetTime
- SysRtcSetTime

Więcej informacji zamieszczono w pomocy online CODESYS IDE.

19.3.1.5 BusDiag.lib

Sterownik 750-8213/040-010 obsługuje następujące bloki funkcyjne biblioteki „BusDiag.lib“:

- DiagGetBusState
- DiagGetState

Dokument z opisem biblioteki oraz zawartych w nich bloków funkcyjnych można pobrać ze strony internetowej www.wago.com.

Zmienne wejściowe „DEVICENUMBER“ funkcji „DiagGetBusState“ i „DiagGetState“ są zależne od urządzenia i sieci obiektowej i dla sterownika „PFC200 G2 2ETH M12 CAN XTR“ (750-8213/040-010) mają wartość:

Tabela 301: Zmienne wejściowe „DEVICENUMBER“

Sieć obiektowa	Wartość
Magistrala systemowa	0
Modbus	1
CANopen	2

19.3.1.6 mod_com.lib

Sterownik 750-8213/040-010 obsługuje następujące bloki funkcyjne biblioteki „mod_com.lib“:

- ADD_PI_INFORMATION

- CRC16
- FBUS_ERROR_INFORMATION
- GET_DIGITAL_INPUT_OFFSET
- GET_DIGITAL_OUTPUT_OFFSET
- KBUS_ERROR_INFORMATION
- MOD_COM_VERSION
- PI_INFORMATION
- SET_DIGITAL_INPUT_OFFSET
- SET_DIGITAL_OUTPUT_OFFSET
- SLAVE_ADDRESS

Dokument z opisem biblioteki oraz zawartych w nich bloków funkcyjnych można pobrać ze strony internetowej www.wago.com.

19.3.1.7 SerComm.lib

Sterownik 750-8213/040-010 obsługuje następujące bloki funkcyjne biblioteki „SerComm.lib“:

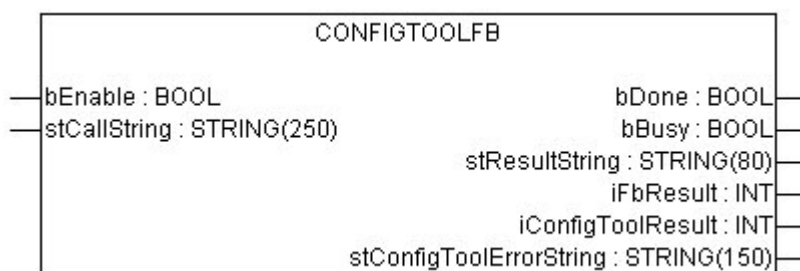
- SERCOMM
- SERCOMM_VERSION

Dokument z opisem biblioteki oraz zawartych w nich bloków funkcyjnych można pobrać ze strony internetowej www.wago.com.

19.3.1.8 WagoConfigToolLIB.lib

Poniższa tabela przedstawia wywołania, które pozwalają na konfigurację i parametryzację sterownika z programu PLC lub Linux® za pomocą bloku funkcyjnego „ConfigToolFB” (patrz parametr „stCallString”). Jest to obok WBM i CBM kolejny wariant konfigurowania sterownika dla dowolnych aplikacji.

Katalog konfiguracji pod Linux® nazywa się: `/etc/config-tools/`



Ilustracja 173: Obraz graficzny bloku funkcyjnego „ConfigToolFB”

Tabela 302: Opis skryptów konfiguracyjnych „Information“

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Controller Details: określa różne informacje o sterowniku				
Product Description	odczyt	get_coupler_details product-description	Opis produktu	od razu
Order Number	odczyt	get_coupler_details order-number	Numer katalogowy sterownika	od razu
Firmware Revision	odczyt	get_coupler_details firmware-revision	Wersja firmware sterownika	od razu
Licence Information	odczyt	get_coupler_details license-information	Informacja o licencji CODESYS	od razu
Network Details X1: określa aktualnie używane parametry interfejsów ETHERNET X1/X2 w trybie „switched“ lub interfejsu ETHERNET X1 w trybie „separated“				
State	odczyt	get_actual_eth_config X1 state	Status interfejsu; możliwe zwracane wartości: - enabled - disabled	od razu
Mac Address	odczyt	get_actual_eth_config X1 mac-address	Adres MAC	od razu
IP Address	odczyt	get_actual_eth_config X1 ip-address	Aktualny adres IP	od razu
Subnet Mask	odczyt	get_actual_eth_config X1 subnet-mask	Aktualna maska podsieci	od razu
Configuration type	odczyt	get_actual_eth_config X1 config-type	Ścieżka, przez którą interfejs uzyskuje swój adres IP; możliwe zwracane wartości: - dhcp - static - bootp	od razu
Cable state	odczyt	get_actual_eth_config X1 cable-state	Status połączenia; możliwe zwracane wartości: - connected - disconnected	od razu
Default gateway	odczyt	get_actual_eth_config X1 default-gateway	Aktualnie zastosowana brama domyślna dla interfejsu X1 (np. gdy brama domyślna została wprowadzona przez serwer DHCP)	od razu
Network Details X2: określa aktualnie używane parametry interfejsu ETHERNET X2 w trybie „separated“				
Patrz „Network Details X1“. Przy wywołaniach zastąpić X1 przez X2 (dopuszczalne tylko w trybie „separated“).				

Tabela 303: Opis skryptów konfiguracyjnych „CODESYS“

Tablica 666: Opis skryptów konfiguracyjnych „CODESYS

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Informacja				
CODESYS Webserver Version	odczyt	get_coupler_details codesys-webserver-version	Wersja serwera WWW CODESYS	od razu
Project Details				
Date	odczyt	get_rts_info project date	Wyświetla informacje o projekcie podane w CODESYS (Menu > Projekt > Informacje o projekcie)	od razu
Title	odczyt	get_rts_info project title		od razu
Version	odczyt	get_rts_info project version		od razu
Author	odczyt	get_rts_info project author		od razu
Description	odczyt	get_rts_info project description		od razu
CODESYS State				
State	odczyt	get_rts_info state	Wyświetla status CODESYS (RUN lub STOP)	od razu
Home Directory (Boot Project Location)				
Home Directory (Boot Project Location)	odczyt	get_runtime_config homedir-on-sdcard	Miejsce zapisu katalogu home; możliwe zwracane wartości: - enabled: katalog home zapisany na karcie SD - disabled: katalog home zapisany na nośniku bootowalnym	po restarcie
	zapis	config_runtime homedir-on-sdcard=<wartość>	Miejsce zapisu katalogu home możliwe wpisy dla wartości: - enabled: zapis katalogu home na karcie SD - disabled: katalog home zapisany na nośniku bootowalnym	
Bootproject Location	odczyt	get_runtime_config boot-project	Miejsce zapisu projektu bootowalnego i aplikacji runtime; możliwe zwracane wartości: - HOME:// (zapis w wewnętrznej pamięci) - CARD:// (zapis na karcie pamięci)	po restarcie
	zapis	config_runtime boot-project=<wartość>	Możliwe wpisy dla <wartość>: - HOME:// (zapis w wewnętrznej pamięci) - CARD:// (zapis na karcie pamięci)	

Tabela 304: Opis skryptów konfiguracyjnych „Networking - Host-/Domainname“

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Host name				
Host name	odczyt	get_coupler_details hostname	Wyświetla nazwę hosta. Wartość zwrótna jest pusta, gdy /etc/hostname jest pusty. patrz parametr „Actual Hostname“.	od razu
	zapis	change_hostname hostname=<String>	Zmiana nazwy hosta; należy podać nazwę hosta dla <String>	od razu
Actual Hostname	odczyt	get_coupler_details actual-hostname	Rzeczywista nazwa hosta (gdy /etc/hostname jest pusty, generowana jest unikatowa nazwa hosta z adresu MAC)	od razu
Domainname				
Domainname	odczyt	get_coupler_details domain-name	Wyświetla nazwę domeny	od razu
	zapis	change_hostname dnsdomain=<String>	Zmiana nazwy domeny; należy podać nazwę domeny dla <String>	

Tabela 305: Opis skryptów konfiguracyjnych „Networking - TCP/IP“

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
IP Address X1: określa parametry IP interfejsów ETHERNET X1/X2 w trybie „switched” lub interfejsu ETHERNET X1 w trybie „separated”				
Type of IP address configuration	odczyt	get_eth_config X1 config-type	Ścieżka, przez którą interfejs uzyskuje swój adres IP; możliwe zwracane wartości: - static (ustawienie statyczne) - dhcp (przez DHC) - bootp (przez BootP)	od razu
	zapis	config_interfaces interface=X1 config-type=<wartość> state=enabled	Metoda, którą interfejs uzyskuje swój adres IP; możliwe wpisy dla <wartość>: - static (ustawienie statyczne) - dhcp (przez DHC) - bootp (przez BootP)	
IP address	odczyt	get_eth_config X1 ip-address	Adres ustawiony dla zastosowania statycznego adresu IP (static IP)	od razu
	zapis	config_interfaces interface=X1 ip-address=<wartość>	Zmiana adresu IP dla IP; <wartość> musi zawierać adres IP w formacie „liczba.liczba.liczba.liczba”.	
Subnet Mask	odczyt	get_eth_config X1 subnet-mask	Maska podsieci ustawiona dla zastosowania statycznego adresu IP (static IP)	od razu
	zapis	config_interfaces interface=X1 subnet-mask=<wartość>	Zmiana maski podsieci dla statycznego adresu IP; <wartość> musi zawierać adres IP w formacie „liczba.liczba.liczba.liczba”	
IP Address X2: określa parametry IP interfejsu ETHERNET X2 w trybie „separated”				
Patrz „IP Address X1” Przy wywołaniach zastąpić X1 przez X2 (dopuszczalne tylko w trybie „separated”).				
Default Gateway 1				
Default Gateway	odczyt	get_default_gateway_ config number=1 state	Aktualny status bramy domyślnej 1; możliwe zwracane wartości: - enabled (włączone) - disabled (wyłączone)	od razu
	zapis	config_default_gatewa y number=1 state=<stateval>	Możliwe wpisy dla <wartość>: - enabled - disabled	
Default Gateway	odczyt	get_default_gateway_ config number=1 value	Aktualny adres IP skonfigurowanej bramy domyślnej 1	od razu
	zapis	config_default_gatewa y number=1 value=<gw>	Tu ustawia się adres IP bramy domyślnej 1; <gw> jest adresem IP w formacie „liczba.liczba.liczba.liczba”	
Default Gateway	odczyt	get_default_gateway_ config number=1 metric	Aktualna metryka (współczynnik kosztu) bramy domyślnej 1; standardowa wartość wynosi „20”	od razu

