TECHDOCS

WAGO I/O System 750/753

Sterownik PFC100 2. generacji, PFC200 2. generacji i PFC300

750-811x, 750-821x, 750-8302



Podręcznik do systemu sterowania
Wersja FW 04.08.xx(30)
3621366155 | 4 | pl | 2026-09-02 09:12

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

WAGO GmbH & Co. KG
Hansastraße 27
D - 32423 Minden
Tel.: +49 (0) 571/887 – 0
e-mail: **info@wago.com**
Strona internetowa: **www.wago.com**

Wsparcie techniczne
Tel.: +49 (0) 571/887 – 44555
e-mail: **support@wago.com**
Strona internetowa: **www.wago.com/support**

Zostały podjęte wszelkie możliwe działania w celu zapewnienia prawidłowości i kompletności niniejszej dokumentacji. Pomimo zachowania najwyższej staranności nie jest możliwe całkowite wykluczenie błędów, dlatego autorzy będą wdzięczni za wszelkiego rodzaju wskazania i sugestie.

e-mail: **documentation@wago.com**

Należy pamiętać, że zastosowane w niniejszej dokumentacji 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 Wymagania 7
1.1 Zakres obowiązywania 7

2 Przegląd 12

3 Funkcje 13
3.1 Przegląd funkcji 13
3.2 Funkcje systemu 14
3.2.1 Status produktu i systemu 14
3.2.2 Zegar czasu rzeczywistego 15
3.2.2.1 Sygnalizacja/ręczne ustawianie 15
3.2.2.2 Ustawianie automatyczne 15
3.2.3 Środowisko systemowe CODESYS V3 16
3.2.3.1 Zakresy pamięci w CODESYS V3 16
3.2.3.1.1 Pamięć programu i danych 16
3.2.3.1.2 Ograniczenie liczby bloków 16
3.2.3.1.3 Zakres znaczników (Memory) i zakres Retain 16
3.2.3.2 Priorytety CODESYS V3 17
3.2.3.3 Ustawienia usługi i portu CODESYS V3 17
3.3 Funkcje sprzętu 18
3.3.1 Przełączanie adresów 18
3.3.2 Przełączanie trybu pracy/przycisk Reset 18
3.3.2.1 Aktywacja/dezaktywacja przełącznika trybu pracy/przycisku Reset 18
3.3.2.2 Tymczasowe ustawianie stałych adresów IP 19
3.3.2.3 Reset programowy (restart) 20
3.3.2.4 Reset sterownika 20
3.3.3 Złącze komunikacyjne 20
3.3.3.1 PFC100/PFC200 20
3.3.3.2 PFC300 21
3.3.4 Złącze serwisowe 22
3.4 Funkcje konfiguracyjne 23
3.4.1 Web Based Management (WBM) 23
3.5 Funkcje sieciowe 24
3.5.1 Konfiguracja sieci 24
3.5.1.1 Konfiguracja interfejsów 24
3.5.1.1.1 Konfiguracja bridge 24
3.5.1.1.2 Interfejsy Dummy 24
3.5.1.1.3 Interfejsy VLAN 24
3.5.1.1.4 Konfiguracja Port Mirror (PFC100 G2, PFC200 G2 - 2-Port, PFC300) 25
3.5.1.1.5 Konfiguracja Storm Control (PFC100 G2, PFC200 G2 - 2-Port) 25
3.5.1.1.6 Konfiguracja Storm Control (PFC200 G2 - 4-Port) 25
3.5.1.1.7 Konfiguracja Storm Control (PFC300) 25
3.5.1.1.8 Konfiguracja interfejsów Ethernet (PFC100 G2, PFC200 G2 - 2-Port) 25
3.5.1.1.9 Konfiguracja interfejsu Ethernet (PFC200 G2 - 4-Port, PFC300) 26
3.5.1.2 Konfiguracja TCP/IP 27
3.5.1.2.1 Bridge Interfaces 27
3.5.1.2.2 Interfejsy Dummy 27
3.5.1.2.3 VLAN-Interfaces 27
3.5.1.2.4 Serwer DNS 28
3.5.1.3 Nazwa hosta/domeny 28
3.5.1.3.1 Nazwa hosta 28

3.5.1.3.2 Nazwa domeny ... 29
3.5.1.4 Routing ... 29
3.5.1.4.1 Routing statyczny ... 30
3.5.1.4.2 Trasy dynamiczne ... 32
3.5.1.4.3 IP-Masquerading ... 32
3.5.1.4.4 Przekierowanie portów ... 33
3.5.2 Bezpieczeństwo sieci ... 33
3.5.2.1 Użytkownicy i hasła ... 33
3.5.2.2 Uwierzytelnianie serwera WWW ... 35
3.5.2.2.1 Szyfrowanie TLS ... 35
3.5.2.3 Certyfikaty Root ... 36
3.5.2.4 Firewall ... 37
3.5.2.4.1 Ustawienia globalne Firewall ... 37
3.5.2.4.2 Ustawienia zapory sieciowej powiązane z interfejsem ... 37
3.5.2.4.3 Filtr adresu MAC ... 38
3.5.2.4.4 User Filter ... 39
3.5.3 Usługi sieciowe ... 39
3.5.3.1 Klient DHCP ... 39
3.5.3.2 DHCP server ... 40
3.5.3.3 Serwer DNS ... 41
3.5.3.4 SNMP ... 42
3.5.3.4.1 SNMP v1/v2c ... 42
3.5.3.4.2 SNMP v3 ... 43
3.5.3.5 FTP/FTPES ... 45
3.5.3.6 HTTP / HTTPS ... 45
3.5.3.7 I/O-CHECK ... 46
3.5.3.8 SSH-Server ... 46
3.5.3.9 Docker® ... 46
3.6 Cloud Connectivity ... 47
3.7 Funkcje sieci obiektowej ... 52
3.7.1 OPC UA ... 52
3.7.2 BACnet ... 53
3.7.3 Master i slave CANopen ... 57
3.7.3.1 Katalog obiektów ... 58
3.7.3.2 Profil komunikacji ... 58
3.7.3.2.1 Konfiguracja mastera ... 61
3.7.3.3 Wymiana danych ... 62
3.7.3.3.1 Obiekty komunikacyjne sterownika ... 62
3.7.3.3.2 Adresowanie specyficzne dla sieci obiektowej ... 63
3.7.3.3.3 Przykłady definicji zmiennych sieciowych PFC ... 65
3.7.3.3.4 Zastosowanie slave CANopen (Device) w CODESYS V3 ... 66
3.7.3.3.5 Zastosowanie jako urządzenie warstwy 2 CAN ... 66
3.8 Funkcje pamięci ... 67
3.8.1 Bezpieczeństwo danych ... 67
3.8.1.1 Funkcja backupu ... 67
3.8.1.2 Funkcja Restore ... 69
3.8.2 Funkcja karty pamięci ... 70
3.8.2.1 Wkładanie karty pamięci podczas pracy ... 70
3.8.2.2 Wyjmowanie karty pamięci podczas pracy ... 71
3.8.2.3 Ustawienia katalogu Home dla systemu runtime ... 71
3.8.2.4 Ładowanie projektu bootowalnego ... 72
3.9 Funkcje diagnostyczne ... 72
3.9.1 Diagnostyka za pomocą elementów sygnalizacyjnych ... 72
3.9.1.1 Diagnostyka za pomocą sekwencji migania ... 72
3.9.1.1.1 Kody błędów LED I/O ... 73
3.9.1.1.2 Kody błędów LED MS ... 76
3.9.2 Diagnostyka poprzez WBM ... 77

4 Uruchamianie ... 79

4.1 Włączanie sterownika ... 79
4.2 Ustalanie adresu IP hosta ... 79
4.3 Ustawianie adresu IP ... 79
4.3.1 Połączenie IP przez USB (PFC300) ... 80
4.3.2 Ustawianie adresu IP przez WMB ... 80
4.3.3 Przydzielanie adresu IP przy pomocy DHCP ... 81
4.3.4 Zmiana adresu IP przy użyciu „WAGO Ethernet Settings“ ... 81
4.3.5 Ustawianie domyślnego adresu IP za pomocą przełącznika adresów ... 82
4.3.6 Tymczasowe ustawianie stałych adresów IP ... 84
4.4 Testowanie połączenia sieciowego ... 84
4.5 Zmiana haseł ... 85
4.6 Wyłączanie/restart ... 86

5 Konfiguracja ... 87

5.1 Konfiguracja za pomocą WBM ... 87
5.1.1 Ogólne informacje o stronie ... 88
5.1.2 Przegląd stron WBM i prawa dostępu ... 89
5.2 Konfiguracja przy pomocy „WAGO Ethernet Settings“ ... 90
5.2.1 Zakładka Identification ... 91
5.2.2 Zakładka Network ... 92
5.2.3 Zakładka PLC ... 93
5.2.4 Zakładka Status ... 93

6 Serwis ... 94

6.1 Zmiany firmware'u ... 94
6.1.1 Przeprowadzanie aktualizacji/aktualizacji wstecznej przy użyciu WAGOupload ... 94
6.1.2 Przeprowadzanie aktualizacji/aktualizacji wstecznej przy użyciu karty pamięci i WBM ... 95
6.2 Wyzwalanie funkcji RESET ... 95
6.2.1 Gorący reset ... 95
6.2.2 Zimny reset ... 95
6.2.3 Reset programowy (restart) ... 96
6.2.4 Reset sterownika ... 96
6.3 Aktualizacja certyfikatów Root ... 97

7 Załącznik ... 98

7.1 Dialogi konfiguracyjne ... 98
7.1.1 Strony WBM ... 98
7.1.1.1 Przegląd stron WBM i prawa dostępu ... 98
7.1.1.2 Zakładka „Information“ ... 99
7.1.1.2.1 Strona „Device Status“ ... 99
7.1.1.2.2 Strona „Vendor Information“ ... 100
7.1.1.2.3 Strona „PLC Runtime Information“ ... 100
7.1.1.2.4 Strona „WAGO Software License Agreement“ ... 101
7.1.1.2.5 Strona „Open Source Licenses“ ... 101
7.1.1.2.6 Strona „WBM Third Party License Information“ ... 101
7.1.1.2.7 Strona „Trademarks Information“ ... 101
7.1.1.2.8 Strona „WBM Version“ ... 101
7.1.1.3 Zakładka „Configuration“ ... 101
7.1.1.3.1 Strona „PLC Runtime Configuration“ ... 101
7.1.1.3.2 Strona „TCP/IP Configuration“ ... 103
7.1.1.3.3 Strona „Ethernet Configuration“ ... 104
7.1.1.3.4 Strona „Configuration of Host and Domain Name“ ... 107
7.1.1.3.5 Strona „Routing“ ... 108
7.1.1.3.6 Strona „Spanning Tree Protocol“ ... 110
7.1.1.3.7 Strona „Clock Settings“ ... 112

7.1.1.3.8 Strona „Configuration of Serial Interface“ ... 113
7.1.1.3.9 Strona „Configuration of Service Interface“ ... 115
7.1.1.3.10 Strona „Create bootable Image“ ... 115
7.1.1.3.11 Strona „Firmware Backup“ ... 116
7.1.1.3.12 Strona „Firmware Restore“ ... 117
7.1.1.3.13 Strona „Active System“ ... 119
7.1.1.3.14 Strona „Mass Storage“ ... 120
7.1.1.3.15 Strona „Software Uploads“ ... 120
7.1.1.3.16 Strona „Configuration of Network Services“ ... 121
7.1.1.3.17 Strona „Configuration of NTP Client“ ... 122
7.1.1.3.18 Strona „PLC Runtime Services“ ... 123
7.1.1.3.19 Strona „SSH Server Settings“ ... 123
7.1.1.3.20 Strona „DHCP Server Configuration“ ... 124
7.1.1.3.21 Strona „Configuration of DNS Server“ ... 124
7.1.1.3.22 Strona „Status overview“ ... 125
7.1.1.3.23 Strona „Configuration of Connection <n>“ ... 125
7.1.1.3.24 Strona „Controls Settings“ ... 129
7.1.1.3.25 Strona „Configuration of general SNMP parameters“ ... 129
7.1.1.3.26 Strona „Configuration of SNMP v1/v2c Parameters“ ... 130
7.1.1.3.27 Strona „Configuration of SNMP v3 Parameters“ ... 130
7.1.1.3.28 Strona „Commissioning Settings“ ... 131
7.1.1.3.29 Strona „Docker Settings“ ... 132
7.1.1.3.30 Strona „WBM User Configuration“ ... 132
7.1.1.4 Zakładka „Fieldbus“ ... 133
7.1.1.4.1 Strona „OPC UA Configuration“ ... 133
7.1.1.4.2 Strona „BACnet Status“ ... 135
7.1.1.4.3 Strona „BACnet Configuration“ ... 135
7.1.1.4.4 Strona „BACnet Data Link“ ... 137
7.1.1.4.5 Strona „BACnet Storage Location“ ... 138
7.1.1.4.6 Strona „BACnet Info" ... 139
7.1.1.5 Zakładka „Security“ ... 141
7.1.1.5.1 Strona „OpenVPN / IPsec“ ... 141
7.1.1.5.2 Strona „General Firewall Configuration“ ... 142
7.1.1.5.3 Strona „Interface Configuration“ ... 142
7.1.1.5.4 Strona „Configuration of MAC address filter“ ... 143
7.1.1.5.5 Strona „Configuration of User Filter“ ... 145
7.1.1.5.6 Strona „Certificates“ ... 145
7.1.1.5.7 Strona „Boot mode configuration“ ... 146
7.1.1.5.8 Grupa „Security Settings“ ... 146
7.1.1.5.9 Strona „Advanced Intrusion Detection Environment (AIDE)“ . 147
7.1.1.5.10 Strona „WAGO Device Access“ ... 148
7.1.1.6 Zakładka „Diagnostic“ ... 149
7.1.1.6.1 Strona „Log Message Viewer“ ... 149
7.1.1.6.2 Strona „Download“ ... 150
7.1.1.6.3 Strona „Network Capture“ ... 150

1 Wymagania

1.1 Zakres obowiązywania

Niniejsza dokumentacja dotyczy następujących produktów:

750-8110 (PFC100; G2; 2ETH; ECO)
Sterownik PFC100; 2. generacji; 2 x ETHERNET; ECO

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8110

750-8111 (PFC100; G2; 2ETH)
Sterownik PFC100; 2. generacji; 2 x ETHERNET

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8111

750-8112 (PFC100; G2; 2ETH; RS)
Sterownik PFC100; 2. generacji; 2 x ETHERNET; RS-232/485

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8112

750-8112/025-000 (PFC100; G2; 2ETH RS; T)
Sterownik PFC100; 2. generacji; 2 x ETHERNET; RS-232/485; rozszerzony zakres temperatury

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8112/025-000

750-8210 (PFC200; G2; 4ETH)
Sterownik PFC200; 2. generacji; 4 x ETHERNET

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8210

750-8210/025-000 (PFC200; G2; 4ETH; T)
Sterownik PFC200; 2. generacji; 4 x ETHERNET; rozszerzony zakres temperatury

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8210/025-000

750-8210/040-000 (PFC200; G2; 4ETH; XTR)
Sterownik PFC200; 2. generacji; 4 x ETHERNET; XTR

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8210/040-000

750-8211 (PFC200; G2; 2ETH 2SFP)
Sterownik PFC200; 2. generacji; 2 x ETHERNET; 2 x SFP

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8211

750-8211/040-000 (PFC200; G2; 2ETH 2SFP; XTR)
Sterownik PFC200; 2. generacji; 2 x ETHERNET; 2 x 100Base-FX; XTR

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8211/040-000

750-8211/040-001 (PFC200; G2; 2ETH 2SFP; Tele; XTR)
Sterownik PFC200; 2. generacji; 2 x ETHERNET; 2 x 100Base-FX; telecontrol; XTR

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8211/040-001

750-8212 (PFC200; G2; 2ETH RS)
Sterownik PFC200; 2. generacji; 2 x ETHERNET; RS-232/-485

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8212

750-8212/025-000 (PFC200; G2; 2ETH RS; T)
Sterownik PFC200; 2. generacji; 2 x ETHERNET; RS-232/-485; rozszerzony zakres temperatury

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8212/025-000

750-8212/025-001 (PFC200; G2; 2ETH RS; Tele; T)
Sterownik PFC200; 2. generacji; 2 x ETHERNET; RS-232/-485; telecontrol; rozszerzony zakres temperatury

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8212/025-001

750-8212/025-002 (PFC200; G2; 2ETH RS; Tele; T; ECO)
Sterownik PFC200; 2. generacji; 2 x ETHERNET; RS-232/-485; telecontrol; rozszerzony zakres temperatury; ECO

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8212/025-002

750-8212/000-100 (PFC200; G2; 2ETH RS BACnet/IP)
Sterownik PFC200; 2. generacji; 2 x ETHERNET; RS-232/-485; BACnet/IP

Wersja firmware'u	04.08.xx(30)

Strona produktu	http://www.wago.com/750-8212/000-100

750-8212/040-000 (PFC200 G2 2ETH RS XTR)
Sterownik PFC200 G2; 2 x ETHERNET; RS-232/-485; XTR