Tabela 305: Opis skryptów konfiguracyjnych „Networking - TCP/IP“

Tabela 666. Opis skryptów konfiguracyjnych „networking” i „ip”				
Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
	zapis	config_default_gateway y number=1 metric=<n>	Tu ustawia się metrykę bramy domyślnej 1; <n> jest liczbą między „0” a „4.294.967.295”.	
Default Gateway 2				
Patrz „Default Gateway 1”. Przy wywołaniach zastąpić numer bramy 1 przez 2.				
DNS-Server 1				
DNS-Server 1	odczyt	get_dns_server 1	Adres serwera DNS z bieżącym numerem 1	od razu
	zapis / zmiana	edit_dns_server dns-server-nr=1 change=change dns-server-name=<wartość>	Tu ustawia się adres serwera DNS z bieżącym numerem 1; <wartość> jest adresem IP w formacie „liczba.liczba.liczba.liczba”	
	zapis / usunięcie	edit_dns_server dns-server-nr=1 delete=delete	Tu usuwa się serwer DNS z bieżącym numerem 1	
DNS-Server 2 ... n				
Patrz „DNS-Server 1”. Przy wywołaniach dopasować numer serwera (2 ... n).				
Add DNS-Server				
Add DNS-Server	zapis	edit_dns_server add=add dns-server-name=<wartość>	Tu dodaje się kolejne adresy DNS; <wartość> jest adresem IP w formacie „liczba.liczba.liczba.liczba”	od razu

Tabela 306: Opis skryptów konfiguracyjnych „Networking – ETHERNET”

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Switch Configuration				
Interface Mode	odczyt	get_dsa_mode	Odpytywanie statusu konfiguracji switcha: możliwe zwracane wartości: - 0 = tryb „switched” - 1 = tryb „separated”	od razu
	zapis	set_dsa_mode -v <Wert>	Ustawianie konfiguracji switcha: możliwe wpisy dla <wartość>: - 0 = tryb „switched” - 1 = tryb „separated”	
Interface X1				
Port State	odczyt	get_eth_config X1 state	Odpytanie statusu portów: możliwe zwracane wartości: - enabled - disabled	od razu
	zapis	config_ethernet port=X1 state=enabled	Włączanie portu: enabled	
		config_ethernet port=X1 state=disabled	Wyłączanie portu: disabled	
Autonegotiation	odczyt	get_eth_config X1 autoneg	Odpytanie statusu funkcji autonegotiacji: możliwe zwracane wartości: - on - off	od razu
	zapis	config_ethernet port=X1 autoneg=on	Włączenie funkcji autonegotiacji: on	
		config_ethernet port=X1 autoneg=off speed=<Wert> duplex=<Wert>	Wyłączenie funkcji autonegotiacji: off; wskazówka: przy wyłączeniu funkcji autonegotiacji podać wartość Speed i Duplex; możliwe wpisy dla Speed: - 10M - 100M możliwe wpisy dla Duplex: - half - full	
Speed and Duplex Settings	odczyt	get_eth_config X1 speed	Wyświetlenie prędkości ETHERNET	od razu
	odczyt	get_eth_config X1 duplex	Wyświetlenie trybu Duplex	
	zapis	config_ethernet port=X1 autoneg=off speed=<Wert> duplex=<Wert>	Zmiana prędkości ETHERNET i trybu Duplex; możliwe wpisy dla Speed: - 10M - 100M możliwe wpisy dla Duplex: - half - full	
Interface X2				
Patrz „Interface X1”. Przy wywołaniach zastąpić X1 przez X2.				

Tabela 307: Opis skryptów konfiguracyjnych „NTP“

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Configuration Data				
State	odczyt	get_ntp_config state	Odpytanie stanu serwera NTP; możliwe zwracane wartości: - enabled - disabled	od razu
	zapis	config_sntp state=<wartość>	Możliwe wpisy dla <wartość>: - enabled - disabled	
Port	odczyt	get_ntp_config port	Numer portu serwera NTP	od razu
	zapis	config_sntp port=<wartość>	Podanie numer portu dla <wartość>	
Time Server	odczyt	get_ntp_config time-server-<N>	Odpytanie adresu IP dla serwera czasowego: N = 1 ... 4 dla zapytania o jeden z 4 serwerów czasowych.	od razu
	zapis	config_sntp time-server-<N>=<wartość>	Podanie adres IP jednego z 4 serwerów czasowych; <N> może być wartością od 1 do 4; <wartość> zawiera adres IP w formacie „liczba.liczba.liczba.liczba“.	
Update Time (seconds)	odczyt	get_ntp_config update-time	Odpytanie czasu w sekundach między dwoma zapytaniami dla serwera czasowego	od razu
	zapis	config_sntp update-time=<wartość>	Podanie <wartości> cyklu odpytywania (w s) serwera czasowego	

Tabela 308: Opis skryptów konfiguracyjnych „Clock“

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Time and Date				
Date on device, local	odczyt	get_clock_data date-local	Lokalny czas i data	od razu
	zapis	config_clock type=local date=<data>	Zmiana daty; format dla <data>: DD.MM.YYYY	
Time on device, UTC	odczyt	get_clock_data time-utc	Godzina/UTC	od razu
	zapis	config_clock type=utc time=<Time>	Zmiana godziny, w odniesieniu do czasu UTC; format dla <Time>: hh:mm:ss xx	
Time on device, local	odczyt	get_clock_data time-local	Godzina/czas lokalny	od razu
	zapis	config_clock type=local time=<Time>	Zmiana godziny, w odniesieniu do czasu lokalnego; format dla <Time>: hh:mm:ss xx	
12-Hour-Format	odczyt	get_clock_data display-mode	Format zegara 12- lub 24-godzinny; możliwe zwracane wartości: - format 12-godzinny - format 24-godzinny	od razu
	zapis	config_clock _display_mode display-mode=<wartość>	Ustawienie formatu zegara; możliwe wpisy dla <wartość>: - format 12-godzinny - format 24-godzinny	
Timezone				
TZ String	odczyt	get_clock_data tz-string	Aktualnie ustawiona strefa czasowa – oryginalny string TZ jak w systemie operacyjnym	od razu
	zapis	config_timezone tz-string=<string>	Bezpośrednia zmiana stringu TZ; przykład dla <string>: CET-1CEST, M3.5.0/2,M10.5.0/3	

Tabela 309: Opis skryptów konfiguracyjnych „Administration“

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Administration				
Configuration of Service Interface				
Configuration of Service Interface	odczyt	get_service_interface_config mode	użytkownik interfejsu szeregowego active: aktualna możliwa wartość configured: ustawiona wartość, ale nieprzejęta przy restarcie możliwe zwracane wartości to: - service (WAGO-I/O-CHECK, WAGO-I/O-PRO, e!COCKPIT) - linux (konsola Linux®) - free (nieużywane, wolne dla aplikacji)	od razu
	zapis	config_service_interface_config mode=<wartość>	użytkownik interfejsu szeregowego możliwe wpisy dla <wartość> to: - service - linux - free	po restarcie
Reboot Controller				
-	zapis	start_reboot	przeprowadzenie restartu sterownika	od razu

Tabela 310: Opis skryptów konfiguracyjnych „Package Server“

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Firmware Update				
Medium for active partition	odczyt	get_filesystem_data active-partition-medium	Podanie nośnika aktywnej partycji (sd-card, internal-flash-emmc).	od razu
Create firmware backup	zapis	firmware_backup package-settings=<wartość1> package-codesys=<wartość2> package-system=<wartość3> device-medium=<wartość4> auto-update=<wartość5> download-dir=<wartość6>	Tworzenie backupu wybranego pakietu na podanym nośniku; parametry: <wartość1> = 1, gdy ma być wybrany pakiet „Settings“ ; <wartość2> = 1, gdy ma być wybrany pakiet „CODESYS Project“; <wartość3> = 1, gdy ma być wybrany pakiet „System“; <wartość4> = nośnik docelowy do zapisu backupu (sd-card, network); <wartość5> = 1, gdy ma być aktywowany Auto-Update; <wartość6> = katalog docelowy dla pliku backup, gdy jako nośnik docelowy wybrano „network“. Parametry, które nie mają być ustawione (1), można ustawić albo na wartość 0 albo pominąć.	od razu

Tabela 311: Opis skryptów konfiguracyjnych „Ports and Services“ – „Network Sevicees“

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Network Services				
Telnet				
Telnet Port	odczyt	get_port_state telnet	Odczyt statusu serwera Telnet; możliwe zwracane wartości: - enabled - disabled	od razu
	zapis	config_port port=telnet state=<wartość>	Możliwe wpisy dla <wartość>: - enabled - disabled	
FTP				
FTP Port	odczyt	config_ssl ftp-status	Odczyt statusu serwera FTP; możliwe zwracane wartości: - enabled - disabled	od razu
	zapis	config_port port=ftp state=<wartość>	Możliwe wpisy dla <wartość>: - enabled - disabled	

Tabela 311: Opis skryptów konfiguracyjnych „Ports and Services” – „Network Services”

Tablica 6-11. Opis skryptów konfiguracyjnych „*ftps*” i „*https*” i „*http*” dla urządzeń „*Network Devices*”

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
FTPS				
FTPS Port	odczyt	config_ssl ftps-status	Odczyt statusu portu FTPS; możliwe zwracane wartości: - enabled - disabled	od razu
	zapis	config_port port=ftps state=<wartość>	Aktywacja / dezaktywacja FTPS; możliwe wpisy dla <wartość>: - enabled - disabled	
HTTP				
HTTP Port	odczyt	config_ssl http-status	Odczyt statusu portu HTTP; możliwe zwracane wartości: - enabled - disabled	od razu
	zapis	config_port port=http state=<wartość>	Aktywacja / dezaktywacja HTTP; możliwe wpisy dla <wartość>: - enabled - disabled	
HTTPS				
HTTPS Port	odczyt	config_ssl https-status	Odczyt statusu portu HTTPS; możliwe zwracane wartości: - enabled - disabled	od razu
	zapis	config_port port=https state=<wartość>	Aktywacja / dezaktywacja HTTPS; możliwe wpisy dla <wartość>: - enabled - disabled	