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8212/040-000

750-8212/040-001 (PFC200 G2 2ETH RS TELE XTR)
Sterownik PFC200 G2; 2 x ETHERNET; RS-232/-485; telecontrol; XTR

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8212/040-001

750-8212/040-010 (PFC200 G2 2ETH M12 RS XTR)
Sterownik PFC200 G2; 2 x ETHERNET M12; RS-232/-485; XTR

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8212/040-010

750-8213 (PFC200; G2; 2ETH CAN)
Sterownik PFC200; 2. generacji; 2 x ETHERNET, CAN, CANopen

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8213

750-8213/040-010 (PFC200 G2 2ETH M12 CAN XTR)
Sterownik PFC200 G2; 2 x ETHERNET M12; CAN; CANopen; XTR

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8213/040-010

750-8214 (PFC200; G2; 2ETH RS CAN)
Sterownik PFC200; 2. generacji; 2 x ETHERNET, RS-232/-485, CAN, CANopen

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8214

750-8215 (PFC200; G2; 4ETH CAN USB)
Sterownik PFC200; 2. generacji; 4 x ETHERNET, CAN, CANopen, USB-A

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8215

750-8216 (PFC200; G2; 2ETH RS CAN DPS)
Sterownik PFC200; 2. generacji; 2 x ETHERNET, RS-232/-485, CAN, CANopen, slave PROFIBUS

Wersja firmware'u	04.08.xx(30)

Strona produktu	http://www.wago.com/750-8216

750-8216/025-000 (PFC200; G2; 2ETH RS CAN DPS; T)
Sterownik PFC200; 2. generacji; 2 x ETHERNET, RS-232/-485, CAN, CANopen, slave PROFIBUS; rozszerzony zakres temperatury

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8216/025-000

750-8216/025-001 (PFC200; G2; 2ETH RS CAN DPS; Tele; T)
Sterownik PFC200; 2. generacji; 2 x ETHERNET, RS-232/-485, CAN, CANopen, slave PROFIBUS; telecontrol; rozszerzony zakres temperatury

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8216/025-001

750-8216/040-000 (PFC200 G2 2ETH RS CAN DPS XTR)
Sterownik PFC200 G2; 2 x ETHERNET; RS-232/-485; CAN; CANopen; slave PROFIBUS; XTR

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8216/040-000

750-8302 (PFC300; 2ETH RS485)
Sterownik PFC300; 2 x ETHERNET, RS-485

Wersja firmware'u	04.08.xx(30)
Strona produktu	http://www.wago.com/750-8302

Kompletna instrukcja obsługi produktów składa się z kilku obowiązujących dokumentów. Produkty wolno instalować i eksploatować wyłącznie zgodnie z zaleceniami zawartymi w kompletnej instrukcji obsługi. Znajomość całej obowiązującej dokumentacji jest warunkiem prawidłowego użytkowania. Kompletną dokumentację i wszystkie informacje można znaleźć na stronach zawierających szczegółowe dane produktu.

Obowiązujące dokumenty

Podręcznik do systemu I/O 750/753
- Wymagania
- Bezpieczeństwo
- Projektowanie
- Transport i magazynowanie
- Montaż i demontaż
- Montaż przewodów
- Wycofanie z eksploatacji

Podręcznik do produktu zastosowanego sterownika PFC100 G2, PFC200 G2 lub PFC300
- Informacje ogólne
- Właściwości
- Projektowanie
- Diagnostyka
- Serwis

Informacja

Niniejszy dokument opisuje pełny zakres funkcji. Nie wszystkie opisane funkcje są obsługiwane przez każdy produkt.

2 Przegląd

Sterownik PFC100

Sterownik PFC100 wyposażony jest w pamięć o pojemności 512 MB, dzięki czemu doskonale nadaje się do zastosowań w automatyce budynkowej oraz w budowie maszyn i urządzeń.

- programowanie w CODESYS zgodnie z normą IEC 61131-1
- otwarta platforma Linux®
- rozbudowane funkcje bezpieczeństwa

Sterownik PFC200

Sterownik PFC200 oferuje szeroki zakres funkcji, dzięki czemu doskonale sprawdza się w automatyce przemysłowej, procesowej i budynkowej.

- niezależność od typu sieci obiektowej
- możliwość programowania w CODESYS zgodnie z normą IEC 61131-1 w systemie operacyjnym Linux®
- rozbudowane funkcje bezpieczeństwa
- wersja XTR do pracy w ekstremalnych warunkach środowiskowych

Sterownik PFC300

Sterownik PFC300 jest wyposażony w 2GB pamięci RAM i procesor 64 bit, co pozwala na jego użycie w złożonych aplikacjach maszynowych, procesowych i budynkach.

- możliwość programowania w CODESYS zgodnie z normą IEC 61131-1 w systemie operacyjnym Linux®
- rozbudowane funkcje bezpieczeństwa
- dwurdzeniowy procesor
- złącze serwisowe USB C

3 Funkcje

3.1 Przegląd funkcji

Nie wszystkie opisane tutaj funkcje są dostępne we wszystkich produktach.
Informacje o funkcjach dostępnych w danym produkcie można znaleźć w przeglądzie funkcji w odpowiedniej instrukcji produktu.

Funkcje te zostały opisane w poniższych punktach.

Funkcje systemu

- **Status produktu i systemu [▸ 14]**
- **Zegar czasu rzeczywistego [▸ 15]**
- **Bezpieczeństwo danych [▸ 67]**
- **Funkcja karty pamięci [▸ 70]**
- **Środowisko systemowe CODESYS V3 [▸ 16]**

Funkcje sprzętu

- **Przełączanie trybu pracy/przycisk Reset [▸ 18]**
- **Złącze komunikacyjne [▸ 20]**
- **Złącze serwisowe [▸ 22]**
- **Przełącznik adresów [▸ 18]**

Funkcje konfiguracyjne

- **Web Based Management (WBM) [▸ 23]**

Funkcje sieciowe

- Konfiguracja sieci
- Bezpieczeństwo sieci
- Usługi sieciowe

Cloud Connectivity

Funkcje sieci obiektowej

- **BACnet [▸ 53]**
- **OPC UA [▸ 52]**
- **Master i slave CANopen [▸ 57]**

Funkcje diagnostyczne

- **Diagnostyka za pomocą elementów sygnalizacyjnych [▸ 72]**
- **Diagnostyka poprzez WBM [▸ 77]**

3.2 Funkcje systemu

3.2.1 Status produktu i systemu

Właściwości produktu wyświetlane są na stronie WBM „Device Status" w grupie „Device Details":

Tabela 1: Strona WBM „Device Status" – grupa „Device Details"

Parametr	Znaczenie
Product Description	Nazwa produktu
Numer zamówieniowy	Numer katalogowy produktu
Unique Item Identifier (UII)	Unikatowy numer identyfikacyjny produktu
License Information	Wskazanie, że system runtime CODESYS jest zainstalowany.
Firmware Revision	Stan firmware'u

Na stronie WBM „Device Status" w grupie „Network TCP/IP Details" wyświetlane są najważniejsze właściwości sieci i interfejsów produktu:

Tabela 2: 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	
Interfejs <n>	Aktualnie skonfigurowany interfejs; Dla każdego skonfigurowanego interfejsu 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 **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
	external	Adres IP przypisywany jest ewentualnie przez aplikację sieciową; Ma to miejsce na przykład wtedy, gdy adres IP zarządzany jest przez aplikację.
IP Address	Aktualny adres IP produktu	
Subnet Mask	Aktualna maska podsieci produktu	

Informacje o aktywowanym systemie runtime są wyświetlane na stronie WBM „PLC Runtime Information" w grupie „Runtime":

Tabela 3: Strona WBM „PLC Runtime Information" – grupa „Runtime"

Parametr	Znaczenie
Wersja	Aktualnie aktywowany system runtime Przy wyłączonym systemie runtime wyświetlana jest informacja „None".

3.2.2 Zegar czasu rzeczywistego

3.2.2.1 Sygnalizacja/ręczne ustawianie

Tabela 4: Strona WBM „Clock" – grupa „Timezone and Format"

Parametr	Znaczenie	
Timezone	Wybierz strefę czasową, ustawienia 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	Powyżej niemożliwy wybór strefy czasowej: podanie nazwy strefy czasowej, kraju i miasta Ustalenie prawidłowej nazwy strefy czasowej: **http://www.timeanddate.com/time/map/**	
Time Format	Format czasowy: 12h / 24h	
Local Date	Data lokalna	
Local Time	Zegar lokalny	
UTC Date	Data	
UTC Time	Czas GMT	

3.2.2.2 Ustawianie automatyczne

Tabela 5: Strona WBM „Configuration of NTP Client" – grupa „NTP Client Configuration"

Parametr	Znaczenie	
Service enabled	Automatyczna aktualizacja czasu; aktywacja/dezaktywacja	
	☐	Aktualizacja czasu jest nieaktywna; ustawienia fabryczne
	☑	Aktualizacja czasu jest aktywna.
Update Interval (sec)	Wprowadzenie interwału odświeżania serwera czasowego.	
Time Server <n>	Wprowadzenie adresów IP serwerów czasu; możliwe są maksymalnie 4 serwery czasu.	
Additionally assigned (DHCP)	Serwer NTP przydzielony przez DHCP; Jeśli nie został przydzielony serwer czasu, wyświetlana jest informacja „No additional servers assigned".	

3.2.3 Środowisko systemowe CODESYS V3

Wskazówka

Przeczytaj dokumentację CODESYS V3!

Informacje na temat instalacji, uruchamiania i programowania CODESYS V3 można znaleźć w podręczniku do CODESYS V3.

Wskazówka

Zamknąć nieużywane porty i usługi!

Przez otwarte porty i usługi osoby nieuprawnione mogą uzyskać dostęp do systemu automatyki.

1. 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 i port 11740 dla CODESYS V3).
2. Porty i usługi dobrze jest otwierać tylko na czas uruchamiania lub konfiguracji.

Wskazówka

Usługi CODESYS są odrzucane przy włączonej zaporze sieciowej, jeśli nie skonfigurowano filtrów użytkownika!

Jeśli wykorzystywane są usługi CODESYS (np. Modbus, OPC-UA, SNMP lub IIOT), w konfiguracji firewalla należy utworzyć odpowiednie filtry użytkownika dla tych usług. Filtry użytkownika muszą być skonfigurowane w taki sposób, aby odpowiednie porty były akceptowane.

3.2.3.1 Zakresy pamięci w CODESYS V3

3.2.3.1.1 Pamięć programu i danych

Pamięć programu (kodu) oraz danych została już zarezerwowana w systemie po pomyślnym pobraniu programu i może być w pełni wykorzystana Zakres pamięci dzielony jest dynamicznie między program i dane. Całkowita pojemność pamięci zależy od konkretnego produktu i jest określona w jego danych technicznych.

3.2.3.1.2 Ograniczenie liczby bloków

Oprócz pamięci programu i danych dostępnej dla aplikacji, w systemie wymagany jest również obszar pamięci do zarządzania poszczególnymi blokami programowymi. Wielkość tego obszaru obliczana jest jako ograniczenie liczby bloków × 12. Suma globalnej pamięci programu i danych oraz pamięci przeznaczonej na ograniczenie liczby bloków określa rzeczywistą wielkość pamięci roboczej żądanej przez system na potrzeby przechowywania danych.

3.2.3.1.3 Zakres znaczników (Memory) i zakres Retain

Zakres znaczników (Memory) i zakres Retain tworzą pamięć nieulotną dla aplikacji IEC 61131. Całkowita pojemność pamięci zależy od konkretnego produktu i jest określona w jego danych technicznych.

3.2.3.2 Priorytety CODESYS V3

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

Tabela 6: 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)
	Przełącznik trybu pracy, monitorowanie	-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) slave/master Modbus (-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 – czas nieokreślony	Komunikacja CODESYS	Background (20)		Komunikacja ze środowiskiem programistycznym CODESYS
	Zadania IEC cykliczne, dowolne i sterowania zdarzeniami		15	m.in. standardowe priorytety i zadania wizualizacji

3.2.3.3 Ustawienia usługi i portu CODESYS V3

Tabela 7: Strona WBM „PLC Runtime Configuration" – grupa „General PLC Runtime Configuration"

Parametr	Znaczenie	
PLC Runtime Version	Wybór aktywnego systemu runtime PLC	
	none	Żaden system runtime nie jest aktywowany.
	CODESYS V3	System runtime CODESYS V3 jest aktywowany.
Home directory on memory card enabled	Wybór lokalizacji dla katalogu Home systemu runtime	
	☐	Katalog Home dla systemu operacyjnego zapisywany jest w wewnętrznej pamięci sterownika.
	☑	Katalog Home dla systemu operacyjnego zapisywany jest na karcie pamięci.

Tabela 8: Strona WBM „PLC Runtime Configuration" – grupa „Webserver Configuration"

Parametr	Znaczenie	
CODESYS 3 Webserver State	Status (enabled/disabled) serwera WWW CODESYS V3	
Default Webserver	Wybór widoku strony przy wpisaniu samego adresu IP produktu	
	Web-Based-Management	Wyświetlany jest Web-Based-Management.
	WebVisu	Wyświetlana jest wizualizacja sieciowa systemu runtime.

Tabela 9: Strona WBM „PLC Runtime Services" – grupa „CODESYS V3"

Parametr	Znaczenie	
CODESYS V3 State	Status systemu runtime	
	disabled	System runtime jest dezaktywowany.
	enabled	System runtime jest aktywowany.
Webserver Enabled	Aktywacja i dezaktywacja serwera WWW dla wizualizacji WWW	
	☐	Serwer WWW jest nieaktywny.
	☑	Serwer WWW jest aktywny.
Separated WebVisu Ports (8080/8081)	Ustawianie portów CODESYS WebVisu dla HTTP/HTTPS	
	☐	CODESYS WebVisu jest udostępniany na portach 80/443 (standard jak WBM).
	☑	CODESYS WebVisu jest dostępny na portach 8080/8081.
Port Authentication Enabled	Aktywacja/dezaktywacja logowania w celu połączenia z urządzeniem	
	☐	Logowanie nie jest wymagane dla połączenia.
	☑	Połączenie wymaga logowania. Domyślną nazwą użytkownika jest admin, a hasłem jest hasło podane w „General Configuration".
Webserver Port Authentication Enabled	Aktywacja/dezaktywacja logowania w celu wywołania wizualizacji internetowej aplikacji Codesys	
	☐	Logowanie nie jest wymagane do wywołania wizualizacji internetowej.
	☑	Do wywołania wizualizacji internetowej wymagane jest zalogowanie. Standardowa nazwa użytkownika to admin, a hasłem jest hasło podane w „General Configuration".

3.3 Funkcje sprzętu

3.3.1 Przełączanie adresów

3.3.2 Przełączanie trybu pracy/przycisk Reset

3.3.2.1 Aktywacja/dezaktywacja przełącznika trybu pracy/przycisku Reset

Przede wszystkim ze względów bezpieczeństwa oraz w przypadku trudno dostępnych instalacji sterownik umożliwia włączenie lub wyłączenie przełącznika trybu pracy oraz przycisku Reset.

Jeśli przełącznik trybu pracy jest wyłączony, sterowanie urządzeniem musi odbywać się za pomocą środowiska programistycznego CODESYS.
Jeśli przycisk Reset jest wyłączony, wykonanie programowego resetu (ponownego uruchomienia) nadal jest możliwe za pośrednictwem WBM.

ⓘ Wskazówka

Przy wyłączonym przełączniku trybu pracy załadowany projekt bootowalny (CODESYS Boot Project) jest automatycznie uruchamiany po ponownym uruchomieniu urządzenia!

Zatrzymanie i zresetowanie działającej aplikacji przy wyłączonym przełączniku trybu pracy jest możliwe wyłącznie za pomocą środowiska programistycznego CODESYS.

Konfiguracji dokonuje się na stronie WBM „Controls Settings", w zakładce „Configuration". Wprowadzona zmiana zacznie obowiązywać dopiero po ponownym uruchomieniu sterownika.

Tabela 10: Strona WBM „Controls Settings" – grupa „OMS Controls"

Parametr	Znaczenie	
Current Mode	Aktualny stan funkcjonalności przełącznika trybu pracy oraz przycisku Reset	
	Inactive	Sterownik ignoruje każde użycie przełącznika trybu pracy i przycisku Reset.
	Active	Sterownik reaguje na użycie przełącznika trybu pracy i przycisku Reset.
Activate	Aktywacja/dezaktywacja przełącznika trybu pracy oraz przycisku Reset	
	☐	Wyłącz przełącznik trybu pracy i przycisk Reset.
	☑	Włącz przełącznik trybu pracy i przycisk Reset.

3.3.2.2 Tymczasowe ustawianie stałych adresów IP

W tym procesie adresy IP dla interfejsów sieciowych X1 ... X<n> ustawia się tymczasowo na stałe adresy IP.
Dla każdego zastosowanego bridge'a przypisywanym interfejsom nadawany jest osobny adres, przy czym bridge 1 otrzymuje adres IP "192.168.1.17", bridge 2 adres IP "192.168.2.17" itd.

Nie jest przeprowadzany reset.