Tabela 312: Opis skryptów konfiguracyjnych „Ports and Services” – „PLC Runtime Services”

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
General Settings				
PLC Runtime Version	odczyt	get_runtime_config running-version	Wersja aktywnego systemu runtime PLC; możliwe zwracane wartości: - 0 = runtime nieaktywny, - 2 = CODESYS V2 aktywny - 3 = e!RUNTIME aktywny	od razu
	zapis	config_runtime runtime-version=<„PLC Runtime Services”>	Ustawienie i zatrzymanie dotychczasowej oraz uruchomienie żądanej wersji systemu runtime; możliwe wpisy dla <wartość>: - 0 = brak aktywacji runtime'u - 2 = aktywacja CODESYS V2 - 3 = aktywacja e!RUNTIME	
Default Webpage	odczyt	get_runtime_config default-webpage	Otwiera się strona internetowa przy wpisaniu adresu IP w przeglądarce internetowej; możliwe zwracane wartości: - WBM (Web Based Management) - Webvisu (wizualizacja internetowa)	od razu
	zapis	config_runtime default-webpage=<wartość>	Możliwe wpisy dla <wartość>: - WBM (Web Based Management) - Webvisu (wizualizacja internetowa)	

Tabela 312: Opis skryptów konfiguracyjnych „Ports and Services” – „PLC Runtime Services”

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Change Authentication Password	zapis	config_linux_user user=admin new- password=<wartość> confirm- password=<wartość>	Zmiana hasła systemu runtime PLC	od razu
CODESYS V2 Settings				
CODESYS2 Webserver State	odczyt	get_runtime_config cfg- version=2 webserver- state	Odczyt statusu serwera WWW specyficznego dla systemu runtime; możliwe zwracane wartości: - enabled - disabled	od razu
	zapis	config_runtime cfg- version=2 webserver- state=<wartość>	Włączenie / wyłączenie serwera WWW specyficznego dla systemu runtime; możliwe wpisy dla <wartość>: - enabled - disabled	
CODESYS2 Port Authentication	odczyt	get_runtime_config cfg- version=2 authentication	Odczyt statusu uwierzytelnienia portu dla komunikacji oprogramowania CODESYS V2 PC ze sterownikiem; możliwe zwracane wartości: - enabled - disabled	od razu
	zapis	config_runtime cfg- version=2 authentication=<wartość >	Możliwe wpisy dla <wartość>: - enabled, - disabled	
CODESYS2 Service State	odczyt	get_runtime_config service-state	Odczyt statusu portu dla komunikacji oprogramowania CODESYS V2 PC ze sterownikiem; możliwe zwracane wartości: - enabled - disabled	od razu
	zapis	config_runtime service- state=<wartość>	Możliwe wpisy dla <wartość>: - enabled - disabled	
CODESYS2 Communication Port	odczyt	get_runtime_config comm-port	Odczyt wartości ustawionego portu sieci obiektowej dla komunikacji PC ze sterownikiem; wartość domyślna to 2455	od razu
	zapis	config_runtime comm- port=<wartość>	Zmiana numeru portu; wpisać numer portu TCP/IP dla <wartość>	

Tabela 312: Opis skryptów konfiguracyjnych „Ports and Services” – „PLC Runtime Services”

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
e!Runtime Settings				
e!RUNTIME Webserver State	odczyt	get_runtime_config cfg-version=3 webserver-state	Odczyt statusu serwera WWW specyficznego dla systemu runtime; możliwe zwracane wartości: - enabled - disabled	od razu
	zapis	config_runtime cfg-version=3 webserver-state=<wartość>	Włączenie / wyłączenie serwera WWW specyficznego dla systemu runtime; możliwe wpisy dla <wartość>: - enabled - disabled	
e!RUNTIME Port Authentication	odczyt	get_runtime_config cfg-version=3 authentication	Odczyt statusu uwierzytelnienia portu dla komunikacji oprogramowania e!COCKPIT PC ze sterownikiem; możliwe zwracane wartości: - enabled - disabled	od razu
	zapis	config_runtime cfg-version=3 authentication=<wartość>	Możliwe wpisy dla <wartość>: - enabled - disabled	

Tabela 313: Opis skryptów konfiguracyjnych „Ports and Services” – „SSH/TFTP”

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
SSH				
SSH-Server				
SSH	odczyt	get_ssh_config state	Odczyt statusu portu SSH; możliwe zwracane wartości: - enabled - disabled	od razu
	odczyt	get_ssh_config root-access-state	Zdefiniowanie, czy komunikat jako Root jest dozwolony; możliwe zwracane wartości: - enabled - disabled	
	odczyt	get_ssh_config password-request-state	Zdefiniowanie, czy uwierzytelnienie przez hasło (alternatywnie do PKI) jest dozwolone; możliwe zwracane wartość: - enabled - disabled	
	odczyt	get_ssh_config port-number	Wystawienie portu SSH	
	zapis	config_ssh state=<wartość>	Aktywacja / dezaktywacja serwera SSH; możliwe wpisy dla <wartość>: - enabled - disabled	
	zapis	config_ssh port-number=<wartość>	Ustawienie portu SSH	
	zapis	config_ssh root-access-state-value=<wartość>	Dopuszczenie / niedopuszczenie komunikatu jako Root; możliwe wpisy dla <wartość>: - enabled - disabled	
zapis	config_ssh password-request-state-value=<wartość>	Dopuszczenie / niedopuszczenie uwierzytelnienia przez hasło; możliwe wpisy dla <wartość>: - enabled - disabled		
TFTP				
TFTP-Server				
TFTP	odczyt	get_tftp_config state	Odczyt statusu portu TFTP; możliwe zwracane wartości: - enabled - disabled	od razu
	odczyt	get_tftp_config download-dir	Odczyt katalogu głównego TFTP;	
	zapis	config_tftp state=<wartość>	Aktywacja / dezaktywacja portu TFTP; możliwe wpisy dla <wartość>: - enabled - disabled	
	zapis	config_tftp download-dir=<wartość>	Utworzenie katalogu głównego TFTP	

Tabela 314: Opis skryptów konfiguracyjnych „SNMP“

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Ogólne parametry informacyjne SNMP				
Name of device	odczyt	get_snmp_data device-name	Określenie parametru SNMP „sysName“	od razu
	zapis	config_snmp device-name=<SNMP>	Zmiana parametru SNMP „sysName“ (<wartość> = string). *	po restarcie
Description	odczyt	get_snmp_data description	Określenie parametru SNMP „sysDescr“	od razu
	zapis	config_snmp description=<wartość>	Zmiana parametru SNMP „sysDescr“ (<wartość> = string). *	po restarcie
Physical location	odczyt	get_snmp_data physical-location	Określenie parametru SNMP „sysLocation“	od razu
	zapis	config_snmp physical- location=<wartość>	Zmiana parametru SNMP „sysLocation“ (<wartość> =sString). *	po restarcie
Contact	odczyt	get_snmp_data contact	Określenie parametru SNMP „sysContact“	od razu
	zapis	config_snmp contact=<wartość>	Zmiana parametru SNMP „sysContact“ (<wartość> = string)	po restarcie
* Przy zadawaniu wartość nie należy stosować spacji z „+“ lub „%20“. W przeciwnym razie wpis nie będzie rozpoznany jako przynależny string.				
SNMP-Manager – konfiguracja dla v1 i v2c				
Protocol status	odczyt	get_snmp_data v1-v2c-state	Dostarczenie status protokołu SNMP dla v1/v2c jako string; możliwe wartości zwrotne: - enabled - disabled	od razu
Local Community Name	odczyt	get_snmp_data v1-v2c-community-name	Określenie nazwy Community ustawionej dla v1/v2c	od razu
Protocol Protokoll Status/ Community Name	zapis	config_snmp v1-v2c- state=<wartość1> v1-v2c-community- name=<wartość2>	Aktywacja / dezaktywacja protokołu v1/v2c (<wartość1> = enabled lub disabled) i nadawanie nazwy Community (<wartość2> = string bez spacji, min. 1, maks. 32 znaki). Wskazówka: Przy wymianie nazwa Community nie wymagana; włączenie możliwe tylko przy nadaniu nazwy Community; zapisanie nazwy Community możliwe tylko przy aktywowanym protokole	po restarcie
Konfiguracja SNMP Trap Receiver dla v1 i v2c Można skonfigurować różnych odbiorców komunikatów trap. Założony odbiorca komunikatów trap jest zawsze aktywny, aby go dezaktywować, należy całkowicie usunąć zestaw danych.				