Aby ustawić tymczasowo stałe adresy IP, należy postępować w następujący sposób:

1. Ustaw przełącznik trybu pracy w pozycji STOP.
2. Naciśnij przycisk resetu przez czas dłuższy niż 8 sekund.

➡ Wykonanie jest zasygnalizowane miganiem wskaźników LED „SYS" na pomarańczowo.

Jeśli po aktywowaniu tymczasowych adresów IP dokonywane będą zmiany w konfiguracji IP brigde'a, nowe ustawienia będą stale przejmowane i natychmiast stosowane. Skonfigurowany bridge opuszcza tym samym tymczasowy tryb adresu IP. Inne bridge'e zachowują swoje tymczasowe adresy IP aż do restartu/resetu.

Aby anulować to ustawienie, postępuj w następujący sposób:

- przeprowadź reset oprogramowania,

lub

- wyłącz i ponownie włącz produkt.

3.3.2.3 Reset programowy (restart)

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

➡ Wykonanie sygnalizowane jest krótkim rozbłyskiem wszystkich wskaźników LED. Po kilku dodatkowych sekundach dioda „SYS" wskazuje, że sterownik został pomyślnie uruchomiony.

3.3.2.4 Reset sterownika

UWAGA

Nie wyłączać sterownika!

Przerwanie procedury aktualizacji wstecznej może uszkodzić sterownik.

- Dlatego podczas procedury Reset nie należy wyłączać sterownika i nie odłączać zasilania!

Przy resecie sterownika („Reset sterownika"):
- parametry i hasła użytkowników Linux i WBM zostają nadpisane,
- zapisane aplikacje, włącznie z danymi dotyczącymi wizualizacji, zostają usunięte,
- zainstalowane później funkcje firmware'u nie zostaną nadpisane,
- licencje na oprogramowanie nie zostaną usunięte,

Nieaktywny system nie zostanie zmieniony podczas resetu sterownika.
W razie pytań należy skontaktować się ze wsparciem technicznym WAGO.

Po resecie sterownik jest ponownie automatycznie uruchamiany.

Aby przeprowadzić reset sterownika, należy postępować w następujący sposób:

✓ Warunek: zasilanie jest aktywne.

1. Naciśnij i przytrzymaj przycisk resetu.
2. Przełącznik trybu pracy należy ustawić w pozycji „RESET" i przytrzymać w tej pozycji.
3. Przytrzymaj oba przyciski, aż LED „SYS" zacznie migać na zmianę na czerwono i zielono (ok. po 8 sek.).
4. Zwolnij przełącznik trybu pracy i przycisk resetu.

➡ Sterownik został zresetowany i wykonuje automatyczny restart.

3.3.3 Złącze komunikacyjne

3.3.3.1 PFC100/PFC200

Sterownik wyposażony jest w konfigurowalny interfejs komunikacyjny.

Tryb pracy interfejsu można przełączać między RS-232 i RS-485.

Interfejs wspiera następujące parametry komunikacji:
- 8 bitów danych
- parzystość/brak parzystości

- 0/1/2 bity stopu

Interfejs komunikacyjny można przypisać do konsoli Linux. W tym przypadku tylko konsola Linux może komunikować się przez interfejs.
Jeśli interfejs nie jest przydzielony, na przykład program CODESYS może uzyskać do niego dostęp za pomocą bloków funkcyjnych.

Interfejs komunikacyjny ustawia się np. na stronie WBM „Configuration of Serial Interface".

Aktualna konfiguracja interfejsu wyświetlana jest w grupie „Current Serial Interface Configuration".

Tabela 11: Strona WBM „Configuration of Serial Interface" – grupa „Current Serial Interface Configuration"

Parametr	Znaczenie	
Assigned to	Przypisanie interfejsu komunikacyjnego	
	Unassigned (usage by Applications, Libraries, PLC Runtime)	Interfejs komunikacyjny nie jest przypisany do żadnej aplikacji. Dzięki temu np. program CODESYS może uzyskać do niego dostęp za pomocą bloków funkcyjnych.
	Linux Console	Interfejs komunikacyjny jest przypisany do konsoli Linux.
Mode	Tryb interfejsu komunikacyjnego	
	RS232	Interfejs komunikacyjny pracuje w trybie RS-232.
	RS485	Interfejs komunikacyjny pracuje w trybie RS-485.

Przyporządkowanie interfejsu ustawia się w grupie „Assign Owner of Serial Interface".

Tabela 12: Strona WBM „Configuration of Serial Interface" – grupa „Assign Owner of Serial Interface"

Parametr	Znaczenie
Unassigned (usage by Applications, Libraries, PLC Runtime)	Interfejs komunikacyjny nie jest przypisany do żadnej aplikacji.
Linux Console	Interfejs komunikacyjny jest przypisany do konsoli Linux.

Tryb pracy interfejsu jest ustawiany w grupie „Assign Mode of Serial Interface".

Tabela 13: Strona WBM „Configuration of Serial Interface" – grupa „Assign Mode of Serial Interface"

Parametr	Znaczenie
RS232	Interfejs komunikacyjny pracuje w trybie RS-232.
RS485	Interfejs komunikacyjny pracuje w trybie RS-485.

3.3.3.2 PFC300

Sterownik wyposażony jest w konfigurowalny interfejs komunikacyjny.

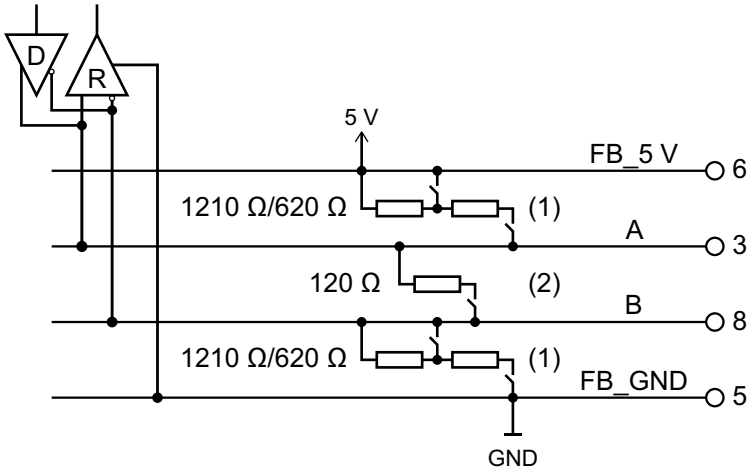
Tryb pracy interfejsu jest ustawiony na stałe na RS-485.

Interfejs wspiera następujące parametry komunikacji:
- 8 bitów danych
- parzystość/brak parzystości
- 0/1/2 bity stopu

Sieć polaryzująca (biasing network) zapobiega oscylacjom na przewodach sieciowych, gdy żaden nadajnik nie jest aktywny Te oscylacje mogą prowadzić do błędów transmisji. Rezystory Pull-up i Pull-Down zapewniają, że w stanie spoczynku wszystkie wejścia odbiornika wykazują różnicę napięć między RxD+ i RxD- większą niż 200 mV.

Rezystor terminujący na każdym końcu przewodów sieciowych zapobiega odbiciom na przewodach sieciowych. Te odbicia mogą również prowadzić do błędów transmisji.

Zgodnie z wymaganiami sieci obiektowej, zintegrowane w interfejsie rezystory pull-up i pull-down (1) w sieci Bias oraz zintegrowany rezystor terminujący (2) mogą być włączane lub wyłączane.



Ilustracja 1: Złącze komunikacyjne, terminator sieci i terminacja bias

Interfejs komunikacyjny ustawia się np. na stronie WBM „Configuration of Serial Interface".

Aktualna konfiguracja interfejsu wyświetlana jest w grupie „Current Serial Interface Configuration".

Tabela 14: Strona WBM „Configuration of Serial Interface" – grupa „Current Serial Interface Configuration"

Parametr	Znaczenie	
Mode	Tryb interfejsu komunikacyjnego	
	RS485	Interfejs komunikacyjny pracuje w trybie RS-485.

Terminację magistrali można ustawić w grupie „Bus Termination".

Tabela 15: Strona WBM „Configuration of Serial Interface" – grupa "Bus Termination"

Parametr	Znaczenie	
Termination enabled	Aktywacja/dezaktywacja terminacji	
	☐	Terminacja dezaktywowana
	☑	Terminacja magistrali jest aktywowana.

Polaryzację magistrali można ustawić w zakładce „Bias Network"

Tabela 16: Strona WBM „Configuration of Serial Interface" – grupa "Bias Network"

Parametr	Znaczenie
Off	Brak aktywnej magistrali
Niski	Aktywna terminacja 1 (640Ohm)
Wysoki	Aktywna terminacja 2 (1210Ohm)

3.3.4 Złącze serwisowe

Złącze serwisowe ustawia się np. na stronie WBM „Configuration of Service Interface".

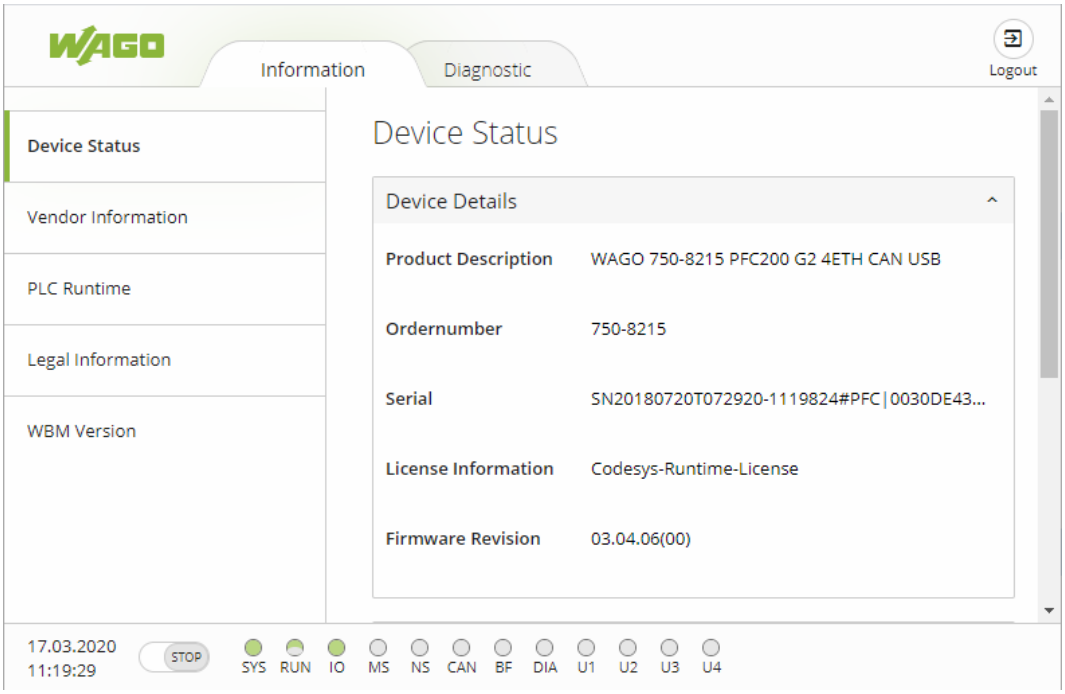
Przyporządkowanie złącza:

Tabela 17: Strona WBM „Configuration of Service Interface" – grupa „ Assign Owner of Service Interface"

Parametr	Znaczenie
WAGO Service Communication	Złącze serwisowe wykorzystywane jest do komunikacji serwisowej WAGO lub komunikacji z systemem runtime.
Linux Console	Złącze serwisowe jest przypisane do konsoli Linux.
Unassigned (usage by Applications, Libraries, PLC Runtime)	Złącze serwisowe nie jest przypisane do żadnej aplikacji. Dzięki temu np. program CODESYS może uzyskać do niego dostęp za pomocą bloków funkcyjnych.

3.4 Funkcje konfiguracyjne

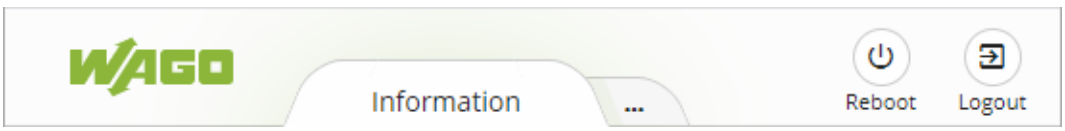
3.4.1 Web Based Management (WBM)



Ilustracja 2: Okno przeglądarki WBM (przykład)

W wierszu nagłówkowym okna przeglądarki wyświetlane są zakładki różnych obszarów WBM i przyciski **[Reboot]** oraz **[Logout]**. Przycisk **[Reboot]** widoczny jest tylko wtedy, gdy zalogowany jest administrator. Naciśnięcie przycisku **[Reboot]** powoduje restart sterownika. Restart może potrwać kilka minut. Przycisk **[Logout]** służy do wylogowania aktualnego użytkownika. Pojawia się wtedy ponownie polecenie zalogowania.

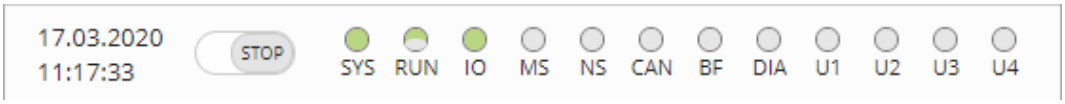
Gdy na wybranej szerokości okna nie mieszczą się wszystkie zakładki, w miejscu niewyświetlonej zakładki widoczna jest zakładka z symbolem (...). Dzięki temu poprzez listę rozwijalną można wybrać zakładki, które nie są wyświetlane.



Ilustracja 3: Wiesz nagłówkowy 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 4: Wiersz statusu WBM (przykład)

- Data i godzina – lokalny czas i lokalna data na urządzeniu
- Stan przełącznika trybu pracy
- Stany LED urządzenia:
  Diodom LED przypisane są odpowiednie oznaczenia (np. SYS, RUN, IO, ...) i ich stany są przedstawione za pomocą grafiki. Możliwe są następujące stany LED:
  – 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. Zawarty jest tu czas wysłania wiadomości.
  Stany wyświetlone w WBM nie odpowiadają w każdym momencie aktualnym stanom na sterowniku. Transmisja danych wymaga określonego czasu, a odpytywanie następuje w określonych interwałach. Czas między odpytywaniami wynosi 30 sekund.

3.5 Funkcje sieciowe

3.5.1 Konfiguracja sieci

3.5.1.1 Konfiguracja interfejsów

3.5.1.1.1 Konfiguracja bridge

Tabela 18: Strona WBM „Ethernet Configuration" – grupa „Bridge Configuration"

Parametr	Znaczenie
Bridge 1 ... <n>	Przyporządkowanie fizycznych portów X1 ... X<n> do logicznego bridge'a, kliknij odpowiedni przycisk opcji. Przyporządkowanie zostaje zaznaczone kolorem. Jeden port może być przyporządkowany do tylko jednej bramy.

3.5.1.1.2 Interfejsy Dummy

Tabela 19: Strona WBM „Ethernet Configuration" – grupa „Dummy Interfaces"

Parametr	Znaczenie
Name	Nazwa wybranego interfejsu Dummy

3.5.1.1.3 Interfejsy VLAN

Tabela 20: Strona WBM „Ethernet Configuration" – grupa „VLAN Interfaces"

Parametr	Znaczenie
Name	Nazwa wybranego interfejsu VLAN

Parametr	Znaczenie
VLAN-ID	VLAN-ID wybranego interfejsu VLAN
Link	Przyporządkowany bridge wybranego interfejsu VLAN

3.5.1.1.4 Konfiguracja Port Mirror (PFC100 G2, PFC200 G2 - 2-Port, PFC300)

Tabela 21: Strona WBM „Ethernet Configuration" – grupa „Port Mirror Settings"

Parametr	Znaczenie	
Enabled	Włączanie/wyłączanie funkcji mirroringu (kopiowania) ruchu sieciowego pomiędzy portami	
	☐	Ruch sieciowy nie jest kopiowany (ustawienie fabryczne).
	☑	Ruch sieciowy jest kopiowany pomiędzy wybranymi portami.
Source	Port źródłowy kopiowanego ruchu sieciowego (X1 ... X<n>)	
Destination	Port docelowy kopiowanego ruchu sieciowego (X1 ... X<n>)	

3.5.1.1.5 Konfiguracja Storm Control (PFC100 G2, PFC200 G2 - 2-Port)

Tabela 22: Strona WBM „Ethernet Configuration" – grupa „Storm Control Settings"

Parametr	Znaczenie	
Broadcast Protection	Wartość graniczna dla pakietów typu Broadcast; Wartość domyślna: 1% maksymalnej przepustowości łącza	
Multicast Protection	Określa, czy ograniczenie ruchu dotyczy wyłącznie pakietów Broadcast, czy też łącznie pakietów Broadcast i Multicast.	
	☐	Ograniczenie liczby pakietów dotyczy wyłącznie pakietów Broadcast.
	☑	Ograniczenie liczby pakietów dotyczy łącznie pakietów Broadcast i Multicast.