Tabela 314: Opis skryptów konfiguracyjnych „SNMP“

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
IP address of a trap receiver	odczyt	get_snmp_data v1-v2c-trap-receiver-address <numer>	Określa adres IP odbiorcy komunikatów trap, do którego sterownik ma wysłać komunikaty trap v1 lub v2. Parametr <numer> (liczba) służy do natychmiastowego odczytu po kolei przynależnych danych pojedynczych skonfigurowanych odbiorców komunikatów trap (bez zmian danych w międzyczasie). Jest numerem bieżącym, niepowiązanym z danymi. Jeśli numer zostanie opuszczony, odczytywane są dane pierwszego odbiornika.	od razu
Community Name	odczyt	get_snmp_data v1-v2c-trap-receiver-community-name <numer>	Określa nazwę Community, którą wysyła agent SNMP sterownika w nagłówku komunikatu trap. Parametr <numer> (liczba) patrz punkt „Adres IP odbiorcy komunikatów trap“.	od razu
Trap Version	odczyt	get_snmp_data v1-v2c-trap-receiver-version <numer>	Określa wersję SNMP („v1“ lub „v2c“), przez którą agent SNMP wysyła komunikaty trap na przynależny adres odbiorcy komunikatów trap. Parametr <numer> (liczba) patrz punkt „Adres IP odbiorcy komunikatów trap“.	od razu

Tabela 314: Opis skryptów konfiguracyjnych „SNMP“

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Creating/ deleting a trap receiver	zapis	config_snmp v1-v2c-trap-receiver- edit=<wartość1> v1-v2c-trap-receiver- address=<wartość2> v1-v2c-trap-receiver- community- name=<wartość3> v1-v2c-trap-receiver- version=<wartość4>	Dodawanie nowego odbiorcy komunikatów trap (wartość1=add) lub usuwanie skonfigurowanego odbiorcy komunikatów trap (wartość1=delete). Dalsze parametry: <wartość2> = adres IP (liczba.liczba.liczba.liczba), na który sterownik ma wysyłać komunikaty trap. <wartość3>: String Community (String), który sterownik wprowadza do nagłówka komunikatu trap. <wartość4>: wersja SNMP, przez którą wysyłane są komunikaty trap (v1 lub v2c). Wskazówka: Przy usuwaniu odbiorcy komunikatów trap trzeba podać wszystkie parametry, ponieważ tylko dzięki temu zestaw danych można jednoznacznie zidentyfikować.	po restarcie
Konfiguracja SNMP v3 Można skonfigurować dowolną liczbę użytkowników SNMP v3. Założony użytkownik jest zawsze aktywny, aby go dezaktywować, należy całkowicie usunąć zestaw danych.				
Authentication Name	odczyt	get_snmp_data v3-auth-name <numer>	Określa nazwę użytkownika v3. Parametr <numer> służy do natychmiastowego odczytu po kolei przynależnych danych pojedynczych skonfigurowanych odbiorców komunikatów trap (bez zmian danych w międzyczasie). Jest numerem bieżącym, niepowiązanym z danymi. Jeśli numer zostanie opuszczony, odczytywane są dane pierwszego użytkownika..	od razu
Authentication encryption type	odczyt	get_snmp_data v3-auth-type <numer>	Określa typ uwierzytelnienia, którego używa użytkownik v3 (none, MD5 lub SHA). Parametr <numer> patrz punkt „Nazwa uwierzytelnienia“.	od razu
Authentication Key	odczyt	get_snmp_data v3-auth-key <numer>	Określa string klucza dla uwierzytelnienia. Parametr <numer> patrz punkt „Nazwa uwierzytelnienia“.	od razu

Tabela 314: Opis skryptów konfiguracyjnych „SNMP“

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Privacy encryption type	odczyt	get_snmp_data v3-privacy <numer>	Określa typ blokady prywatności dla użytkownika v3 (none, DES lub AES). Parametr <numer> patrz punkt „Nazwa uwierzytelnienia“.	od razu
Privacy Key	odczyt	get_snmp_data v3-privacy-key <numer>	Określa string klucza prywatności. Jeśli tu nie ma żadnej wartości, agent SNMP wykorzysta tu „Authentication Key“. Parametr <numer> patrz punkt „Nazwa uwierzytelnienia“.	od razu
Trap Receiver Adress	odczyt	get_snmp_data v3-notification-receiver <numer>	Adres IP managera SNMP, na który agent wysyła komunikaty trap dla tego użytkownika v3. Jeśli nie ma tu żadnej wartości, dla tego użytkownika nie są wysyłane komunikaty trap. Parametr <numer> patrz punkt „Nazwa uwierzytelnienia“.	od razu

Tabela 314: Opis skryptów konfiguracyjnych „SNMP“

Parametr	Status	Wywołanie	Wejście / wyjście	Ważność
Add new v3-User	zapis	config_snmp v3-edit=add v3-auth-name=<wartość1> v3-auth-type=<wartość2> v3-auth-key=<wartość3> v3-privacy=<wartość4> v3-privacy-key=<wartość5> v3-notification-receiver=<wartość6>	Tworzenie nowego użytkownika v3. Nazwa użytkownika nie mogła być nadana. Parametry: nazwa użytkownika (<wartość1> = string, min. 8 i maks. 32 znaki, w tym małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9), znaki specjalne !()*~'._ ale bez spacji); typ szyfrowania (<wartość2> = none, MD5 lub SHA); wzór stringu dla uwierzytelnienia, (<wartość3> = string, min. 8 i maks. 32 znaki, w tym małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9), znaki specjalne !()*~'._ ale bez spacji) typ szyfrowania prywatności (<wartość4> = none, DES lub AES); wzór stringu prywatności (<wartość5> = string, min. 8 i maks. 32 znaki, w tym małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9), znaki specjalne !()*~'._ ale bez spacji), może być pusty; w tym przypadku zastosowany zostaje klucz uwierzytelnienia. Jako Notification Receiver (<wartość6> = liczba.liczba.liczba.liczba) transmitowany jest adres IP odbiorcy komunikatów trap. Jeśli komunikaty trap v3 nie mają być wysyłane, ten wpis znika.	po restarcie
Delete v3 user	zapis	config_snmp v3-edit=delete v3-auth-name=<wartość>	Usuwanie istniejącego użytkownika v3. Ponieważ przy tworzeniu użytkownika podwójne nadanie tej samej nazwy Usera jest przez skrypt ignorowane, do identyfikacji danych przy usuwaniu wystarczy nazwa (<wartość> = string).	po restarcie

19.3.1.9 WagoLibCpuUsage.lib

Sterownik 750-8213/040-010 obsługuje następujące bloki funkcyjne biblioteki „WagoLibCpuUsage.lib“:

- CPU_Usage

Dokument z opisem biblioteki oraz zawartych w nich bloków funkcyjnych można pobrać ze strony internetowej www.wago.com.

19.3.1.10 WagoLibDiagnosticIDs.lib

Sterownik 750-8213/040-010 obsługuje następujące bloki funkcyjne biblioteki „WagoLibDiagnosticIDs.lib“:

- DIAGNOSTIC_SEND_ID
- DIAGNOSTIC_SET_TEXT_FOR_ID

Dokument z opisem biblioteki oraz zawartych w nich bloków funkcyjnych można pobrać ze strony internetowej www.wago.com.

19.3.1.11 WagoLibLed.lib

Sterownik 750-8213/040-010 obsługuje następujące bloki funkcyjne biblioteki „WagoLibLed.lib“:

- LED_SET_STATIC
- LED_SET_BLINK
- LED_SET_FLASH
- LED_SET_ERROR
- LED_RESET_ERROR
- LED_RESET_ALL_ERRORS
- LED_GET_STATE
- LED_GET_STATE_ASYNC

Dokument z opisem biblioteki oraz zawartych w nich bloków funkcyjnych można pobrać ze strony internetowej www.wago.com.

19.3.1.12 WagoLibNetSnmp.lib

Sterownik 750-8213/040-010 obsługuje następujące bloki funkcyjne biblioteki „WagoLibNetSnmp.lib“:

- snmpGetValueCustomOID_INT32
- snmpGetValueCustomOID_STRING
- snmpGetValueCustomOID_UINT32
- snmpRegisterCustomOID_INT32
- snmpRegisterCustomOID_STRING
- snmpRegisterCustomOID_UINT32
- snmpSetValueCustomOID_INT32
- snmpSetValueCustomOID_STRING

- snmpSetValueCustomOID_UINT32

Dokument z opisem biblioteki oraz zawartych w nich bloków funkcyjnych można pobrać ze strony internetowej www.wago.com.

19.3.1.13 WagoLibNetSnmManager.lib

Sterownik 750-8213/040-010 obsługuje następujące bloki funkcyjne biblioteki „WagoLibNetSnmManager.lib“:

- SNMPM_DINT_TO_TLV
- SNMPM_UDINT_TO_TLV
- SNMPM_STRING_TO_TLV
- SNMPM_TLV_TO_DINT
- SNMPM_TLV_TO_UDINT
- SNMPM_TLV_TO_STRING
- SNMPM_GET
- SNMPM_GET_V3
- SNMPM_SET
- SNMPM_SET_V3

Dokument z opisem biblioteki oraz zawartych w nich bloków funkcyjnych można pobrać ze strony internetowej www.wago.com.

19.3.1.14 WagoLibSSL.lib

Sterownik 750-8213/040-010 obsługuje następujące bloki funkcyjne biblioteki „WagoLibSSL.lib“:

- SSL_CTX
- SSL_CTX_load_verify_locations
- SSL_CTX_sess_set_cache_size
- SSL_CTX_set_client_CA_list
- SSL_CTX_set_method
- SSL_CTX_use_certificate_file
- SSL_CTX_use_PrivateKey_file
- SSL_free
- SSL_get_error
- SSL_Hdshk_Accept
- SSL_Hdshk_Connect
- SSL_load_client_CA_file
- SSL_read
- SSL_shutdown
- SSL_write

Dokument z opisem biblioteki oraz zawartych w nich bloków funkcyjnych można pobrać ze strony internetowej www.wago.com.

19.3.1.15 WagoLibTerminalDiag.lib

Sterownik 750-8213/040-010 obsługuje następujące bloki funkcyjne biblioteki „WagoLibTerminalDiag.lib“:

- GET_TERMINALDIAG

Dokument z opisem biblioteki oraz zawartych w nich bloków funkcyjnych można pobrać ze strony internetowej www.wago.com.

19.3.2 Biblioteki do integracji CANopen i CANLayer2

W tym rozdziale omówiono ogólne biblioteki do integracji CANopen i CANLayer2, obsługiwane przez sterownik 750-8213/040-010.

19.3.2.1 WagoCANLayer2_02.lib

Sterownik 750-8213/040-010 obsługuje następujące moduły biblioteki „WagoCANLayer2_02.lib“:

- CAN_CLOSE
- CAN_ERROR_INFO
- CAN_LAYER2_VERSION
- CAN_OPEN
- CAN_RESET
- CAN_RX_11BIT_FRAME
- CAN_RX_29BIT_FRAME
- CAN_SET_LED
- CAN_TX_11BIT_FRAME
- CAN_TX_29BIT_FRAME

Dokument z opisem biblioteki oraz zawartych w nich bloków funkcyjnych można pobrać ze strony internetowej www.wago.com.

19.3.2.2 WagoCANopen_02.lib

Sterownik 750-8213/040-010 obsługuje następujące moduły biblioteki „WagoCANopen_02.lib“:

- CIA405_GET_KERNEL_STATE
- CIA405_GET_LOCAL_NODE_ID
- CIA405_RECV_EMCY
- CIA405_RECV_EMCY_DEV
- CIA405_GET_STATE
- CIA405_RECV_EMCY_DEV
- CIA405_NMT
- CANOPEN_VERSION
- NMT_GUARD_ERROR
- NMT_GUARD_ERROR_DEV
- CIA405_SDO_WRITE4
- CIA405_SDO_READ4
- CIA405_SDO_WRITEXX
- CIA405_SDO_READXX

Dokument z opisem biblioteki oraz zawartych w nich bloków funkcyjnych można pobrać ze strony internetowej www.wago.com.

19.3.2.3 WagoCANopenDiag.lib

Sterownik 750-8213/040-010 obsługuje następujące moduły biblioteki „WagoCANopenDiag.lib“:

- CANOPEN_DIAG

Dokument z opisem biblioteki oraz zawartych w nich bloków funkcyjnych można pobrać ze strony internetowej www.wago.com.

Spis ilustracji

Ilustracja 1: Widok.....	29
Ilustracja 2: Miejsce na numer produkcyjny	31
Ilustracja 3: Zaciski CAGE CLAMP®	32
Ilustracja 4: Złącze serwisowe (klapka złącza serwisowego opuszczona i uniesiona)	33
Ilustracja 5: Złącza sieciowe – X1, X2	34
Ilustracja 6: Złącze sieci obiektowej CANopen – X3	35
Ilustracja 7: Standardowe złącze sieci CANopen.....	36
Ilustracja 8: Styki magistrali systemowej.....	37
Ilustracja 9: Styki magistrali obiektowej	38
Ilustracja 10: LED dla zasilania	39
Ilustracja 11: LED dla systemu / sieci obiektowej	40
Ilustracja 12: LED gniazda karty pamięci.....	41
Ilustracja 13: LED LNK (obok gniazd M12).....	42
Ilustracja 14: Przełącznik trybu pracy	43
Ilustracja 15: Przycisk resetu.....	44
Ilustracja 16: Gniazdo karty pamięci SC	45
Ilustracja 17: Schemat połączeń wewnętrznych	46
Ilustracja 18: Przykład przyporządkowania interfejsów przez WBM.....	62
Ilustracja 19: 1 bridge z 2 portami.....	64
Ilustracja 20: 2 bridge z portami 1/1.....	64
Ilustracja 21: Podłączenie sterownika do usługi chmury (przykład).....	76
Ilustracja 22: Układ współrzędnych: szerokość (x), wysokość (y), głębokość (z)	86
Ilustracja 23: Pozycje montażu.....	87
Ilustracja 24: Odstępy.....	91
Ilustracja 25: Blokada montażowa sterownika	93
Ilustracja 26: Wkładanie modułu I/O (przykład).....	94
Ilustracja 27: Montaż zatraskowy modułu I/O (przykład)	94
Ilustracja 28: Przykłady rozmieszczenia styków mocy	95
Ilustracja 29: Podłączanie przewodów do CAGE CLAMP®	96
Ilustracja 30: Koncepcja zasilania	99
Ilustracja 31: Przykład zasilania dla interfejsów/sterowników sieciowych XTR..	100
Ilustracja 32: Styk uziemiający (przykład)	103
Ilustracja 33: Ekran przewodu z potencjałem uziemienia.....	104
Ilustracja 34: Obejmy do ekranów na szynie montażowej (przykład)	105
Ilustracja 35: 5 obejm do ekranów na szynie zbiorczej (przykład).....	105
Ilustracja 36: „Open DHCP, przykład widoku“.....	109
Ilustracja 37: Menu główne CBM (przykład)	110
Ilustracja 38: CBM – wybór „Networking“	111
Ilustracja 39: CBM – wybór „TCP/IP“	111
Ilustracja 40: CBM – wybór „IP Address“	111
Ilustracja 41: CBM – wybór adresu IP	112
Ilustracja 42: CBM – wpisywanie nowego adresu IP	112
Ilustracja 43: „WAGO Ethernet Settings“ – ekran startowy (przykład).....	113
Ilustracja 44: „WAGO Ethernet Settings“ – zakładka „Network“	114
Ilustracja 45: Przykład testu działania.....	116
Ilustracja 46: Wpisywanie uwierzytelnienia (przykład)	123

Ilustracja 47: Przypomnienie o konieczności zmiany hasła.....	125
Ilustracja 48: Okno przeglądarki WBM (przykład)	128
Ilustracja 49: Wiesz nagłówek WBM z niewyświetlanymi zakładkami (przykład)	128
Ilustracja 50: Wiersz statusu WBM (przykład)	128
Ilustracja 51: Menu główne CBM (przykład)	130
Ilustracja 52: „WAGO Ethernet Settings” – ekran startowy (przykład).....	134
Ilustracja 53: „WAGO Ethernet Settings” – konfiguracja połączeń komunikacyjnych.....	135
Ilustracja 54: „WAGO Ethernet Settings” – zakładka Identification (przykład) ...	136
Ilustracja 55: „WAGO Ethernet Settings” – zakładka Network	137
Ilustracja 56: „WAGO Ethernet Settings” – zakładka PLC	139
Ilustracja 57: „WAGO Ethernet Settings” – zakładka Status	140
Ilustracja 58: Ustawienia systemu docelowego (1)	142
Ilustracja 59: Ustawienia systemu docelowego (2)	142
Ilustracja 60: Tworzenie nowego bloku funkcyjnego.....	143
Ilustracja 61: Interfejs programowania z blokiem funkcyjnym PLC_PRG	143
Ilustracja 62: Zakładka „Resources”	144
Ilustracja 63: PLC Configuration – Edit.....	144
Ilustracja 64: Przycisk „Start WAGO-I/O-CHECK and scan”	145
Ilustracja 65: WAGO-I/O-CHECK – ekran startowy	145
Ilustracja 66: Pusty konfigurator I/O.....	146
Ilustracja 67: Przycisk „Add I/O Modules”	146
Ilustracja 68: Okno „Module Selection”	147
Ilustracja 69: Konfigurator I/O z wyświetlonymi modułami I/O.....	147
Ilustracja 70: Deklaracja zmiennych	148
Ilustracja 71: Konfiguracja sterownika: moduły I/O z przydzielonymi adresami.	148
Ilustracja 72: Function block.....	149
Ilustracja 73: Asystent deklaracji zmiennych (Input assistant)	149
Ilustracja 74: Przykład przypisywania zmiennej	150
Ilustracja 75: Nawiązywanie połączenia komunikacyjnego – krok 1.....	151
Ilustracja 76: Nawiązywanie połączenia komunikacyjnego – krok 2.....	152
Ilustracja 77: Nawiązywanie połączenia komunikacyjnego – krok 3.....	152
Ilustracja 78: Task configuration	154
Ilustracja 79: Zmiana nazwy zadania 1	155
Ilustracja 80: Wywołanie dołączenia bloku funkcyjnego.....	156
Ilustracja 81: Zadanie cykliczne.....	157
Ilustracja 82: Zadanie dowolne.....	158
Ilustracja 83: Debugowanie (przypadek 1).....	159
Ilustracja 84: Debugowanie (przypadek 2).....	159
Ilustracja 85: Debugowanie (przypadek 3).....	160
Ilustracja 86: Debugowanie (przypadek 4).....	160
Ilustracja 87: Debugowanie (przypadek 5).....	161
Ilustracja 88: Debugowanie (przypadek 6).....	161
Ilustracja 89: Debugowanie (przypadek 7).....	162
Ilustracja 90: CODESYS – System Events	163
Ilustracja 91: CODESYS – program wywołujący dzielenie przez „0”	165
Ilustracja 92: CODESYS – tworzenie i aktywowanie zdarzeń	165
Ilustracja 93: CODESYS – wygenerowany nowy moduł	166
Ilustracja 94: CODESYS – zapisanie zdarzenia w zmiennych globalnych	166

Ilustracja 95: CODESYS – zawartość zmiennych przed dzieleniem przez „0” ..	167
Ilustracja 96: CODESYS – zawartość zmiennych po dzieleniu przez „0”	167
Ilustracja 97: Obraz procesu.....	168
Ilustracja 98: Zakres znaczników.....	169
Ilustracja 99: Synchronizacja magistrali systemowej (przypadek 1).....	173
Ilustracja 100: Synchronizacja magistrali systemowej (przypadek 2).....	175
Ilustracja 101: Synchronizacja magistrali systemowej (przypadek 3).....	176
Ilustracja 102: Synchronizacja magistrali systemowej (przypadek 4).....	177
Ilustracja 103: Ustawienia magistrali systemowej	178
Ilustracja 104: Pamięć programu (przykład)	181
Ilustracja 105: Pamięć danych i ograniczenie modułu (przykład).....	182
Ilustracja 106: Pamięć RAM nieulotna (przykład)	183
Ilustracja 107: Pamięć znaczników i Retain (przykład)	183
Ilustracja 108: Ogólne ustawienia systemu docelowego.....	184
Ilustracja 109: Wybór wariantu wizualizacji w ustawieniach systemu docelowego.....	185
Ilustracja 110: Tworzenie strony startowej wizualizacji PLC_VISU	186
Ilustracja 111: Pamięć RAM nieulotna	194
Ilustracja 112: Konfiguracja sterownika w CODESYS – ustawienia Modbus	196
Ilustracja 113: Obraz procesu Modbus	201
Ilustracja 114: Zakres znaczników	202
Ilustracja 115: Diagram stanów, tryb pracy STANDARD_WATCHDOG	212
Ilustracja 116: Diagram stanów, tryb pracy ALTERNATIVE_WATCHDOG	213
Ilustracja 117: Diagram ilustrujący możliwe stany przy przełączaniu trybów pracy	214
Ilustracja 118: Przegląd adresów Modbus	223
Ilustracja 119: Diagram stanów, tryb pracy ADVANCED_WATCHDOG	226
Ilustracja 120: Diagram stanów, tryb pracy SIMPLE_WATCHDOG	227
Ilustracja 121: Diagram ilustrujący możliwe stany przy przełączaniu trybów pracy	227
Ilustracja 122: Zależność między zmiennymi „IEC 61131-3” i PFC.....	245
Ilustracja 123: Dodawanie CANopen master	249
Ilustracja 124: Zakładka parametrów bazowych (master)	250
Ilustracja 125: Zakładka parametrów CAN (master)	251
Ilustracja 126: Zakładka parametrów modułu (master)	252
Ilustracja 127: Dodawanie urządzeń CANopen slave	254
Ilustracja 128: Zakładka parametrów bazowych (slave).....	254
Ilustracja 129: Zakładka „CAN parameters” (slave	256
Ilustracja 130: Zakładka „CAN Module Selection”	259
Ilustracja 131: Zakładka „PDO-Mapping”	260
Ilustracja 132: Okno właściwości PDO	261
Ilustracja 133: Zakładka „Service Data Objects”	263
Ilustracja 134: Dostosowanie SDO	264
Ilustracja 135: Zakładka „Module parameters” (slave)	265
Ilustracja 136: Dodawanie CANopen slave.....	266
Ilustracja 137: Konfiguracja CANopen slave.....	266
Ilustracja 138: Konfiguracja zmiennych CANopen slave.....	267
Ilustracja 139: Konfiguracja parametrów sieci CANopen slave	268
Ilustracja 140: Zakładka „Resources”	270
Ilustracja 141: Okno dialogowe „Open”	271