3.5.1.1.6 Konfiguracja Storm Control (PFC200 G2 - 4-Port)

Tabela 23: Strona WBM „Ethernet Configuration" – grupa „Storm Control Settings"

Parametr	Znaczenie
Broadcast Protection	Wartość graniczna dla pakietów typu Broadcast; Wartość domyślna: 1 Mb
Multicast Protection	Wartość graniczna dla pakietów typu Multicast; Wartość domyślna: 1 Mb

3.5.1.1.7 Konfiguracja Storm Control (PFC300)

Tabela 24: Strona WBM „Ethernet Configuration" – grupa „Storm Control Settings"

Parametr	Znaczenie
Broadcast Protection	Wartość graniczna dla pakietów typu Broadcast; Wartość domyślna: 20 000 pakietów na sekundę
Multicast Protection	Wartość graniczna dla pakietów typu Multicast; Wartość domyślna: 20 000 pakietów na sekundę

3.5.1.1.8 Konfiguracja interfejsów Ethernet (PFC100 G2, PFC200 G2 - 2-Port)

Tabela 25: Strona WBM „Ethernet Configuration" – grupy „Ethernet Interface Configuration"

Parametr	Znaczenie
Interface X<n>	Dla każdego interfejsu zintegrowanego w sterowniku wyświetlany jest osobny obszar.

Parametr	Znaczenie	
Enabled	Aktywacja/dezaktywacja interfejsu	
	☐	Interfejs jest dezaktywowany.
	☑	Interfejs jest aktywny.
MAC Learning	Aktywacja/dezaktywacja funkcji "MAC Learning" dla interfejsu	
	☐	Funkcja „MAC Learning" jest dezaktywowana.
	☑	Funkcja „MAC Learning" jest aktywna.
Broadcast Protection Enabled	Aktywacja/dezaktywacja Broadcast-Protection	
	☐	Broadcast Protection jest dezaktywowany.
	☑	Broadcast Protection jest aktywowany.
Current Speed/Duplex	Aktualna prędkość transmisji i aktualny typ transmisji	
Speed/Duplex	Wybór prędkości transmisji oraz i typu transmisji; Lista dostępnych opcji jest generowana w zależności od urządzenia i interfejsu. Przy aktywowanej opcji „Autonegotiation" tryby łączeniowe negocjowane są automatycznie z urządzeniem przeciwstawnym.	

3.5.1.1.9 Konfiguracja interfejsu Ethernet (PFC200 G2 - 4-Port, PFC300)

Tabela 26: Strona WBM „Ethernet Configuration" – grupy „Ethernet Interface Configuration"

Parametr	Znaczenie	
Interface X<n>	Dla każdego interfejsu zintegrowanego w sterowniku wyświetlany jest osobny obszar.	
Enabled	Aktywacja/dezaktywacja interfejsu	
	☐	Interfejs jest dezaktywowany.
	☑	Interfejs jest aktywny.
MAC Learning	Aktywacja/dezaktywacja funkcji "MAC Learning" dla interfejsu	
	☐	Funkcja „MAC Learning" jest dezaktywowana.
	☑	Funkcja „MAC Learning" jest aktywna.
Broadcast Protection Enabled	Aktywacja/dezaktywacja Broadcast-Protection.	
	☐	Broadcast Protection jest dezaktywowany.
	☑	Broadcast Protection jest aktywowany.
Multicast Protection Enabled	Aktywacja/dezaktywacja Multicast Protection.	
	☐	Multicast Protection jest dezaktywowany.
	☑	Multcast Protection jest aktywowany.
Current Speed/Duplex	Aktualna prędkość transmisji i aktualny typ transmisji	
Speed/Duplex	Wybierz prędkość i metodę transmisji; Lista wyboru jest generowana w zależności od urządzenia i interfejsu. Przy aktywowanej opcji „Autonegotiation" tryby łączeniowe negocjowane są automatycznie z urządzeniem przeciwstawnym.	

3.5.1.2 Konfiguracja TCP/IP

3.5.1.2.1 Bridge Interfaces

Tabela 27: Strona WBM „TCP/IP Configuration“ – grupa „Bridge Interfaces“

Parametr	Znaczenie	
Bridge <n>	Ustawienia dla wybranego bridge'a	
Current IP Address	Aktualny adres IP	
Current Subnet Mask	Aktualna maska podsieci	
Current Default Gateway	Adres IP aktualnej domyślnej bramy	
IP Source	Wybierz adres IP.	
	Static IP	Statyczne adresowanie IP
	DHCP	Dynamiczne adresowanie IP przez DHCP
	BootP	Dynamiczne adresowanie IP przez BootP
Static IP Address	Wprowadzanie statycznego adresu IP; adres IP jest aktywny, gdy w polu wyboru **IP Source** zaznaczona jest „Static IP".	
Subnet Mask	Wprowadzanie maski podsieci; maska podsieci jest aktywna, gdy w polu wyboru **IP Source** zaznaczona jest „Static IP".	
Default Gateway	Wprowadzanie adresu IP bramy domyślnej	

3.5.1.2.2 Interfejsy Dummy

Tabela 28: Strona WBM „TCP/IP Configuration“ – grupa „Dummy Interfaces“

Parametr	Znaczenie	
Dummy <n>	Ustawienia dla wybranego interfejsu Dummy	
Current IP Address	Aktualny adres IP	
Current Subnet Mask	Aktualna maska podsieci	
IP Source	Wybierz adres IP.	
	Static IP	Statyczne adresowanie IP
Static IP Address	Wprowadzanie statycznego adresu IP; adres IP jest aktywny, gdy w polu wyboru **IP Source** zaznaczona jest „Static IP".	
Subnet Mask	Wprowadzanie maski podsieci; maska podsieci jest aktywna, gdy w polu wyboru **IP Source** zaznaczona jest „Static IP".	

3.5.1.2.3 VLAN-Interfaces

Tabela 29: Strona WBM „TCP/IP Configuration“ – grupa „VLAN Interfaces“

Parametr	Znaczenie	
VLAN <n>	Ustawienia wybranego interfejsu VLAN	
Current IP Address	Aktualny adres IP	
Current Subnet Mask	Aktualna maska podsieci	
IP Source	Wybierz adres IP.	
	Static IP	Statyczne adresowanie IP
	DHCP	Dynamiczne adresowanie IP
Static IP Address	Wprowadzanie statycznego adresu IP; adres IP jest aktywny, gdy w polu wyboru **IP Source** zaznaczona jest „Static IP".	
Subnet Mask	Wprowadzanie maski podsieci; maska podsieci jest aktywna, gdy w polu wyboru **IP Source** zaznaczona jest „Static IP".	

3.5.1.2.4 Serwer DNS

Sterownik może korzystać z maksymalnie 3 aktywnych serwerów DNS. Serwery DNS mogą być przypisane przez DHCP lub ręcznie.

Rzeczywiste zastosowanie serwerów DNS polega na kolejnym połączeniu przypisanych przez DHCP serwerów DNS z przypisanymi ręcznie serwerami DNS.
Pierwszy serwer DNS, który został przypisny przez DHCP, otrzymuje najwyższy priorytet.

Wyświetlanie przypisanych serwerów DNS oraz ręczne przypisywanie dodatkowych serwerów DNS jest możliwe np. przez stronę WBM „Konfiguracja TCP/IP" w grupie „Serwer DNS".

Tabela 30: Strona WBM „TCP/IP Configuration" – grupa „DNS Server"

Parametr	Znaczenie
Active	Aktywny serwer DNS; Indeks odzwierciedla kolejność zapytań.
Assigned by DHCP	Serwery DNS przypisane przez DHCP (lub BootP); Jeśli żaden serwer DNS nie został przypisany przez DHCP (lub BootP), wyświetli się komunikat „no DNS Servers assigned by DHCP".
Assigned by user	Adresy serwerów DNS wprowadzonych przez użytkownika; Jeśli nie został wprowadzony żaden serwer, pojawi się komunikat „no DNS Servers configured".

3.5.1.3 Nazwa hosta/domeny

3.5.1.3.1 Nazwa hosta

Bez konfiguracji nazwy hosta sterownik otrzymuje standardową nazwę, w skład której wchodzą ostatnie trzy wartości adresu MAC sterownika. 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.

W przypadku kilku interfejsów sieciowych z DHCP nazwa hosta jest przejmowana z interfejsu sieciowego (bridge lub Wwan) o najwyższym priorytecie. Priorytet jest ustawiany alfanumerycznie przez nazwę interfejsu sieciowego. Tak więc Bridge1 ma najwyższy priorytet, a kolejne to Bridge2, Bridge3, ..., Wwan0.

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.

Ustawienia nazwy hosta są możliwe np. na stronie WBM „Configuration of Host- and Domain Name" w grupie „Host Name".

Tabela 31: Strona WBM „Configuration of Host and Domain Name" – grupa „Hostname"

Parametr	Znaczenie
Currently used	Aktualna nazwa hosta
Configured	Wprowadzanie opcjonalnej nazwy hosta
[Clear]	Usuwanie opcjonalnej nazwy hosta i przywracanie wartości domyślnej

3.5.1.3.2 Nazwa domeny

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

Ustawienia nazwy domeny można wykonać np. na stronie WBM „Configuration of Host- and Domain Name" w grupie „Domain Name".

Tabela 32: Strona WBM „Configuration of Host and Domain Name“ – grupa „Domain Name“

Parametr	Znaczenie
Currently used	Aktualnie używana nazwa domeny
Configured	Wprowadzanie opcjonalnej nazwy domeny
[Clear]	Usuwanie opcjonalnej nazwy domeny

3.5.1.4 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. 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. Trasa routingu składa się z następujących danych:

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

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 zaznaczyć „Enabled“ w grupie „IP Forwarding through multiple interfaces“. W tym przypadku sterownik może pełnić funkcję routera.

Przy komunikacji sieciowej wykorzystującej funkcję przesyłania danych przy pomocy rutera należy pamiętać, że nie tylko ruter, lecz także punkty końcowe muszą otrzymać odpowiednie parametry routowania. Parametry routowania punktów końcowych powinny zapewniać przesyłanie żądanych pakietów danych zarówno przy nawiązywaniu połączenia, jak i przy odpowiedziach przez rutera.

Przekazywanie pakietów danych IP można ustawić np. na stronie WBM „Routing" w grupie "IP Forwarding through multiple interfaces".

Tabela 33: Strona WBM „Routing“ – grupa „IP Forwarding through multiple interfaces“

Parametr	Znaczenie	
Enabled	Umożliwia przekazywanie pakietów danych IP pomiędzy różnymi interfejsami sieciowymi	
	☐	Ustawienia w sekcji „Static Routes” są stosowane również wtedy, gdy pakiety IP docierające do sterownika przez jeden interfejs sieciowy nie mogą być przekazywane dalej przez inny interfejs.
	☑	Pakiety IP mogą być przekazywane między interfejsami. Mogą być wymagane dodatkowe ustawienia.

3.5.1.4.1 Routing statyczny

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 sieciowych przeznaczonego do przekazania zawsze wybierany jest wpis routingu, który najdokładniej odpowiada parametrom adresu docelowego (Destination Address) i maski docelowej (Destination Mask), czyli posiada najbardziej szczegółowe dopasowanie. Brama domyślna odpowiada najbardziej ogólnej trasie routingu. Wszystkie pakiety danych o adresie docelowym (Destination Address) i adresie maski (Destination Mask), dla których nie istnieje specyficzna trasa routingu, wysyłane są do tej bramy domyślnej.

Brama domyślna

Bramy domyślne, zwane też domyślnymi routingami, ustawiane są zasadniczo w połączeniu z konfiguracją IP. Każda brama domyślna posiada metrykę, która jest unikatowa wśród wszystkich bram domyślnych. Bridge <n> posiada metrykę 19+<n>. Brama domyślna może być także definiowana przez konfigurację trasy, np. w celu zdefiniowania indywidualnej metryki. W oknie „Destination Address“ powinna być wpisana wartość „default“, a w oknie „Destination Mask“ wartość „0.0.0.0“.

Routing

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.

Alternatywnie w polu „Interface“ można podać bridge, modem lub VPN, przez który przesyłane są wszystkie pakiety danych kierowane na „Destination Address“. Edycja pola „Interface“ jest opcjonalna. Nie trzeba definiować pola „Gateway Adress“, „Interface“, ani obu tych pól równocześnie.

Jeśli adres IP bramy leży poza zakresem adresów osiągalnym dla sterownika, odpowiednia trasa nie zostaje aktywowana. Dotyczy to także tras, przy których podany jest interfejs, który np. nie jest aktywny podczas konfiguracji bridge'a.

Każdej trasie 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 zadana dla sterownika.

Przykład trasy do 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 routingu

Przykład trasy:

Routing 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 routingu

Przykład trasy przez interfejs:

W poniższym przykładzie należy podać trasę do hosta o adresie IP 192.168.1.2. Trasa biegnie przez interfejs br1, odpowiadający bridge'owi 2. Aby w sterowniku z aktywowanym brige'em 2 skonfigurować trasę do hosta docelowego przez bridge 2, 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 Metric:	20	Priorytet routingu
Interfejs:	br1	Interfejs, przez który kierowany jest pakiet

Ustawienia tras statycznych można wprowadzić na stronie WBM „Routing" - grupa "Custom Routes".

Dla każdej skonfigurowanej trasy statycznej wyświetlany jest osobny obszar. Gdy nie zostały wprowadzone statyczne trasy, wyświetlana jest informacja „no custom routes".

Tabela 34: Strona WBM „Routing" – grupa „Custom Routes"

Parametr	Znaczenie	
Enabled	Zastosowanie wybranej trasy	
	☐	Trasa nie jest zastosowana.
	☑	Trasa jest zastosowana.
Destination Address	Adres docelowy urządzenia	
	Default	Dostępni są dowolni uczestnicy komunikacji sieciowej.
	Network address	Dostępne jest tylko określone urządzenie lub urządzenie z danej puli adresów.

Parametr	Znaczenie
Destination Mask	Maska podsieci urządzenia Jeśli Destination Address jest zdefiniowany jako „default“, należy tu wpisać wartość „0.0.0.0“.
Gateway Address	Adres bramy Jeśli pole „Interface“ jest puste, należy tu wpisać wartości. Jeśli w polu „Interface“ wpisana jest wartość, wypełnienie tego pola jest opcjonalne.
Gateway Metric	Metryka trasy 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. Najmniejsza wartość wynosi 0. Największa wartość to $2^{32} - 1 = 4.294.967.295$.
Interfejs	Interfejs, przez który prowadzone są pakiety kierowane do Destination Address. Można użyć bridge'ów (br0 … br3), modemu (wwan0) lub nazwy interfejsu VPN. Jeśli pole „Gateway Address" jest puste, należy je wypełnić. Jeśli w polu „Gateway Address“ wpisana jest wartość, wypełnienie tego pola jest opcjonalne.

3.5.1.4.2 Trasy dynamiczne

Oprócz ręcznej konfiguracji tras można także ustawiać bramy domyślne przy pomocy odpowiedzi DHCP. Wszystkie bramy domyślne nadane przez DHCP otrzymują unikatową metrykę.

Przydzielanie metryki rozpoczyna się od 10 i odbywa się w zależności od interfejsu sieciowego, przez który otrzymana jest odpowiedź DHCP. Metryka jest przydzielana rosnąco, na podstawie alfanumerycznego sortowania nazw interfejsów sieciowych (np. br0, br1, … wwan0).

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 specyficzna trasa routingu, sterownik wysyła do bramy 192.168.1.2. Serwer DHCP musi przy rozdziale uwzględnić oprócz adresu IP i maski sieci, 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.

Wszystkie bramy domyślne otrzymane przez DHCP wyświetlane są na stronie WBM „Routing" - grupa „Dynamic Routes (assigned by DHCP)".

Dla każdej trasy dynamicznej wyświetlany jest osobny obszar. Jeśli poprzez DHCP nie została odebrana żadna trasa dynamiczna, wyświetlany jest komunikat „no dynamic route“.

Tabela 35: Strona WBM „Routing" – grupa „Dynamic Routes (assigned by DHCP)“

Parametr	Znaczenie
Destination Address	Adres docelowy urządzenia
Destination Mask	Maska podsieci urządzenia
Gateway Address	Adres bramy
Gateway Metric	Metryka routingu
Interfejs	Interfejs, przez który kierowane są pakiety na adres docelowy

3.5.1.4.3 IP-Masquerading

Oprócz konfiguracji tras statycznych sterownik wspiera 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 przesyłane są przez sterownik dalej, sieć znajdująca się za sterownikiem zostaje ukryta pod jednym adresem.

Tabela 36: Strona WBM „Routing" – grupa „IP-Masquerading"

Parametr	Znaczenie	
Enabled	Stosowanie IP-Masquerading	
	☐	IP-Masquerading nie jest zastosowany.
	☑	IP-Masquerading jest zastosowany.
Interfejs	Wybierz jedną z podanych nazw dla interfejsu sieciowego Przy wybraniu opcji „other" możliwa jest dowolna nazwa interfejsu sieciowego.	

3.5.1.4.4 Przekierowanie portów

Sterownik dopuszcza również konfigurację parametrów przekierowania portów. 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.