Ilustracja 142: Symbol modułu na pasku menu; język programowania FDB	271
Ilustracja 143: Instancja bloku funkcyjnego DiagGetBusState() w FBD	271
Ilustracja 144: Blok funkcyjny DiagGetState() w FBD	272
Ilustracja 145: Widok offline okna zmiennych w CODESYS	272
Ilustracja 146: Widok offline okna zmiennych w CODESYS (górne okno) w FBD	273
Ilustracja 147: Przykład diagnostyki	274
Ilustracja 148: Wywołanie diagnostyki DiagGetState()	275
Ilustracja 149: Widok Online dla Array EXTENDEDINFO w formie binarnej	276
Ilustracja 150: Dodawanie CANopen master	279
Ilustracja 151: Dodawanie prędkości transmisji	280
Ilustracja 152: Plik EDS „Generic CAN-Device“	280
Ilustracja 153: Zakładka „Module parameters“	281
Ilustracja 154: Zakładka „CAN parameters“	281
Ilustracja 155: Dołączanie urządzenia CAN Layer2	282
Ilustracja 156: LED dla zasilania	283
Ilustracja 157: LED dla systemu / sieci obiektowej	284
Ilustracja 158: LED "LNK"	293
Ilustracja 159: LED gniazda karty pamięci	294
Ilustracja 160: Diagram przebiegu sekwencji migania	295
Ilustracja 161: Wkładanie karty pamięci	304
Ilustracja 162: Zwolnienie zaczepu ryglującego	310
Ilustracja 163: Usuwanie modułu I/O (przykład)	311
Ilustracja 164: Przykład nadruku zgodnie z ATEX i IECEX	315
Ilustracja 165: Szczegół – przykład nadruku zgodnie z ATEX i IECEX	315
Ilustracja 166: Przykład nadruku na certyfikowanym module I/O Ex i z godnie z ATEX i IECEX	317
Ilustracja 167: Szczegół – przykład nadruku na certyfikowanym module I/O Ex i zgodnie z ATEX i IECEX	317
Ilustracja 168: Przykład nadruku zgodnie z NEC	319
Ilustracja 169: Szczegół – przykład nadruku zgodnie z NEC 500	319
Ilustracja 170: Szczegół – przykład nadruku na certyfikowanym module I/O Ex i zgodnie z NEC 505	320
Ilustracja 171: Szczegół – przykład nadruku na certyfikowanym module I/O Ex i zgodnie z NEC 506	320
Ilustracja 172: Szczegół – przykład nadruku na certyfikowanym module I/O Ex i zgodnie z CEC 18 załącznik J	321
Ilustracja 173: Obraz graficzny bloku funkcyjnego „ConfigToolFB“	466

Spis tabel

Tabela 1: Zastosowane systemy liczbowe.....	18
Tabela 2: Sposoby zapisu	18
Tabela 3: Opis ilustracji „Widok”	30
Tabela 4: Opis ilustracji „Zaciski CAGE CLAMP®”	32
Tabela 5: Złącze serwisowe	33
Tabela 6: Opis ilustracji „Złącza sieciowe – X1, X2”	34
Tabela 7: Opis ilustracji „Złącze sieci obiektowej CANopen – X3”	35
Tabela 8: Opis ilustracji „Styki magistrali obiektowej”	38
Tabela 9: Opis ilustracji „LED dla zasilania”	39
Tabela 10: Opis ilustracji „LED dla systemu/sieci obiektowej”	40
Tabela 11: Opis ilustracji „LED gniazda karty pamięci”	41
Tabela 12: Opis ilustracji „LED LNK (obok gniazd M12)”	42
Tabela 13: Przełącznik trybu pracy.....	43
Tabela 14: Przełącznik trybu pracy.....	43
Tabela 15: Dane techniczne – urządzenie.....	47
Tabela 16: Dane techniczne – dane systemowe	47
Tabela 17: Dane techniczne – zasilanie	48
Tabela 18: Dane techniczne – zegar	49
Tabela 19: Dane techniczne – programowanie	49
Tabela 20: Dane techniczne – magistrala systemowa	49
Tabela 21: Dane techniczne – ETHERNET	50
Tabela 22: Dane techniczne – CANopen.....	50
Tabela 23: Dane techniczne – oprzewodowanie	51
Tabela 24: Dane techniczne – styki magistrali obiektowej	51
Tabela 25: Dane techniczne – styki magistrali systemowej	51
Tabela 26: Dane techniczne – warunki mechaniczne	51
Tabela 27: Dane techniczne – warunki klimatyczne	51
Tabela 28: Normy i warunki użytkowania dla zastosowań w ochronie przeciwwybuchowej	55
Tabela 29: Warunki klimatyczne i mechaniczne, przemysł stoczniowy	56
Tabela 30: EMC – normy produktowe i techniczne.....	57
Tabela 31: EMC – odporność na zakłócenia	58
Tabela 32: EMC – emisja zakłóceń	60
Tabela 33: Normy i warunki użytkowania do zastosowań kolejowych (EN 50155:2017).....	61
Tabela 34: Przyporządkowanie MAC-ID i adresów IP dla 1 bridge'a z 2 portami	64
Tabela 35: Przyporządkowanie MAC-ID i adresów IP dla 2 bridge'ów z portami 1/1	64
Tabela 36: Usługi i użytkownicy	65
Tabela 37: Użytkownicy WBM.....	66
Tabela 38: Użytkownicy Linux®	66
Tabela 39: Lista parametrów wysyłanych przez DHCP.	74
Tabela 40: Komponenty pakietu oprogramowania Cloud Connectivity	77
Tabela 41: Ładowanie projektu bootowalnego	84
Tabela 42: Szyny montażowe WAGO	90
Tabela 43: Szyny montażowe WAGO dopuszczone do zastosowania z XTR PFC200 przy obciążeniu wibracjami >4g.....	90

Tabela 44: Filtry zasilania 24 V	98
Tabela 45: Opis ilustracji „Koncepcja zasilania”	99
Tabela 46: Opis ilustracji „Przykład zasilania”	100
Tabela 47: Złączki PE WAGO	102
Tabela 48: Fabryczne ustawienie dla adresowania IP interfejsu ETHERNET ...	108
Tabela 49: Maska sieci 255.255.255.0	108
Tabela 50: Fabryczne ustawienia użytkownika	125
Tabela 51: Prawa dostępu dla stron WBM	126
Tabela 52: Struktura menu CBM	131
Tabela 53: Sposób zapisywania adresów logicznych	153
Tabela 54: Events	164
Tabela 55: Dostęp do obrazów procesu danych wejściowych i wyjściowych – magistrala systemowa	170
Tabela 56: Dostęp do obrazów procesu danych wejściowych i wyjściowych – Modbus	171
Tabela 57: Dostęp do obrazów procesu danych wejściowych i wyjściowych – CANopen	171
Tabela 58: Dostęp do obrazów procesu danych wejściowych i wyjściowych – znaczniki	171
Tabela 59: Przyporządkowanie modułów I/O na potrzeby przykładu adresowania	172
Tabela 60: Przyporządkowanie modułów I/O na potrzeby przykładu adresowania	172
Tabela 61: Ustawienia magistrali systemowej	179
Tabela 62: Błędy i ich rozwiązanie	189
Tabela 63: Priorytety CODESYS V3	193
Tabela 64: Modbus settings	197
Tabela 65: Modbus TCP settings	198
Tabela 66: Modbus UDP settings	198
Tabela 67: Modbus RTU settings	199
Tabela 68: Mapowanie Modbus dla usług dostępu bitowego typu odczyt FC1, FC2	203
Tabela 69: Mapowanie Modbus dla usług dostępu bitowego typu zapis FC5, FC15	204
Tabela 70: Mapowanie Modbus dla usług dostępu do rejestru typu odczyt FC3, FC4, FC23	205
Tabela 71: Mapowanie Modbus dla usług dostępu do rejestru typu zapis FC6, FC16, FC22, FC23	208
Tabela 72: Rejestry Modbus WAGO	209
Tabela 73: Polecenia watchdoga	215
Tabela 74: Status watchdoga	216
Tabela 75: Konfiguracja watchdoga	217
Tabela 76: Tryby pracy watchdoga	218
Tabela 77: Diagnostyka przez serwer błędów	220
Tabela 78: Rejestry Modbus WAGO	224
Tabela 79: Polecenia watchdoga	228
Tabela 80: Status watchdoga	229
Tabela 81: Konfiguracja watchdoga	230
Tabela 82: Przegląd adresów w katalogu obiektów	235
Tabela 83: Indeksowanie zmiennych „IEC 61131-3” w katalogu obiektów	243

Tabela 84: Dostęp od strony sieci obiektowej do danych wyjściowych PFC	244
Tabela 85: Przykłady dla dostępów w CODESYS do zmiennych PFC	246
Tabela 86: Maksymalne indexy i subindexy zmiennych „IEC 61131-3”	247
Tabela 87: Przykład dla zmiennych wyjściowych „IEC 61131-3”	248
Tabela 88: Opis parametrów bazowych (master)	250
Tabela 89: Opis parametrów CAN (master).....	252
Tabela 90: Opis parametrów modułu (master)	253
Tabela 91: Opis parametrów bazowych (slave).....	255
Tabela 92: Opis parametrów CAN (slave)	257
Tabela 93: Opis mapowania PDO nadawczych i odbiorczych	261
Tabela 94: Opis okna właściwości PDO	262
Tabela 95: Opis parametrów modułu (slave).....	265
Tabela 96: Opis okna „CANopen Variables” (slave)	267
Tabela 97: Opis ustawień CANopen slave	268
Tabela 98: Bity informacji diagnostycznej.....	274
Tabela 99: Diagnostyka zasilania systemowego	283
Tabela 100: Diagnostyka zasilania sieciowego.....	283
Tabela 101: Diagnostyka LED „SYS”	285
Tabela 102: Diagnostyka LED „SYS”	286
Tabela 103: Diagnostyka LED „RUN”	287
Tabela 104: Diagnostyka LED „RUN”	288
Tabela 105: Diagnostyka LED „I/O”	290
Tabela 106: Diagnostyka LED „MS”	291
Tabela 107: Diagnostyka LED „CAN”	292
Tabela 108: Diagnostyka LED „LNK”	293
Tabela 109: Diagnostyka LED gniazda karty pamięci.....	294
Tabela 110: Przegląd kodów błędu LED „I/O”	297
Tabela 111: Kod błędu 1, znaczenie kodu migania i sposoby usuwania błędu .	298
Tabela 112: Kod błędu 2, znaczenie kodu migania i sposoby usuwania błędu .	299
Tabela 113: Kod błędu 3, znaczenie kodu migania i sposoby usuwania błędu .	300
Tabela 114: Kod błędu 4, znaczenie kodu migania i sposoby usuwania błędu .	301
Tabela 115: Kod błędu 5, znaczenie kodu migania i sposoby usuwania błędu .	301
Tabela 116: Kod błędu 7, znaczenie kodu migania i sposoby usuwania błędu .	301
Tabela 117: Kod błędu 9, znaczenie kodu migania i sposoby usuwania błędu .	302
Tabela 118: Przegląd kodów błędu LED „MS”	303
Tabela 119: Kod błędu 1, znaczenie kodu migania i sposoby usuwania błędu .	303
Tabela 120: Opis przykładowego nadruku zgodnie z ATEX i IECEx.....	316
Tabela 121: Opis przykładowego nadruku na certyfikowanym module I/O Ex i zgodnie z ATEX i IECEx.....	318
Tabela 122: Opis przykładowego nadruku zgodnie z NEC 500	319
Tabela 123: Opis przykładowego nadruku na certyfikowanym module I/O Ex i zgodnie z NEC 505	320
Tabela 124: Opis przykładowego nadruku na certyfikowanym module I/O Ex i zgodnie z NEC 506	320
Tabela 125: Opis przykładowego nadruku na certyfikowanym module I/O Ex i zgodnie z CEC 18 załącznik J	321
Tabela 126: Strona WBM „Device Status” – grupa „Device Details”	325
Tabela 127: Strona WBM „Device Status” – grupa „Network TCP/IP Details” ...	326
Tabela 128: Strona WBM „PLC Runtime Information” – grupa „Runtime”	328

Tabela 129: Strona WBM „PLC Runtime Information” – grupa „Projekt Details”	329
Tabela 130: Strona WBM „PLC Runtime Information” – grupa (grupy) „Task n”	329
Tabela 131: Strona WBM „PLC Runtime Configuration” – grupa „General PLC Runtime Configuration”	334
Tabela 132: Strona WBM „PLC Runtime Configuration” – grupa „Webserver Configuration”	336
Tabela 133: Strona WBM „TCP/IP Configuration” – grupa „TCP/IP Configuration”	337
Tabela 134: Strona WBM „TCP/IP Configuration” – grupa „DNS Server”	338
Tabela 135: Strona WBM „Ethernet Configuration” – grupa „Bridge Configuration”	339
Tabela 136: Strona WBM „Ethernet Configuration” – grupa „Switch Configuration”	340
Tabela 137: Strona WBM „Ethernet Configuration” – grupa „Ethernet Interface Configuration”	341
Tabela 138: Strona WBM „Configuration of Host and Domain Name” – grupa „Hostname”	342
Tabela 139: Strona WBM „Configuration of Host and Domain Name” – grupa „Domain Name”	342
Tabela 140: Strona WBM „Routing” – grupa „IP Forwarding through multiple interfaces”	344
Tabela 141: Strona WBM „Routing” – grupa „Default Static Routes”	345
Tabela 142: Strona WBM „Routing” – grupa „IP-Masquerading”	346
Tabela 143: Strona WBM „Routing” – grupa „Port Forwarding”	347
Tabela 144: Strona „Clock Setting” – grupa „Timezone and Format”	348
Tabela 145: Strona WBM „Clock Settings” – grupa „UTC Time and Date”	348
Tabela 146: Strona WBM „Clock Settings” – grupa „Local Time and Date”	349
Tabela 147: Strona WBM „Configuration of Service Interface” – grupa „Assign Owner of Service Interface”	350
Tabela 148: Strona WBM „Create bootable Image” – grupa „Create bootable image from boot device”	351
Tabela 149: Strona WBM „Firmware Backup” – grupa „Firmware Backup”	352
Tabela 150: Strona WBM „Firmware Restore” – grupa „Firmware Restore”	354
Tabela 151: Strona WBM „Active System” – grupa „Boot Device”	356
Tabela 152: Strona WBM „Active System” – grupa „System <n> (Internal Flash)”	356
Tabela 153: Strona WBM „Mass Storage” – grupa „Devices”	357
Tabela 154: Strona WBM „Mass Storage” – grupa „Create new Filesystem on Memory Card”	357
Tabela 155: Strona WBM „Software Uploads” – grupa „Upload new Software”	358
Tabela 156: Strona WBM „Configuration of Network Services” – grupa „Telnet”	359
Tabela 157: Strona WBM „Configuration of Network Services” – grupa „FTP”	359
Tabela 158: Strona WBM „Configuration of Network Services” – grupa „FTPS”	359
Tabela 159: Strona WBM „Configuration of Network Services” – grupa „HTTP”	360

Tabela 160: Strona WBM „Configuration of Network Services” – grupa „HTTPS”	360
Tabela 161: Strona WBM „Configuration of Network Services” – grupa „I/O-CHECK”	360
Tabela 162: Strona WBM „Configuration of NTP Client” – grupa „NTP Client Configuration”	361
Tabela 163: Strona WBM „PLC Runtime Services” – grupa „General Configuration”	362
Tabela 164: Strona WBM „PLC Runtime Services” – grupa „CODESYS 2”	362
Tabela 165: Strona WBM „PLC Runtime Services” – grupa „e!RUNTIME”	363
Tabela 166: Strona WBM „SSH Server Settings” – grupa „SSH Server”	364
Tabela 167: Strona WBM „TFTP Server” – grupa „TFTP Server”	365
Tabela 168: Strona WBM „DHCP Server Configuration” – grupa „DHCP Configuration Bridge <n>”	366
Tabela 169: Strona WBM „Configuration of DNS Server” – grupa „DNS Server”	367
Tabela 170: Strona WBM „Overview” – grupa „Service”	368
Tabela 171: Strona WBM „Overview” – grupa „Connection <n>”	368
Tabela 172: Strona WBM „Configuration of Connection <n>” – grupa „Configuration”	369
Tabela 173: Zależność pól wyboru i edycji dla platformy chmury	372
Tabela 174: Strona WBM „Configuration of general SNMP parameter” – grupa „General SNMP Configuration”	374
Tabela 175: Strona WBM „Configuration of SNMP v1/v2c parameters” – grupa „SNMP v1/v2c Manager Configuration”	375
Tabela 176: Strona WBM „Configuration of SNMP v1/v2c parameters” – grupa „Actually configured Trap Receivers”	376
Tabela 177: Strona WBM „Configuration of SNMP v3 Users” – grupa „Actually configured v3 Users”	377
Tabela 178: Strona WBM „Users Configuration” – grupa „Change Passwords”	379
Tabela 179: Strona WBM „OPC UA Configuration” – grupa „OPC UA Server”	380
Tabela 180: Strona WBM „OPC UA Configuration” – grupa „General OPC UA Server Configuration”	381
Tabela 181: Strona WBM „OPC UA Configuration” – grupa „OPC UA Endpoints”	382
Tabela 182: Strona WBM „OPC UA Configuration” – grupa „OPC UA Security Settings”	383
Tabela 183: Strona WBM „OPC UA Information Model” – grupa „OPC UA Server Information Model”	384
Tabela 184: Strona WBM „Modbus Services Configuration” – grupa „Modbus TCP”	385
Tabela 185: Strona WBM „Modbus Services Configuration” – grupa „Modbus UDP”	385
Tabela 186: Strona WBM „OpenVPN / IPsec Configuration” – grupa „OpenVPN”	387
Tabela 187: Strona WBM „OpenVPN / IPsec Configuration” – grupa „IPsec”	388
Tabela 188: Strona WBM „General Firewall Configuration” – grupa „Global Firewall Parameter”	389
Tabela 189: Strona WBM „Interface Configuration” – grupa „Firewall Configuration Bridge <n> / VPN”	390