Tabela 37: Strona WBM „Routing" – grupa „Port Forwarding"

Parametr	Znaczenie	
Enabled	Użyj przekierowania portów	
	☐	Port Forwarding nie jest zastosowany.
	☑	Port Forwarding jest zastosowany.
Interfejs	Wybierz jedną z podanych nazw dla interfejsu sieciowego Przy wybraniu opcji „other" możliwa jest dowolna nazwa interfejsu sieciowego.	
Port	Wybór portu, po którym przesyłane pakiety danych mają dotrzeć do produktu.	
Protocol	Wybierz protokół, który ma być uwzględniony dla Port-Forwarding; Do wyboru są TCP, UDP lub oba protokoły.	
Destination Address	Wybierz adres sieciowy urządzenia docelowego Ten adres zastępuje pierwotny adres docelowy pakietu danych.	
Destination Port	Wybierz numer portu urządzenia docelowego Wartość ta zastępuje pierwotny port docelowy pakietu danych.	

3.5.2 Bezpieczeństwo sieci

3.5.2.1 Użytkownicy i hasła

Istnieją różne grupy użytkowników, które mogą być wykorzystywane do realizacji różnych zadań.

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

Wskazówka

Zmienić hasła!

Ustawione fabrycznie, standardowe hasła podane w niniejszej instrukcji obsługi nie stanowią wystarczającego zabezpieczenia!

- Należy zmienić te hasła stosownie do potrzeb.

Usługi i użytkownicy

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

Tabela 38: Usługi i użytkownicy

	Użytkownik			
Usługa	**Linux®**			**SNMP**
	root	**admin**	**User**	
Web Based Management (WBM)	x	x	x	
Konsola Linux®	x	x	x	
Console-Based-Management (CBM)	x			
CODESYS		x		
FTP	x	x	x	
FTPS	x	x	x	
SSH	x	x	x	
SNMP				x

Grupa użytkowników Linux®

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

Tabela 39: Użytkownik 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 WBM lub połączenie terminalowe.

Wskazówka

Zmienić hasła!

Ustawione fabrycznie, standardowe hasła podane w niniejszej instrukcji obsługi nie stanowią wystarczającego zabezpieczenia!

- Należy zmienić te hasła stosownie do potrzeb.

ⓘ Wskazówka

Dopuszczalne znaki w hasłach

Hasło może zawierać tylko następujące znaki:
małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9) oraz znaki spcjalne (! " # $ % & ' ( ) * + , . / : ; < = > ? @ [ ] ^ _ ` { } | ~ –).

ⓘ Wskazówka

Uwzględnić długość hasła!

Hasło do CODESYS musi zawierać więcej niż 1 znak i mniej niż 60 znaków!

Dla zalogowanego użytkownika Linux® hasło można zmienić przez stronę WBM „WBM User Configuration" w grupie „Change Passwords".

Tabela 40: Strona WMB „Users Configuration" – grupa „Change Passwords"

Parametr	Znaczenie
Old Password	Wprowadzanie aktualnie używanego hasła do uwierzytelnienia.
New Password	Wprowadzanie nowego hasła.
Confirm Password	Wprowadzanie nowego hasła do kontroli.

Grupa użytkowników SNMP

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

3.5.2.2 Uwierzytelnianie serwera WWW

Strony WBM można otwierać przy pomocy protokołu internetowego 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.

3.5.2.2.1 Szyfrowanie TLS

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

Dopuszczalne wersje TLS i metody kryptograficzne są konfigurowalne („Standard"/„Strong"). Ustawienie „Standard" zezwala na wersje TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 a także metody kryptograficzne, które obecnie nie są już uważane za bezpieczne. Użycie jest zalecane tylko w przypadku zgodności wstecznej ze starszymi systemami.

Przy ustawieniu „Strong" serwer internetowy zezwala tylko na wersję TLS 1.2, TLS1.3 i na silne algorytmy. Starsze oprogramowanie i starsze systemy operacyjne mogą nie obsługiwać protokołu TLS 1.2, TLS 1.3 i algorytmów szyfrowania.

ⓘ Wskazówka

Techniczna dyrektywa TR-02102 BSI

Zasady dotyczące ustawienia „Strong" są oparte na wytycznej technicznej TR-02102 Federalnego Urzędu ds. Bezpieczeństwa Informacji. Wytyczne znajdują się na stronie: **www.bsi.bund.de**.

ⓘ Wskazówka

Wytyczne BSI dotyczące migracji do TLS 1.2 lub TLS 1.3

Wytyczne Federalnego Urzędu ds. Bezpieczeństwa Informacji dotyczące migracji do TLS 1.2 lub TLS 1.3 zawierają „matryce zgodności", które określają, które oprogramowanie jest zgodne z TLS 1.2 lub TLS 1.3. Przewodnik można znaleźć na stronie: **www.bsi.bund.de**.

Dozwolone dla HTTPS algorytmy kryptograficzne oraz obsługiwane wersje TLS można zmieniać w grupie „TLS Configuration" na stronie WBM „Security Settings".

Tabela 41: Strona WBM „Security Settings" – grupa „TLS Configuration"

Parametr	Znaczenie	
TLS Configuration	Ustawianie dozwolonych wersji TLS i procedur kryptograficznych dla HTTPS	
	standard	Serwer WWW zezwala na wersje TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 oraz innych algorytmów kryptograficznych, które obecnie nie są już uznawane za bezpieczne.
	Strong	Serwer WWW zezwala tylko na wersję TLS 1.2, TLS 1.3 i na silne algorytmy.

3.5.2.3 Certyfikaty Root

Przy komunikacji szyfrowanej przez TLS w celu sprawdzania wierzytelności 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.

Zobacz też

Aktualizacja certyfikatów Root [▸ 97]

3.5.2.4 Firewall

3.5.2.4.1 Ustawienia globalne Firewall

Tabela 42: Strona WBM „General Firewall Configuration“ – grupa „Global Firewall Parameter“

Parametr	Znaczenie
Firewall enabled entirely	Aktywacja/dezaktywacja pełnej funkcjonalności firewalla. To ustawienie ma najwyższy priorytet. Gdy firewall jest wyłączony, wszystkie inne ustawienia nie mają bezpośredniego znaczenia. Konfiguracja innych parametrów jest mimo to możliwa, aby przed włączeniem funkcji Firewall można było prawidłowo ustawić jej parametry. To ustawienie jest niezależne od ustawienia opcji „Filter enabled" w grupie „MAC address filter state Bridge <n>" na stronie „MAC address filter state Bridge".
ICMP echo broadcast protection	Aktywacja/dezaktywacja zabezpieczenia „ICMP echo broadcast“
Max. UDP connections per second	Wprowadzanie maksymalnej liczby połączeń UDP na sekundę
Max. TCP connections per second	Wprowadzanie maksymalnej liczby połączeń TCP na sekundę

ⓘ Wskazówka

Usługi CODESYS są odrzucane przy włączonej zaporze sieciowej, jeśli nie skonfigurowano filtrów użytkownika!

Jeśli wykorzystywane są usługi CODESYS (np. Modbus, OPC-UA, SNMP lub IIOT), w konfiguracji firewalla należy utworzyć odpowiednie filtry użytkownika dla tych usług. Filtry użytkownika muszą być skonfigurowane w taki sposób, aby odpowiednie porty były akceptowane.

3.5.2.4.2 Ustawienia zapory sieciowej powiązane z interfejsem

Tabela 43: Strona WBM „Interface Configuration“ – grupa „Firewall Configuration Bridge <n> / VPN / WAN“

Parametr	Znaczenie
Firewall enabled for Interface	Aktywowanie/dezaktywowanie funkcji Firewall dla poszczególnych interfejsów
ICMP echo protection	Aktywacja/dezaktywacja zabezpieczenia „ICMP echo“ dla poszczególnych interfejsów
ICMP echo limit per second	Wprowadzanie maksymalnej liczby „ICMP pings" na sekundę. „0“ = „Disabled“
ICMP burst limit (0=disabled)	Wprowadzanie maksymalnej liczby „ICMP echo burst" na sekundę
Service Configuration	Aktywacja/dezaktywacja funkcji firewall dla poszczególnych usług
FTP/FTPES	Nie każda z przedstawionych tu usług jest dostępna dla każdego produktu. Same usługi muszą być włączane i wyłączane osobno przez stronę „Ports and Services“.
FTPS (implicit)	
HTTP	
HTTPS	
I/O Check	
PLC Runtime	
WebVisu – HTTP (port 8080)	
WebVisu – HTTPS (port 8081)	
SSH	
SNMP	
OPC UA (port 4840)	
BACnet (port 47808)	
PROFINET IO	

Parametr	Znaczenie
DNP3 (port 20000)	
IEC60870-5-104 (port 2404)	
IEC61850 (port 102)	

W przypadku sterowników z funkcjonalnością telesterowania otwierane są standardowo porty Firewall wymienione w tabeli poniżej. Przez te porty mogą być realizowane odpowiednie usługi telesterowania, bez blokowania ich komunikacji przez Firewall.

Tabela 44: Porty dla funkcjonalności telecontrol

Protokół	Port
DNP3	20000
IEC60870-5-104	2404
IEC 61850	102

3.5.2.4.3 Filtr adresu MAC

Ustawienia globalne

Tabela 45: Strona WBM „Configuration of MAC address filter“ – grupa „Global MAC address filter state“

Parametr	Znaczenie
Filter enabled	Aktywowanie/dezaktywowanie globalnego filtra adresów MAC

Ustawienia powiązane z bridge'em

Tabela 46: Strona WBM „Configuration of MAC address filter“ – grupa „MAC address filter state Bridge <n>“

Parametr	Znaczenie
Filter enabled	Aktywacja/dezaktywacja filtra adresu MAC dla danego bridge'a; To ustawienie jest niezależne od ustawienia „Firewall enabled entirely" w grupie „Global Firewall Parameter" na stronie „General Firewall Configuration".

Biała lista filtrów adresu MAC

„MAC Address Filter Whitelist“ otrzymuje dwa domyślne wpisy o następujących wartościach:
- Opis: Wszystkie urządzenia WAGO
  Adres MAC: 00:30:DE:00:00:00
  Maska MAC: ff:ff:ff:00:00:00
- Opis: Enable docker bridges
  Adres MAC: 02:42:00:00:00:00
  Maska MAC: ff:ff:00:00:00:00

Po włączeniu pierwszego domyślnego wpisu można komunikować ze sobą w sieci różne produkty WAGO.

Dla każdego skonfigurowanego filtra wyświetlany jest osobny obszar.
Jeśli nie został utworzony filtr adresu MAC, wyświetlana jest informacja „no MAC Address filters".

W obszarze „Add filter to whitelist" można utworzyć maksymalnie 10 filtrów adresów MAC.

Tabela 47: Strona WBM „Configuration of MAC address filter“ – grupa „MAC address filter whitelist“

Parametr	Znaczenie
Description	Opis urządzeń lub obszary, które przy ogólnie aktywowanym firewallu można odblokować przez aktywację filtra. Opis widoczny jest tylko przy wpisach, które pojawiły się w ustawieniu fabrycznym.

Parametr	Znaczenie
MAC address	Adres MAC pozycji na liście
MAC mask	Maska MAC pozycji na liście
Filter enabled	Aktywacja/dezaktywacja filtra dla pozycji na liście

3.5.2.4.4 User Filter

Dla każdego skonfigurowanego filtra wyświetlany jest osobny obszar.
Jeśli użytkownik nie został utworzony, wyświetlana jest informacja „no user filters".

W obszarze „Add new user filter" można utworzyć maksymalnie 10 filtrów użytkownika.
W polach należy wpisać wartości, które mają być użyte dla filtra.
Należy wpisać co najmniej 1 wartość, pozostałe pola mogą zostać puste.

Tabela 48: Strona WBM „Configuration of User Filter" – grupa „User filter"

Parametr	Znaczenie	
Policy	Zezwól/wyłącz urządzenie sieciowe przez filtr	
	Allow	Urządzenie sieciowe jest dopuszczone.
	Drop	Urządzenie sieciowe jest wykluczone.
Source IP address	Źródłowy adres IP dla filtra	
Source Netmask	Maska sieci źródłowej dla filtra	
Source Port	Numer portu źródłowego dla filtra	
Destination IP address	Docelowy adres IP dla filtra	
Destination Netmask	Maska sieci docelowej dla filtra	
Destination Port	Numer portu docelowego dla filtra	
Protocol	Protokoły dla filtra	
	TCP/UDP	Serwisy TCP i UDP są filtrowane.
	TCP	Serwis TCP jest filtrowany.
	UDP	Serwis UDP jest filtrowany.
Input interface	Interfejsy do filtra	
	Any	Wszystkie interfejsy są filtrowane.
	Bridge <n>	Filtrowane są interfejsy przypisane do bridge'a <n>. Wyświetlane są tylko skonfigurowane bridge.
	VPN	Interfejs VPN jest filtrowany.

ⓘ Wskazówka

Usługi CODESYS są odrzucane przy włączonej zaporze sieciowej, jeśli nie skonfigurowano filtrów użytkownika!

Jeśli wykorzystywane są usługi CODESYS (np. Modbus, OPC-UA, SNMP lub IIOT), w konfiguracji firewalla należy utworzyć odpowiednie filtry użytkownika dla tych usług. Filtry użytkownika muszą być skonfigurowane w taki sposób, aby odpowiednie porty były akceptowane.

3.5.3 Usługi sieciowe

3.5.3.1 Klient DHCP

Poprzez klienta DHCP sterownik może pobierać parametry sieci z zewnętrznego serwera DHCP.

Pobierane są następujące parametry:

- Adres IP
- Maska podsieci
- Router/Gateway
- Hostname
- domena
- DNS server
- Serwer NTP

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

W przypadku kilku interfejsów sieciowych z DHCP nazwa hosta jest przejmowana z interfejsu sieciowego (bridge lub Wwan) o najwyższym priorytecie. Priorytet jest ustawiany alfanumerycznie przez nazwę interfejsu sieciowego. Tak więc Bridge1 ma najwyższy priorytet, a kolejne to Bridge2, Bridge3, ..., Wwan0.

3.5.3.2 DHCP server

Oferowana przez sterownik usługa serwera DHCP 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 obu interfejsów, a w trybie „Separated" definiowane są dla każdego z interfejsów osobno.

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

Tabela 49: Lista parametrów wysyłanych przez DHCP

Parametry	Znaczenie
Adres IP	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.
Maska podsieci	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.
Adres broadcast	Adres IP, przy pomocy 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 przez protokół zobowiązane do wysłania ponownego zapytania po upływie połowy czasu ważności ustawień sieciowych. Lease-Time jest konfigurowany w WBM.

Parametry	Znaczenie
Hostname	Nazwa sieci przesyłana jest do urządzenia. Zazwyczaj urządzenie wysyła swoją nazwę wraz z zapytaniem o adres IP. Wykorzystywana jest ona potem przez serwer DHCP w odpowiedziach.
Nazwa serwera	Serwer DHCP przekazuje swój własny adres IP jako serwer DNS do urządzenia w sieci.
Brama domyślna	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 przez DHCP nadane kolejne parametry, serwer DHCP musi być konfigurowany 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".

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

Tabela 50: Strona WBM „DHCP Server Configuration" – grupa „DHCP Configuration Bridge <n>"

Parametr	Znaczenie	
Service active	Aktywacja/dezaktywacja usługi serwera DHCP dla bridge <n>	
	☐	Usługa serwera DHCP dla bridge <n> nie jest aktywowana.
	☑	Usługa serwera DHCP dla bridge <n> jest aktywowana.
Start IP for Range	Wprowadzanie wartości początkowej dostępnego zakresu adresów IP.	
End IP for Range	Wprowadzanie wartości końcowej dostępnego zakresu adresów IP.	
Lease time (min)	Wprowadzanie czasu dzierżawy w minutach. Ustawienia fabryczne: 120 minut	
Static Hosts	Statyczne przypisania identyfikatorów MAC-ID lub nazw hostów do adresów IP; Jeśli brak przypisania, wyświetlany jest komunikat "No static hosts configured".	
Add Static Host	Dodawanie statycznych przyporządkowań adresów MAC lub nazw hosta do adresów IP; możliwe jest maks. 15 przyporządkowań.	
MAC Address or Hostname	Wpisywanie adresu MAC lub nazwy hosta; np. "01:02:03:04:05:06=192.168.1.20"lub "hostname=192.168.1.20".	
IP Address	Wprowadzanie adresu IP	

3.5.3.3 Serwer DNS

Oferowana przez sterownik usługa serwera DNS 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 nielokalne, 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 (zoptymalizowane pod względem przepustowości).
  W trybie przekaźnikowym zapytania są przekazywane bezpośrednio do nadrzędnego serwera nazw.

- 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".

Tabela 51: Strona WBM „Configuration of DNS Server" – grupa „DNS Server"

Parametr	Znaczenie	
Service active	Aktywacja/dezaktywacja usługi serwera DNS	
	☐	Usługa serwera DNS jest nieaktywna.
	☑	Usługa serwera DNS jest aktywowana.
Mode	Ustawianie trybu pracy;	
	Proxy	Zapytania buforowane są w celu optymalizacji przepustowości komunikacji.
	Relay	Wszystkie zapytania są przesyłane bezpośrednio dalej.
Static Hosts	Statyczne przyporządkowanie nazw hostów do adresów IP; Jeśli nie ma przyporządkowania, wyświetlana jest informacja „No static hosts configured".	
Add Static Host	Statyczne przyporządkowywanie adresów IP do nazw hosta; możliwe jest maks. 10 przyporządkowań.	
IP Address	Wprowadzanie adresu IP; np. "192.168.1.20:hostname"	
Hostname	Wprowadzanie nazwy hosta.	