Tabela 190: Strona WBM „Configuration of MAC address filter“ – grupa „Global MAC address filter state“	391
Tabela 191: Strona WBM „Configuration of MAC address filter“ – grupa „MAC address filter state Bridge <n>“	392
Tabela 192: Strona WBM „Configuration of MAC address filter“ – grupa „MAC address filter whitelist“	392
Tabela 193: Strona WBM „Configuration of User Filter“ – grupa „User filter“	394
Tabela 194: Strona WBM „Configuration of OpenVPN and IPsec“ – grupa „Certificate List“	396
Tabela 195: Strona WBM „Configuration of OpenVPN and IPsec“ – grupa „Private Key List“	396
Tabela 196: Strona WBM „Security Settings“ – grupa „TLS Configuration“	397
Tabela 197: Strona WBM „Advanced Intrusion Detection Environment (AIDE)“ – grupa „Run AIDE check at startup“	398
Tabela 198: Strona WBM „Advanced Intrusion Detection Environment (AIDE)“ – grupa „Control AIDE and show log“	398
Tabela 199: Strona WBM „Diagnostic Information“	400
Tabela 200: Menu „Information“	401
Tabela 201: Podmenu „Information“ > „Controller Details“	401
Tabela 202: Podmenu „Information“ > „Network Details“	402
Tabela 203: Menu „PLC Runtime“	403
Tabela 204: Podmenu „PLC Runtime“ > „Information“	403
Tabela 205: Podmenu „PLC Runtime“ > „Information“ > „Runtime Version“	404
Tabela 206: Podmenu „PLC Runtime“ > „Information“ > „Webserver Version“ ..	404
Tabela 207: Podmenu „PLC Runtime“ > „Information“ > „State“	404
Tabela 208: Podmenu „PLC Runtime“ > „Information“ > „Number of Tasks“	405
Tabela 209: Podmenu „PLC Runtime“ > „Information“ > „Project Details“	405
Tabela 210: Podmenu „PLC Runtime“ > „Information“ > „Tasks“	405
Tabela 211: Podmenu „PLC Runtime“ > „Information“ > „Tasks“ > „Task n“	406
Tabela 212: Podmenu „PLC Runtime“ > „General Configuration“	406
Tabela 213: Podmenu „PLC Runtime“ > „General Configuration“ > „PLC Runtime Version“	407
Tabela 214: Podmenu „PLC Runtime“ > „General Configuration“ > „Home Dir On SD Card“	407
Tabela 215: Podmenu „PLC Runtime“ > „WebVisu“	408
Tabela 216: Menu „Networking“	409
Tabela 217: Podmenu „Networking“ > „Host-/Domain Name“	409
Tabela 218: Podmenu „Networking“ > „Host-/Domain Name“ > „Hostname“	410
Tabela 219: Podmenu „Networking“ > „Host-/Domain Name“ > „Domain Name“	410
Tabela 220: Podmenu „Networking“ > „TCP/IP“	410
Tabela 221: Podmenu „Networking“ > „TCP/IP“ > „IP Address“	411
Tabela 222: Podmenu „Networking“ > „TCP/IP“ > „IP Address“ > „Xn“	411
Tabela 223: Podmenu „Networking“ > „TCP/IP“ > „Default Gateway“	412
Tabela 224: Podmenu „Networking“ > „TCP/IP“ > „Default Gateway“ > „Default Gateway n“	412
Tabela 225: Podmenu „Networking“ > „TCP/IP“ > „DNS Server“	413
Tabela 226: Podmenu „Networking“ > „Ethernet“	413
Tabela 227: Podmenu „Networking“ > „Ethernet“ > „Switch Configuration“	414
Tabela 228: Podmenu „Networking“ > „Ethernet“ > „Ethernet Ports“	414

Tabela 229: Podmenu „Networking“ > „Ethernet“ > „Ethernet Ports“ > „Interface Xn“	415
Tabela 230: Menu „Firewall“	416
Tabela 231: Podmenu „Firewall“ > „General Configuration“	417
Tabela 232: Podmenu „Firewall“ > „General Configuration“ > „Interface xxx“	418
Tabela 233: Podmenu „Firewall“ > „MAC Address Filter“	420
Tabela 234: Podmenu „Firewall“ > „MAC Address Filter“ > „MAC address filter whitelist“	421
Tabela 235: Podmenu „Firewall“ > „MAC Address Filter“ > „MAC address filter whitelist“ > „Add new / No (n)“	421
Tabela 236: Podmenu „Firewall“ > „User Filter“	422
Tabela 237: Podmenu „Firewall“ > „User Filter“ > „Add New / No (n)“	423
Tabela 238: Menu „Clock“	424
Tabela 239: Menu „Administration“	425
Tabela 240: Podmenu „Administration“ > „Users“	426
Tabela 241: Podmenu „Administration“ > „Create Image“	426
Tabela 242: Menu „Package Server“	427
Tabela 243: Podmenu „Package Server“ > „Firmware Backup“	427
Tabela 244: Podmenu „Package Server“ > „Firmware Backup“ > „Auto Update Feature“	428
Tabela 245: Podmenu „Package Server“ > „Firmware Backup“ > „Auto Update Feature“	428
Tabela 246: Podmenu „Package Server“ > „Firmware Restore“	429
Tabela 247: Podmenu „Package Server“ > „Firmware Restore“ > „Select Package“	429
Tabela 248: Podmenu „Package Server“ > „System Partition“	430
Tabela 249: Menu „Mass Storage“	431
Tabela 250: Podmenu „Mass Storage“ > „SD Card“	431
Tabela 251: Menu „Ports and Services“	433
Tabela 252: Podmenu „Ports and Services“ > „Telnet“	434
Tabela 253: Podmenu „Ports and Services“ > „FTP“	434
Tabela 254: Podmenu „Ports and Services“ > „FTPS“	435
Tabela 255: Podmenu „Ports and Services“ > „HTTP“	435
Tabela 256: Podmenu „Ports and Services“ > „HTTPS“	436
Tabela 257: Podmenu „Ports and Services“ > „NTP“	436
Tabela 258: Podmenu „Ports and Services“ > „SSH“	437
Tabela 259: Podmenu „Ports and Services“ > „TFTP“	437
Tabela 260: Podmenu „Ports and Services“ > „DHCPD“	438
Tabela 261: Podmenu „Ports and Services“ > „DHCPD“ > „Xn“	438
Tabela 262: Podmenu „Ports and Services“ > „DNS“	439
Tabela 263: Podmenu „Ports and Services“ > „IOCHECK PORT“	440
Tabela 264: Podmenu „Ports and Services“ > „Modbus TCP“	440
Tabela 265: Podmenu „Ports and Services“ > „Modbus UDP“	441
Tabela 266: Podmenu „Ports and Services“ > „OPC UA“	441
Tabela 267: Podmenu „Ports and Services“ > „...“ > „Firewall Status“	442
Tabela 268: Podmenu „Ports and Services“ > „PLC Runtime Services“	443
Tabela 269: Podmenu „Ports and Services“ > „PLC Runtime Services“ > „CODESYS 2“	444
Tabela 270: Podmenu „Ports and Services“ > „PLC Runtime Services“ > „e!RUNTIME“	445

Tabela 271: Menu „SNMP“	446
Tabela 272: Podmenu „SNMP“ > „General SNMP Configuration“	446
Tabela 273: Podmenu „SNMP“ > „SNMP v1/v2c Manager Configuration“	447
Tabela 274: Podmenu „SNMP“ > „SNMP v1/v2c Trap Receiver Configuration“	447
Tabela 275: Podmenu „SNMP“ > „SNMP v3 Configuration“	448
Tabela 276: Podmenu „SNMP“ > „(Secure)SNMP firewalling“	449
Tabela 277: 2-kanalowe moduły wejść dwustanowych	451
Tabela 278: 8-kanalowe moduły wejść dwustanowych	451
Tabela 279: 16-kanalowe moduły wejść dwustanowych	451
Tabela 280: 2-kanalowe moduły wyjść dwustanowych	452
Tabela 281: 2-kanalowe moduły wyjść dwustanowych z diagnostyką i danymi wejściowymi	452
Tabela 282: 4-kanalowe moduły wyjść dwustanowych	453
Tabela 283: 4-kanalowe moduły wyjść dwustanowych z diagnostyką i danymi wejściowymi	453
Tabela 284: 8-kanalowe moduły wyjść dwustanowych	453
Tabela 285: 8-kanalowe moduły wyjść dwustanowych z diagnostyką i danymi wejściowymi	454
Tabela 286: 16-kanalowe moduły wyjść dwustanowych	454
Tabela 287: 2-kanalowe moduły wejść analogowych	455
Tabela 288: 4-kanalowe moduły wejść analogowych	455
Tabela 289: Moduł pomiaru mocy 3-fazowej	456
Tabela 290: 2-kanalowe moduły wyjść analogowych	457
Tabela 291: 4-kanalowe moduły wyjść analogowych	457
Tabela 292: Interfejsy szeregowo z alternatywnym formatem danych	458
Tabela 293: Interfejsy SSI z alternatywnym formatem danych	459
Tabela 294: Moduł interfejsu enkodera przyrostowego	459
Tabela 295: Liczniki	460
Tabela 296: Licznik, tryb pracy „2 licznik góra/16 bitów/5 kHz“	460
Tabela 297: Gateway CAN	461
Tabela 298: Biblioteki systemowe CODESYS	462
Tabela 299: Możliwe makra dla dostępu do danych	464
Tabela 300: Możliwe makra dla dostępu do danych	465
Tabela 301: Zmienne wejściowe „DEVICENUMBER“	465
Tabela 302: Opis skryptów konfiguracyjnych „Information“	467
Tabela 303: Opis skryptów konfiguracyjnych „CODESYS“	468
Tabela 304: Opis skryptów konfiguracyjnych „Networking - Host-/Domainname“	469
Tabela 305: Opis skryptów konfiguracyjnych „Networking - TCP/IP“	470
Tabela 306: Opis skryptów konfiguracyjnych „Networking - ETHERNET“	472
Tabela 307: Opis skryptów konfiguracyjnych „NTP“	473
Tabela 308: Opis skryptów konfiguracyjnych „Clock“	474
Tabela 309: Opis skryptów konfiguracyjnych „Administration“	475
Tabela 310: Opis skryptów konfiguracyjnych „Package Server“	476
Tabela 311: Opis skryptów konfiguracyjnych „Ports and Services – Network Services“	476
Tabela 312: Opis skryptów konfiguracyjnych „Ports and Services – PLC Runtime Services“	478
Tabela 313: Opis skryptów konfiguracyjnych „Ports and Services – SSH/TFTP“	481
Tabela 314: Opis skryptów konfiguracyjnych „SNMP“	482



WAGO GmbH & Co. KG
Postfach 2880 • 32385 Minden
Hansastraße 27 • 32423 Minden
tel.: 0571/887 – 0
faks: 0571/887 – 844169
e-mail: info@wago.com
strona [www: www.wago.com](http://www.wago.com)