3.5.3.4 SNMP

SNMP (Simple-Network-Management-Protokoll) jest standardowym protokołem do monitorowania i zarządzania urządzeniami w sieci TCP/IP. Służy on do transportu danych kontrolnych, umożliwiających wymianę informacji o zarządzaniu, statusie i statystycznych pomiędzy poszczególnymi komponentami sieci a systemem zarządzania.

Protokół jest dostępny w wersjach v1, v 2c i v3. Wersje są od siebie niezależne i mogą być aktywowane i używane równolegle lub pojedynczo.

Ogólne ustawienia dla SNMP można wprowadzić np. na stronie WBM „Configuration of general SNMP parameters".

Tabela 52: Strona WBM „Configuration of General SNMP Parameter" – grupa „General SNMP Configuration"

Parametr	Znaczenie	
Service active	Aktywowanie/dezaktywowanie usługi SNMP	
	☐	Usługa SNMP jest dezaktywowana.
	☑	Usługa SNMP jest aktywna.
Name of Device	Wprowadzanie nazwy produktu (sysName)	
Description	Wprowadzanie opisu produktu (sysDescription).	
Physical Location	Wprowadzanie lokalizacji produktu (sysLocation).	
Contact	Wprowadzanie kontaktowego adresu e-mail (sysContact)	
ObjectID	Wprowadzanie Object ID.	

3.5.3.4.1 SNMP v1/v2c

SNMP v1 i v2c jest wymianą wiadomości w ramach grupy o wspólnej nazwie Community.

Nazwa społeczności (Community Name) służy do definiowania relacji między menedżerami SNMP (odbiornikami komunikatów Trap) a agentami SNMP. Każda z tych relacji tworzy tzw. społeczność (community). Grupy Community sterują identyfikacją i dostępem między uczestnikami SNMP.
Odbiornik trapów może analizować nazwę Community.
Aby móc korzystać z protokołu SNMP, zawsze musi być podana prawidłowa nazwa Community.
Nazwa Community może mieć maksymalnie 32 znaki i nie może zawierać spacji. Wartość standardowa: „public“

Prawa dostępu dla Społeczności i wersji SNMP, przez którą mają być wysyłane komunikaty trap, można ustawić.

Ustawienia parametrów SNMP v1/v2c można wprowadzać np. na stronie WBM „Configuration of SNMP v1/v2c Parameters".

SNMP Community

Dla każdej skonfigurowanej Społeczności wyświetlany jest osobny obszar „Community <n>“. Jeśli nie skonfigurowano Społeczności, wyświetlana jest informacja „(no Communities configured)“.

W obszarze „Add new Community“ możesz dodać nową Społeczność.

Tabela 53: Strona WBM „Configuration of SNMP v1/v2c Parameters“ – grupa „Communities“

Parametr	Znaczenie
Name	Nazwa Społeczności do konfiguracji managera SNMP
Access	Prawa dostępu dla Społeczności; Możliwe wartości to: ▪ ReadOnly ▪ ReadWrite

Trap Receiver

Dla każdego skonfigurowanego odbiorcy komunikatów trap wyświetlany jest osobny obszar „Trap Receiver <n>“.
Jeśli odbiorca komunikatów trap nie został skonfigurowany, wyświetlana jest informacja „(no Trap Receivers configured)“.

W obszarze „Add new Trap Receiver" można utworzyć nowego odbiorcę komunikatów trap.

Tabela 54: Strona WBM „Configuration of SNMP v1/v2cparameters" – grupa „Trap Receivers"

Parametr	Znaczenie
Host	Nazwa hosta lub adres IP nowego odbiorcy komunikatów trap (Managementstation)
Community Name	Nazwa Społeczności do konfiguracji odbiorcy komunikatów trap
Wersja	Wersja SNMP, przez którą powinny być wysyłane komunikaty trap; Możliwe wartości: ▪ v1 ▪ v2c

3.5.3.4.2 SNMP v3

SNMP v3 jest stosowany w sieciach wymagających wysokiego poziomu bezpieczeństwa. Dane użytkowe komunikatów SNMP mogą być szyfrowane w czasie transferu, a wartości zadane i zapisywane nie mogą być podsłuchiwane przez ETHERNET.

Możliwe jest skonfigurowanie uwierzytelnienia za pomocą hasła i kodu szyfrowania.

Nazwa użytkownika musi być unikalna, już istniejąca nazwa użytkownika nie zostanie zaakceptowana przy ponownym wprowadzeniu.
Nazwa użytkownika musi zawierać co najmniej 8 znaków i nie może przekraczać 32 znaków.
Nazwa użytkownika może zawierać małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9), znaki specjalne (! () * ~ ' . - _), ale nie może zawierać spacji.

Hasło (Authentication Key) oraz kod szyfrowania (Privacy Key) muszą zawierać co najmniej 8 znaków i nie mogą przekraczać 32 znaków.
Hasło i kod szyfrowania mogą zawierać małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9), znaki specjalne (! () * ~ ' . - _), ale nie mogą zawierać spacji.

Ustawienia dla parametrów SNMP v3 są dostępne np. na stronie WBM "Configuration of SNMP v3 Parameters".

User

Dla każdego skonfigurowanego użytkownika v3 wyświetlany jest osobny obszar „User <n>".
Jeśli użytkownik v3 nie został skonfigurowany, wyświetlana jest informacja „(no Users configured)".

W obszarze „Add new v3 User" można wpisać nowego użytkownika v3.
Można wpisać maksymalnie 10 użytkowników.

Tabela 55: Strona WBM „Configuration of SNMP v3 Parameters" – grupa „User"

Parametr	Znaczenie
Security Authentication Name	Nazwa użytkownika
Authentication Type	Typ uwierzytelnienia dla pakietów SNMP v3; Możliwe wartości: ▪ Brak uwierzytelnienia („None") ▪ Message Digest 5 ("MD5") ▪ Secure Hash Algorithm ("SHA", "SHA224", "SHA256", "SHA384", "SHA512")
Authentication Key	Hasło do uwierzytelnienia
Privacy	Algorytm szyfrowania dla wiadomości SNMP; Możliwe wartości: ▪ Brak szyfrowania („None") ▪ Data Encryption Standard ("DES") ▪ Advanced Encryption Standard ("AES", "AES128", "AES192", "AES192C", "AES256", "AES256C")
Privacy Key	Kod szyfrowania
Access	Prawa dostępu dla użytkownika v3; Możliwe wartości: ▪ ReadOnly ▪ ReadWrite

Trap Receiver

Dla każdego skonfigurowanego odbiorcy komunikatów trap v3 wyświetlany jest osobny obszar „Trap Receiver <n>".
Jeśli odbiorca komunikatów trap v3 nie został skonfigurowany, wyświetlana jest informacja „(no Trap Receivers configured)".

W obszarze „Add new Trap Receiver" można utworzyć nowego odbiorcę trap v3.
Można utworzyć maksymalnie 10 odbiorców komunikatów trap.

Tabela 56: Strona WBM „Configuration of SNMP v3 Parameters“ – grupa „Trap Receivers“

Parametr	Znaczenie
Security Authentication Name	Nazwa użytkownika
Authentication Type	Typ uwierzytelnienia dla pakietów SNMP v3; Możliwe wartości: ▪ Brak uwierzytelnienia („None“) ▪ Message Digest 5 ("MD5") ▪ Secure Hash Algorithm ("SHA", "SHA224", "SHA256", "SHA384", "SHA512")
Authentication Key	Hasło do uwierzytelnienia
Privacy	Algorytm szyfrowania dla wiadomości SNMP; Możliwe wartości: ▪ Brak szyfrowania („None“) ▪ Data Encryption Standard ("DES") ▪ Advanced Encryption Standard ("AES", "AES128", "AES192", "AES192C", "AES256", "AES256C")
Privacy Key	Kod szyfrowania
Host	Nazwa hosta lub adres IP odbiorcy komunikatów trap v3

3.5.3.5 FTP/FTPES

Tabela 57: Strona WBM „Configuration of Network Services“ – grupa „FTP“

Parametr	Znaczenie	
Service active	Aktywacja/dezaktywacja serwera FTP	
	☐	Usługa FTP jest nieaktywna; Ustawienia fabryczne
	☑	Usługa FTP jest aktywna.

Tabela 58: Strona WBM „Configuration of Network Services“ – grupa „FTPES (explicit FTPS)“

Parametr	Znaczenie	
Service active	Aktywacja/dezaktywacja usługi FTPES (explicit FTPS);	
	☐	Usługa FTPES jest nieaktywna; Ustawienia fabryczne
	☑	Usługa FTPES jest aktywna.

3.5.3.6 HTTP / HTTPS

Tabela 59: Strona WBM „Configuration of Network Services“ – grupa „HTTP“

Parametr	Znaczenie	
Service active	Aktywacja/dezaktywacja serwisu HTTP	
	☐	Serwis HTTP jest dezaktywowany; Ustawienia fabryczne
	☑	Serwis HTTP jest aktywowany.

Tabela 60: Strona WBM „Configuration of Network Services“ – grupa „HTTPS“

Parametr	Znaczenie	
Service active	Status serwisu HTTPS	
	☐	Usługa HTTPS jest nieaktywna.
	☑	Serwis HTTPS jest aktywowany.

3.5.3.7 I/O-CHECK

Wskazówka

Zamknąć nieużywane porty i usługi!

Przez otwarte porty i usługi osoby nieuprawnione mogą uzyskać dostęp do systemu automatyki.

1. 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 i port 11740 dla CODESYS V3).
2. Porty i usługi dobrze jest otwierać tylko na czas uruchamiania lub konfiguracji.

Tabela 61: Strona WBM „Configuration of Network Services“ – grupa „I/O-CHECK“

Parametr	Znaczenie	
Service active	Aktywowanie/dezaktywowanie serwisu WAGO I/O-*CHECK*	
	☐	Serwis WAGO I/O-*CHECK* jest dezaktywowany; nastawa fabryczna
	☑	Serwis WAGO I/O-*CHECK* jest aktywowany.

3.5.3.8 SSH-Server

Tabela 62: Strona WBM „SSH Server Settings“ – grupa „SSH Server“

Parametr	Znaczenie	
Service active	Aktywacja/dezaktywacja usługi serwera SSH	
	☐	Usługa serwera SSH jest nieaktywna.
	☑	Usługa serwera SSH jest aktywna.
Port Number	Wprowadzanie numeru portu.	
Allow root login	Blokada lub zezwolenie na dostęp do katalogu głównego	
Allow password login	Aktywowanie/dezaktywowanie pytania o hasło	

3.5.3.9 Docker®

Tabela 63: Strona WBM „Docker Settings“ – grupa „Docker Status“

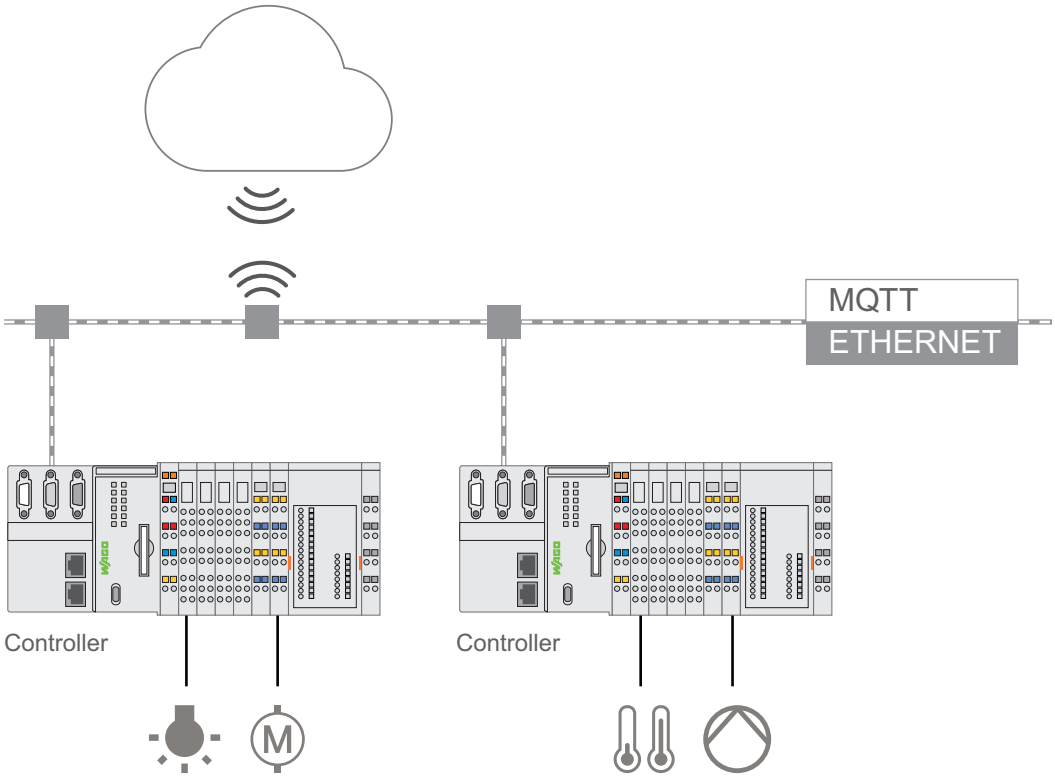
Parametr	Znaczenie	
Current State	Aktualny status usługi „Docker®“	
	stopped	Usługa „Docker®“ została zatrzymana.
	running	Usługa „Docker®“ jest aktywna.

Parametr	Znaczenie	
Service Enabled	Aktywacja/dezaktywacja usługi Docker®	
	☐	Usługa „Docker®" jest nieaktywna.
	☑	Usługa „Docker®" jest aktywna.

3.6 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 z 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 i Amazon Web Services.



Ilustracja 5: Podłączenie sterownika do usługi chmury (przykład)

Dane przenoszone są ze sterownika do chmury w formacie JSON. Połączenie można zaszyfrować przez TLS, patrz „Szyfrowanie TLS".

Ustawienia dotyczące funkcjonalności Cloud Connectivity, które należy wprowadzić w sterowniku, można znaleźć w rozdziale **Konfiguracja przy pomocy Web-Based-Management (WBM) [▸ 87]**.

Konfiguracja parametrów komunikacyjnych odbywa się np. w WBM.
Konfiguracja danych, które mają być wymieniane między chmurą a sterownikiem, odbywa się z aplikacji IEC przy użyciu odpowiedniej biblioteki CODESYS V3.

Tabela 64: Komponenty pakietu oprogramowania Cloud Connectivity

Komponent	Nazwa
CODESYS V3: WagoAppCloudWagoAppSparkplug	Biblioteka IEC do tworzenia aplikacji PLC; bloki funkcyjne umożliwiają wysyłanie i odbieranie danych między PLC i chmurą. Zmienne dotyczące transmisji danych można definiować.

ⓘ Wskazówka

Uwzględnić dodatkową dokumentację!

Szczegółowy opis pakietu oprogramowania Cloud Connectivity z PFC100/200 oraz informacje na temat programowania PLC znaleźć można w instrukcji A500920 w zakładce Do pobrania na stronie www.wago.com!

ⓘ Wskazówka

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 w zakładce Do pobrania na stronie **www.wago.com**.

Tabela 65: Strona WBM „Overview" – grupa „Connection <n>"

Parametr	Znaczenie
Operation	Status aplikacji z połączeniem z chmurą
Data from PLC Runtime	Liczba kolekcji danych (Data-Collections), które zostały zarejestrowane przez aplikację IEC w celu przesyłania danych do chmury.
Cloud Connection	Status połączenia z chmurą
Heartbeat	Aktualnie skonfigurowany interwał heartbeat w sekundach
Telemetry data transmission	Status transmisji danych
Cache fill level (QoS 1 and 2)	Stan zapełnienia pamięci dla wiadomości wychodzących, wyrażony w procentach.

Tabela 66: Strona WBM „Configuration of Connection <n>" – grupa „Configuration"

Parametr	Znaczenie
Enabled	Aktywacja/dezaktywacja funkcji Cloud Connectivity
Cloud platform	Platforma chmury
Hostname	Nazwa hosta lub adres IP dla wybranej platformy chmury
ID Scope	Punkt końcowy dla usługi Azure Device Provisioning Service (DPS).
Registration ID	ID rejestru dla usługi Azure Device Provisioning Service (DPS).
Port number	Numer portu, do którego ma być utworzone połączenie. Wartości typowe: ▪ 8883 dla połączeń szyfrowanych ▪ 1883 dla połączeń nieszyfrowanych
Device ID	Device ID dla wybranej platformy chmury
Client ID	Client ID dla wybranej platformy chmury
Authentication	Metoda uwierzytelniania, np. „Shared Key Acces", „X.509 Certificate"
Activation Key	Kod aktywacji dla wybranej platformy chmury

Parametr	Znaczenie
Clean Session	Aktywacja Clean-Session przy połączeniu z usługą chmury Clean Session jest aktywna: informacje i wiadomości dotyczące tego połączenia z usługą chmury nie są zapisywane.
TLS	Aktywacja/dezaktywacja szyfrowania TLS dla połączenia z platformą chmury Amazon Web Services (AWS) stosuje TLS.
CA file	Ścieżka do pliku zakodowanego w formacie PEM, który zawiera zaufany certyfikat CA używany do nawiązania szyfrowanego połączenia. Wartość standardowa: certyfikat CA /etc/ssl/certs/ca-certificates.crt
User	Nazwa użytkownika
Password	Hasło
Certification file	Tu wpisuje się ścieżkę do pliku zakodowanego w formacie PEM, wykorzystywanego do uwierzytelnienia usługi chmury.
Key file	Ścieżka do pliku zakodowanego w formacie PEM, który zawiera prywatny kod do uwierzytelnienia usługi chmury.
Use websockets	Aktywacja/dezaktywacja połączenia z platformą chmury za pomocą protokołu Websocket przez port 443 Jeśli dezaktywowane: połączenie z platformą chmury za pomocą protokołu MQTT przez port 8883
HTTP Proxy Host	Nazwa hosta lub adres IP serwera proxy
HTTP Proxy Port	Numer portu serwera proxy
HTTP Proxy User	Nazwa użytkownika proxy
HTTP Proxy Password	Hasło użytkownika proxy
Use compression	Aktywacja/dezaktywacja kompresji danych za pomocą kompresji GZIP
Data Protocol	Protokół danych
Cache mode	Lokalizacja pamięci podręcznej dla telegramów danych Pole wyboru jest aktywne tylko wtedy, gdy wetknięta jest prawidłowo sformatowana karta SD. Więcej informacji znaleźć można w instrukcji A500920.
Last Will	Aktywacja/dezaktywacja komunikatu Last Will Po aktywacji pojawią się kolejne pola edycji
(Last Will) Topic	Tu wpisuje się temat dla wysyłanej wiadomości Last Will.
(Last Will) Message	Wiadomość, która ma być wysłana jako wiadomość Last Will
(Last Will) QoS	„Quality of Service“ (QoS) wiadomości Last Will
(Last Will) Retain	Aktywacja/dezaktywacja ostatniej wiadomości Last-Will wysłanej przez brokera pod danym tematem jako wiadomości zapisanej (Retained Message).
Device info	Aktywacja/dezaktywacja wiadomości Device Info, informującej usługę chmury o podstawowej konfiguracji sterownika. Więcej informacji znaleźć można w instrukcji A500920.
Device status	Aktywacja/dezaktywacja wiadomości Device State informująca usługę chmury o zmianach przełącznika trybu pracy i wskaźników LED. Więcej informacji znaleźć można w instrukcji A500920.
Standard commands	Aktywacja/dezaktywacja zintegrowanych komend standardowych Więcej informacji znaleźć można w instrukcji A500920. Jeśli nieaktywne: wspierane są tylko komendy zdefiniowane w programie IEC.

Parametr	Znaczenie
Application property template	Tworzenie własności dla poszczególnych wiadomości MQTT do chmury Azure Ten parametr jest opcjonalny, tzn. gdy pole pozostawione jest puste, ta własność nie jest wysyłana. Miejsce na tworzenie: ▪ <m>: Message type ▪ <p>: Protocol version ▪ <d>: DeviceId Przykłady: ▪ MyKey=HelloWorld_<m> ▪ TestKey=<m>/<p>/<d> ▪ DeviceId=<d>

Tabela 67: Zależności między polami wyboru i edycji a poszczególnymi platformami chmury

Pole wyboru lun edycji	Platforma chmury					
	WAGO Cloud	Azure	MQTT AnyCloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
Enabled	x	x	x	x	x	x
Cloud platform	x	x	x	x	x	x
Hostname	x	x	x	x	x	
Port Number			x	(X)	x	
Device ID	x	x				
Client ID			x	x	x	
Authentication		x				x
Activation Key	x	X2				X2
Clean Session			x	(X)	x	
TLS			x	(X)	x	
CA file			x	x	x	x
User			x			
Password			x			
Certification file		X2	x	x	x	
Key file		X2	x	x	x	
Use websockets	x	X1				x
Proxy Type	X4	X4				X4
HTTP Proxy Host	X5	X5				X5
HTTP Proxy Port	X5	X5				X5
HTTP Proxy User	X5	X5				X5
HTTP Proxy Password	X5	X5				X5
Data Protocol		x	x	x	(X)	x
Use compression	x	X1	X1			X1
Cache mode	x	x	x	x	x	x
Last Will			x	x	x	
Last Will Topic			X3	X3	X3	
Last Will Message			X3	X3	X3	
Last Will QoS			X3	X3	X3	
Last Will Retain			X3	(X3)	X3	
Device info		X1	X1	X1		X1
Device status		X1	X1	X1		X1

Pole wyboru lun edycji	Platforma chmury					
	WAGO Cloud	Azure	MQTT AnyCloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
Standard commands		X1	X1	X1		X1
Application property template		X1				X1
X: Widoczne i aktywne						
(X): Widoczne, ale nieaktywne						
X1: Widoczne i aktywne, zależnie od wybranego protokołu danych						
X2: Widoczne i aktywne, zależnie od wybranego uwierzytelnienia						
X3: Widoczne i aktywne, gdy włączony jest „Last Will“.						
(X3): Widoczne ale nieaktywne, gdy włączony jest „Last Will“.						
X4: Aktywne, gdy włączony jest „Use websockets“.						
X5: Widoczne i aktywne, gdy włączony jest „Use websockets“ i gdy jako „Proxy Type“ ustawiony jest „HTTP“.						

Tabela 68: Możliwość wyboru protokołu danych dla poszczególnych platform chmury

Protokół danych	Platforma chmury					
	WAGO Cloud	Azure	MQTT AnyCloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
WAGO Protocol		x	x	x		x
WAGO Protocol 1.5		x	x	x		x
Native MQTT			x	x	(X)	
Sparkplug payload B		x	x	x		
X: Możliwość wyboru						
(X): Stała konfiguracja						

Tabela 69: Zależności między polami wyboru i edycji a poszczególnymi protokołami danych

Pole wyboru lub edycji	Protokół danych			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
Client ID	x	x	x	x
Use compression	x	x	x	
Device info	x	x		
Device status	x	x		
Standard commands	x	x		
Application property template	x	x		
X: Widoczne i aktywne				

Tabela 70: Możliwość wyboru trybu pamięci podręcznej zależnie od wybranego protokołu danych

Tryb pamięci podręcznej	Protokół danych			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
RAM	x	x	x	(X)
SD-Card	X1	X1	X1	
X: Możliwość wyboru				
X1: Możliwość wyboru tylko wtedy, gdy nie jest włączona opcja „Compression“				

Tryb pamięci podręcznej	Protokół danych			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
(X): Stała konfiguracja				

Tabela 71: Zależności między polami wyboru i edycji a poszczególnymi uwierzytelnieniami

Pole wyboru lub edycji	Uwierzytelnienie	
	Shared Access Key	X.509 Certificate
Activation Key	x	
Certification file		x
Key file		x
X: Widoczne i aktywne		

3.7 Funkcje sieci obiektowej

3.7.1 OPC UA

Tabela 72: Strona WBM „OPC UA Configuration" – grupa „OPC UA Server Configuration"

Parametr	Znaczenie	
Enabled	Aktywowanie/dezaktywowanie serwera OPC UA	
	☐	Serwer OPC UA jest dezaktywowany.
	☑	Serwer OPC UA jest aktywowany.
Log Level	Wybór poziomu logowania; Wybrany poziom logowania wpływa na czas reakcji serwera. Dlatego należy wybrać najniższy niezbędny poziom, np. „Debug" dla dogłębnych analiz. Do ustawienia są następujące wartości:	
	Error	Wyświetlane są tylko komunikaty o błędach.
	Warning	Wyświetlane są komunikaty o błędach i ostrzeżenia.
	Info	Wyświetlane są komunikaty o błędach, ostrzeżenia i komunikaty o statusie.
	Debug	Wyświetlane są komunikaty o błędach, komunikaty ostrzegawcze, komunikaty o statusie oraz komunikaty debugowania.
Ctrl Configuration name	Wrowadzanie nazwy konfiguracji, którą otrzymuje sterownik wewnątrz PLC Open Device Set.	

Tabela 73: Strona WBM „OPC UA Configuration" – grupa „OPC UA Server Security Settings"

Parametr	Znaczenie	
Anonymous Access	Zablokuj/Zezwól na anonimowy dostęp do serwera.	
	☐	Dostęp anonimowy jest niedozwolony.
	☑	Dostęp anonimowy jest dozwolony; pod warunkiem że uwierzytelnianie portu runtime jest również wyłączone.
Allow Password On Plaintext	Transmisja hasła w czytelnym formacie	
	☐	

Parametr	Znaczenie	
	☑	
Security Modes	Tryb bezpieczeństwa serwera OPC UA; W zależności od wybranego trybu pracy dostępne są różne punkty końcowe OPC UA do nawiązania połączenia.	
	None	Zaznaczona tylko opcja OPC UA Endpoint **None**. Umożliwia nawiązanie niezabezpieczonego połączenia z serwerem OPC UA.
	None + Sign + SignAndEncrypt	Punkty końcowe **None**, **Sign** i **SignAndEncrypt** są dostępne. **Sign** udostępnia punkt końcowy, który jest chroniony hasłem. **SignAndEncrypt** udostępnia punkt końcowy, który oprócz hasła udostępnia również szyfrowanie.
	Sign + SignAndEncrypt	Punkty końcowe **Sign** i **SignAndEncrypt** są dostępne.
	SignAndEncrypt	Tylko Endpoint **SignAndEncrypt** jest dostępny.
Security Policies	Wybór polityki bezpieczeństwa; Tu ustawia się moc szyfrowania serwera OPC UA. Do wyboru są: Aes128Sha256RsaOaep and better, Basic256Sha256 and better, Aes256Sha256RsaPss.	

3.7.2 BACnet

BACnet jest licencjonowanym rozszerzeniem, licencjonowanie może być realizowane poprzez Add-on-Licensing.

Nieograniczone czasowo zastosowanie BACnet wymaga klucza licencyjnego. Przez ograniczony czas można korzystać z BACnet także bez klucza licencyjnego. Do okresu testowego wlicza się tylko czas rzeczywistego użytkowania. Po upływie okresu testowego dostęp bez klucza licencyjnego nie jest możliwy.

ⓘ Wskazówka

Ograniczenie komunikacji BACnet

Komunikacja BACnet możliwa jest tylko przez port X1 oraz porty przyporządkowane do konfiguracji sieci bridge 1 (br0).

Więcej informacji można znaleźć w dokumencie BACnet Protocol Implementation Conformance Statement (PICS) na stronie ↗ **www.wago.com**.

Tabela 74: Strona WBM „BACnet Status" – grupa „BACnet Information"

Parametr	Znaczenie	
State	Status sieci obiektowej BACnet	
	☐	Sieć BACnet jest dezaktywowana.
	☑	Sieć BACnet jest aktywowana.
Mode	Tryb pracy BACnet	
	ip	Komunikacja poprzez BACnet/IP
	sc	Komunikacja poprzez BACnet/SC
Wersja	Zainstalowana wersja BACnet	
Status Info	Status sieci obiektowej BACnet	
Device-ID	Aktualny Device ID produktu	

Tabela 75: Strona WBM „BACnet Status" – grupa „BACnet License"

Parametr	Znaczenie
Type	Wyświetlanie licencji dla BACnet
User Objects	Wyświetlanie liczby istniejących obiektów oraz liczby obiektów możliwych do użycia na podstawie licencji BACnet

Tabela 76: Strona WBM „BACnet Status" – grupa „BACnet Data Link"

Parametr	Znaczenie
Connection Info	Wskaźnik statutu płączenia

Tabela 77: Strona WBM „BACnet Configuration" – grupa „PLC Runtime"

Parametr	Znaczenie
[Restart]	Restart runtime

Tabela 78: Strona WBM „BACnet Configuration" – grupa „BACnet Service"

Parametr	Znaczenie	
Service active	Aktywowanie/dezaktywowanie sieci obiektowej BACnet	
	☐	Sieć BACnet jest dezaktywowana.
	☑	Sieć BACnet jest aktywowana.
Mode	Tu wybiera się tryb pracy BACnet.	
	ip	Komunikacja poprzez BACnet/IP
	sc	Komunikacja poprzez BACnet/SC
Who-Is online interval time (sec)	Odstęp czasowy między zapytaniami sterownika dla sieci obiektowej, które inne urządzenia są dostępne online (minimalny: 60 s).	
Broadcast I-Am answer	Umożliwia aktywację/dezaktywację wysyłania przez urządzenie komunikatów I-Am na broadcast BACnet.	
	☐	Wiadomości I-AM nie są wysyłane na adres BACnet Broadcast.
	☑	Wiadomości I-AM są wysyłane na adres BACnet Broadcast.

Tabela 79: Strona WBM „BACnet Configuration" – grupa „BACnet Data"

Parametr	Znaczenie
Delete Persistence Data	Trwałe dane BACnet zostaną usunięte podczas następnego uruchomienia.
Reset all BACnet Data and Settings to Default	Przy kolejnym restarcie specyficzne ustawienia i dane BACnet zostają zresetowane do ustawień fabrycznych.
override. xmlChose file ...	Wybór pliku na PC
[Upload]	Przesyłanie wybranego pliku z PC do sterownika

Tabela 80: Strona WBM „BACnet Configuration" – grupa „BACnet Log Level"

Parametr	Znaczenie	
Error	Aktywacja/dezaktywacja edycji dziennika błędów	
	☐	Wpisy do dziennika błędów nie są wyświetlane.
	☑	Wyświetlane są wpisy do dziennika błędów.
Warning	Aktywacja/dezaktywacja wyjścia dziennika ostrzeżeń	
	☐	Wpisy do dziennika ostrzeżeń nie są wyświetlane.
	☑	Wyświetlane są wpisy do dziennika ostrzeżeń.
Info	Aktywacja/dezaktywacja edycji dziennika zdarzeń	
	☐	Wpisy do dziennika zdarzeń nie są wyświetlane.
	☑	Wyświetlane są wpisy do dziennika zdarzeń.
Debug	Aktywacja/dezaktywacja wyjścia dziennika błędów	
	☐	Wpisy w dzienniku debugowania nie są wyświetlane.
	☑	Wyświetlane są wpisy do dziennika błędów.

Tabela 81: Strona WBM „BACnet Configuration" – grupa „BACnet Network Capture"

Parametr	Znaczenie	
Enable	Aktywacja/dezaktywacja rejestrowania ruchu sieciowego przy użyciu odpowiednich filtrów BACnet	
	☐	Ruch sieciowy nie jest rejestrowany.
	☑	Rejestracja ruchu sieciowego
Log pre-master secrets	Aktywacja/dezaktywacja zapisu secrets w celu odszyfrowania ruchu sieciowego BACnet/SC	
	☐	Secrets nie są zapisywane.
	☑	Secrets są zapisywane.
BACnet Network Capture Archive **[Download]**	Za pomocą przycisku [Download] można pobrać z urządzenia zarejestrowany ruch sieciowy, w tym dane uwierzytelniające, jeśli ta opcja jest włączona.	

Tabela 82: Strona WBM „BACnet Data Link" – grupa „BACnet Restart"

Parametr	Znaczenie
[Restart]	Restart usługi BACnet

Tabela 83: Strona WBM „BACnet Data Link" – grupa „BACnet/IP"

Parametr	Znaczenie
Port Number	Wprowadzanie portu dla komunikacji BACnet/IP

Tabela 84: Strona WBM „BACnet Data Link" – grupa „BACnet/SC"

Parametr	**Znaczenie**	
Mode	Wybór trybu pracy BACnet/SC	
	regular	Urządzenie pracuje jako BACnet/SC Node.
	primary	Urządzenie pracuje jako BACnet/SC Primary HUB.
	failover	Urządzenie pracuje jako BACnet/SC Failover HUB.
Port Number	Wprowadzanie portu dla komunikacji BACnet/SC	
Primary Hub URI	Wpisanie URI dla głównego HUB-a (Primary HUB); wss://<IP-Adresse>:<Port HUBs> lub wss://<Domainname>:<Port HUBs> (np. wss://192.168.178.19:47808 lub wss://PFC200V3-XXXXXX.localdomain.lan:47808)	
Failover Hub URI	Wpisanie URI dla HUB przełączania awaryjnego; wss://<adres IP>:<Port HUBs> lub wss://<Domainname>:<Port HUBs> (np. wss://192.168.178.19:47808 lub wss://PFC200V3-XXXXXX.localdomain.lan:47808)	
Allow self signed Certificates	Aktywuj/dezaktywuj, czy komunikacja może być nawiązywana za pomocą certyfikatów z sygnaturą własną.	
Allow expired Certificates	Aktywuj/dezaktywuj, czy komunikacja przez wygasłe certyfikaty może być nawiązana.	
Allow any Certificates	Aktywuj/dezaktywuj, czy komunikacja może być nawiązywana przez dowolne certyfikaty.	

Tabela 85: Strona WBM „BACnet Data Link" – grupa „BACnet/SC Certificate Authority (CA)"

Parametr	**Znaczenie**
Chose file ...	Wybór certyfikatu CA na komputerze w celu przesłania do urządzenia
[Upload]	Przesłanie wybranego certyfikatu CA do urządzenia; Po restarcie certyfikat ten jest używany jako certyfikat CA do komunikacji BACnet/SC.

Tabela 86: Strona WBM „BACnet Data Link" – grupa „BACnet/SC Certificate"

Parametr	**Znaczenie**
Chose file ...	Wybór certyfikatu urządzenia na komputerze w celu przesłania do urządzenia
[Upload]	Przesłanie wybranego certyfikatu urządzenia na urządzenie; Po restarcie certyfikat ten jest używany do komunikacji BACnet/SC.

Tabela 87: Strona WBM „BACnet Configuration" – grupa „BACnet/SC Certificate Signing Request (CSR)"

Parametr	**Znaczenie**
Country	Wprowadzanie nazwy kraju dla CSR lub certyfikatu urządzenia (dwie litery)
State	Dane dotyczące państwa dla CSR lub certyfikatu urządzenia
Locality	Wprowadzanie lokalizacji dla CSR lub certyfikatu urządzenia.
Organization	Wprowadzanie nazwy firmy lub organizacji dla CSR lub certyfikatu urządzenia.
Organizational Unit	Wprowadzanie nazwy działu dla CSR lub certyfikatu urządzenia.
Common Name	Wprowadzanie nazwy urządzenia dla CSR lub certyfikatu urządzenia.
[Generate]	Tworzenie na urządzeniu CSR i nowego klucza prywatnego
[Download]	Pobieranie CSR z urządzenia

Tabela 88: Strona WBM „BACnet Data Link" – grupa „BACnet/SC Default Certificates"

Parametr	Znaczenie
[Generate]	Tworzenie nowego certyfikatu

Tabela 89: Strona WBM „BACnet Storage Location" – grupa „BACnet Persistence"

Parametr	Znaczenie	
Storage Location	Wybierz lokalizację dla danych trwałych; wybór możliwy jest tylko wtedy, gdy oba nośniki są dostępne.	
	Internal Flash	Dane są zapisywane w wewnętrznej pamięci sterownika.
	SD-Card	Dane zapisywane są na karcie pamięci. Jeśli wybrana jest opcja „SD-Card", ale karta pamięci jest już wyjęta, opcja ta nie jest już aktywna i można wybrać tylko „Internal-Flash".

Tabela 90: Strona WBM „BACnet Storage Location" – grupa „BACnet Trendlog"

Parametr	Znaczenie	
Storage Location	Wybierz lokalizację danych trendów; wybór jest możliwy tylko wtedy, gdy oba nośniki są dostępne.	
	Internal Flash	Dane są zapisywane w wewnętrznej pamięci sterownika.
	SD-Card	Dane zapisywane są na karcie pamięci. Jeśli wybrana jest opcja „SD-Card", ale karta pamięci jest już wyjęta, opcja ta nie jest już aktywna i można wybrać tylko „Internal-Flash".

Tabela 91: Strona WBM „BACnet Storage Location" – grupa „BACnet Eventlog"

Parametr	Znaczenie	
Storage Location	Wybierz lokalizację dla danych dziennika zdarzeń; Wybór możliwy jest tylko wtedy, gdy oba nośniki są dostępne.	
	Internal Flash	Dane są zapisywane w wewnętrznej pamięci sterownika.
	SD-Card	Dane zapisywane są na karcie pamięci. Jeśli wybrana jest opcja „SD-Card", ale karta pamięci jest już wyjęta, opcja ta nie jest już aktywna i można wybrać tylko „Internal-Flash".

3.7.3 Master i slave CANopen

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 wspiera 512 TXPDO i 512 RX PDO oraz 128 SDO.

W lokalnym obrazie procesu jako obszar wejść i wyjść dla wymiany danych przez interfejs CANopen przewidziany jest obszar 4096 bajtów. Bezpośredni dostęp do modułów I/O przez sieć obiektową nie jest przewidziany.

Pozycje w obrazie procesu mogą być w razie potrzeby mapowane na RX PDO i TX PDO. Pełny zakres danych wejściowych i wyjściowych może być odczytywany i zapisywany za pomocą SDO.

Po inicjalizacji komunikacja CANopen działa niezależnie od aplikacji IEC. Przy zastosowaniu jako slave CANopen możliwa jest zmiana prędkości transmisji i adresu sieci obiektowej zgodnie z protokołem CANopen LSS.

3.7.3.1 Katalog obiektów

Wszystkie obiekty komunikacyjne i procesowe CANopen są umieszczane w katalogu obiektów.

Poniższa tabela daje ogólny przegląd ustaleń w definicji CANopen:

Tabela 92: Przegląd adresów w katalogu obiektów

Zakres indeksów	Zastosowanie
0000	Nieużywany
0001-009F	Typy danych
00A0-0FFF	Zarezerwowany (adresy wykorzystywane do innych usług)
1000-1FFF	Profil komunikacji
2000-5FFF	Obszar 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	Zarezerwowane

Obiekty dostępne i istotne dla PFC są opisane poniżej.

3.7.3.2 Profil komunikacji

0x1000 Device type

Stos zgłasza się w sieci jako device 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 mastera i slave'a

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 już istniejące błędy przesuwane są o jeden subindex w dół. Wspieranych jest maksymalnie 20 błędów. Gdy wystąpi więcej niż 20 błędów, kolejny błąd jest nadpisywany w subindexie 20. Przez wpisanie „0" w subindeksie 0 cała pamięć błędów zostaje usunięta.

Standardowa wartość: 0 we wszystkich wpisach

0x1005 COB IB Sync

Obiekt definiuje COB ID dla komunikatu o synchronizacji.

Standardowa wartość: 0x80

0x1006 Communication Cycle Period

Czas trwania cyklu synchronizacji w µs 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. „750-8216"

0x1009 Manufacturer Hardware Version

Wpis: „V 1.0" lub wyższa

0x100A Manufacturer Software Version

Wpis: „04.02.05(00)" lub wyższa

0x100C Node Guarding Time

Obiekt podaje Guarding Time w milisekundach. Master NMT cyklicznie odpytuje slave'a NMT o stan. Guard Time to czas między dwoma zapytaniami.

Standardowa wartość: 0 (Node Guarding dezaktywowany)

0x100D Life Time Factor

Life Time Factor jest częścią protokołu Node Guarding. Slave NMT sprawdza, czy został odpytany w trakcie Node Life Time (Guardtime pomnożony przez Life Time Factor). Jeśli tak się nie stało, slave musi założyć, że master NMT 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 Emergency Message. Tu podawany jest ID tego obiektu (przy masterze 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 deaktywuje 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. W indeksie 0 wpisywana jest liczba monitorowanych urządzeń, inne parametry zawierają czas heartbeat w milisekundach w najniższym bicie 16 i ID urządzenia sieciowego w bicie 8.

Standardowe wartości:

Indeks 0: 0 (127 = liczba możliwych parametrów)

Wszystkie inne parametry 0 (Ta funkcja nie jest wspierana przez mastera CAN w wersji firmware'u 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

0x1018h Identity

Obiekt określa zastosowane urządzenie. ID producenta zawiera unikatową liczbę charakterystyczną dla producenta. Dla WAGO to ID wynosi 33.

Kod produktu zawiera kod urządzenia.

Nr wersji zawiera określone zachowanie CANopen. Major Rev. Nr. określa funkcjonalność CANopen. Przy zmianie funkcjonalności zwiększa się także Major Rev. Nr. Na podstawie Minor Rev. Nr. można rozróżnić różne wersje o tym zachowaniu CANopen.

Numer jest niezależny od wersji firmware'u. Przy zastosowaniu jako slave CANopen z CODESYS 3.5 można dowolnie ustawić Vendor ID, kod produktu i numer rewizji w konfiguracji slave'a.

Subindeks 0	Liczba wpisów:	4
Subindeks 1	Vendor ID:	33
Subindeks 2	Product_code:	np. 8216 dla 750-8216
Subindeks 3	Revision_number:	0x00010003 lub wyższy
Subindeks 4	Serial_number	odpowiada ostatnim 4 bajtom adresu MAC.

0x1200 Server SDO Parameter Channels

Tu wprowadza się parametry komunikacyjne transferu SDO jako serwera. Maksymalnie wspierany jest 1 kanał serwera SDO.

0x1280 ... 0x128E Client SDO Parameter Channels

Tu wprowadza się parametry komunikacyjne transferu SDO jako klienta. Maksymalnie wspieranych jest 16 kanałów klienta SDO.

0x1029h Error behavior

Ten obiekt określa, jak zachowuje się slave w przypadku błędu.

Subindeks 0	Liczba wpisów:	1	
Subindeks 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

3.7.3.2.1 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 deaktywuje 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, mastera można uruchomić przez zapis 0x1F w tym obiekcie.

0x1F81 ... 0x1F8A Slave Konfiguration

Te listy zawierają skonfigurowane slave'y. Wszystkie parametry sprawdzane są przy starcie mastera lub przesyłane do salve'ów.

0x1F81 NMT Slave Assignment

Subindeks 0:	128 = liczba możliwych parametrów	
Subindeks 1 ... 128:	Bit 0	Slave dostępny
	Bit 2	Slave wymagany do uruchomienia
	Bit 3	Slave resetowany przy uruchomieniu
	Bit 8 ... 15:	Guard Retry Factor
	Bit 16 ... 31:	Guard Time
Subindeks 128:	Cała sieć (Write-Only)	

0x1F82 Request NMT

Subindex 0: 127 = liczba możliwych parametrów

Subindeks = Master Node ID Master NMT State

0x1F84 Device type identification

Subindex 0: 127 = liczba możliwych parametrów

Subindex 1 ... 127: Device Type slave

0x1F85 Vendor identification

Subindex 0: 127 = liczba możliwych parametrów

Subindeks 1 ... 127: Vendor Identification slave`a (domyślnie nieużywane)

0x1F86 Product code

Subindex 0: 127 = liczba możliwych parametrów

Subindeks 1 ... 127: Product Code slave`a (standardowo niewykorzystywane)

0x1F87 Revision number

Subindex 0: 127 = liczba możliwych parametrów

Subindeks 1 ... 127: Revision Number slave`a (standardowo niewykorzystywane)

0x1F88 Serial number

Subindex 0: 127 = liczba możliwych parametrów

Subindeks 1 ... 127: Serial Number slave`a (standardowo niewykorzystywane)

0x1F89 Boot Time

Czas w ms między uruchomieniem urządzeń Slave a gotowością operacyjną wszystkich urządzeń Slave.

Standardowa wartość: 0 = dezaktywowany

0x1F8A Restore configuration

Subindex 0: 127 = liczba możliwych parametrów

Subindex 1 ... 127: bit 0 = 1 Wyślij przy starcie Restore Configuration do slave'a

3.7.3.3 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).

Przy pomocy 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.

3.7.3.3.1 Obiekty komunikacyjne sterownika

Sterownik obsługuje następujące obiekty komunikacyjne:

- 512 Tx-PDOs, do wymiany danych procesowych wejściowych sterownika sieciowego,
- 512 Rx-PDOs do wymiany danych procesowych wyjściowych sterownika sieciowego,

- Obiekty synchronizacji sieci (SYNC),
- Obiekty Emergency (EMCY),
- Obiekty zarządzania siecią,
  - Module Control Protocols,
  - Error Control Protocols,
  - Bootup Protocol.

3.7.3.3.2 Adresowanie specyficzne dla sieci obiektowej

Po konfiguracji interfejsu CAN jako mastera lub slave zmienne CODESYS dla sieci CAN są mapowane w katalogu obiektów (inicjalizacja). Urządzenie sieci CANopen stosuje 16-bitowe indeksy i 8-bitowe podindeksy 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, usw.) oraz wejścia i wyjścia. Dostęp przez PDO może mieć charakter zapisu lub odczytu.

Ponieważ CANopen nie transmituje danych w sposób bitowy, zmienne zostają zebrane przez typ danych Boolean w bajtach i przyporządkowane odpowiedniemu indeksowi: zmienne wejściowe przez Boolean do indeksu 0xA080, zmienne wyjściowe przez Boolean do indeksu 0xA500.

Przyporządkowanie danych zmiennych, które reprezentowane są w obrazie procesu 1 bajtem lub kilkoma, odbywa się analogicznie do odpowiedniego indeksu.

ⓘ Wskazówka

Przestrzegać kierunku transmisji danych!

Zmienne wejściowe i wyjściowe IEC 61131-3 są zdefiniowane z punktu widzenia sieci obiektowej CAN,
tzn.: zmienne wejściowe
IEC 61131-3 to zmienne wyjściowe PFC,
a zmienne wyjściowe IEC 61131-3 to zmienne wejściowe PFC.

Przegląd indeksów zmiennych „IEC 61131-3“ zawiera poniższa tabela.

Tabela 93: Indeksowanie zmiennych „IEC 61131-3“ w katalogu obiektów

Typ danych	Zmienne wyjściowe „IEC61131-3"	Zmienne wejściowe „IEC61131-3"
	Indeks	
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

Typ danych	Zmienne wyjściowe „IEC61131-3"	Zmienne wejściowe „IEC61131-3"
	Indeks	
Integer40	0xA2C0	0xA740
Unsigned48	0xA300	0xA780
Integer48	0xA340	0xA7C0
Unsigned56	0xA380	0xA800
Integer56	0xA3C0	0xA840
Integer64	0xA400	0xA880
Unsigned64	0xA440	0xA8C0

Przez indeksy 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.

Przy pomocy subindeksu wybiera się określony bajt.

Przy zastosowaniu indeksów dla większych bloków danych możliwy jest natomiast dostęp do większej ilości bajtów równocześnie.
Przy pomocy indeksu Integer16 (0xA0C0) lub Unsigned16 (0xA100) można uzyskać dostęp np. w postaci słowa do opisanych zmiennych wyjściowych PFC, a przy pomocy indeksu 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 94: Dostęp od strony sieci obiektowej do danych wyjściowych PFC

Dostęp	Dane wyjściowe PFC	Odczyt przez indeks (Integer / Unsigned)	Sub-Index
W postaci bajtu (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 tabela przedstawiają przegląd adresowania danych o różnych reprezentacjach w obrazie procesu.

Każde miejsce zapisu dla zmiennych sieci obiektowej (bajt 6000 do 9999) ma przyporządkowany indeks w zależności od reprezentacji w obrazie procesu.

Indeksowanie ujęte w tabelach uwzględnia maksymalny indeks i subindeks.

3.7.3.3.3 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.

3.7.3.3.3.1 Dostęp w CODESYS do zmiennych PFC

Tabela 95: Przykłady dla dostępów w CODESYS do zmiennych PFC

Typ danych zmiennych PFC	Zmienne wejściowe PFC		Zmienne wyjściowe PFC	
	Definicja wg IEC 61131-3	Indeks/Subindeks	Definicja wg IEC 61131-3	Indeks/Subindeks
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

3.7.3.3.3.2 Indeksy maksymalne

Maksymalne indeksy i subindeksy tworzone są na podstawie wielkości pamięci sterownika sieciowego 4096 bajtów i reprezentacji w obrazie procesu tych typów danych.

Przegląd maksymalnych indeksów i subindeksów zmiennych IEC 61131-3 zawiera poniższa tabela.

Tabela 96: Maksymalne indeksy i subindeksy zmiennych „IEC 61131-3"

Typ danych	Zmienne wyjściowe „IEC61131-3"		Zmienne wejściowe „IEC61131-3"	
	Maks. Indeks	Maks. Subindeks	Maks. Indeks	Maks. Subindeks
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

Typ danych	Zmienne wyjściowe „IEC61131-3"		Zmienne wejściowe „IEC61131-3"	
	Maks. Indeks	Maks. Subindeks	Maks. Indeks	Maks. Subindeks
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 przy pomocy typu danych Unsigned16.

Adresowanie 257 słów danych odbywa się w następujący sposób:
- Indeks 0xA580, subindeks 1 do 255
- Indeks 0xA581, subindeks 1 i 2.

Tabela 97: Przykład dla zmiennych wyjściowych „IEC 61131-3“

Indeks	Sub-Index	Spis treści	Nazwa
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.

3.7.3.3.4 Zastosowanie slave CANopen (Device) w CODESYS V3

Konfigurator slave'a CODESYS 3.5 wykorzystuje inne adresy obiektów dla danych procesowych niż te zdefiniowane w normie CANopen CiA 405 dla urządzeń IEC 61131. Dlatego przy pracy jako slave CODESYS V3, stosuje się numery obiektów CODESYS V3:

0x3000 .. 0x31FF	odbiór danych procesowych (master => slave)
0x3800 .. 0x39FF	wysyłanie danych procesowych (slave => master)
0x5000 .. 0x507F	SDO dostęp do odczytu/zapisu
0x5800 .. 0x587F	SDO dostęp do odczytu

Szczegółowy opis zastosowania interfejsu CANopen znajduje się w podręczniku online CODESYS V3. Funkcje specyficzne dla WAGO są dostępne w bibliotekach WagoAppCanOpen i WagoAppCanLayer2.

3.7.3.3.5 Zastosowanie jako urządzenie warstwy 2 CAN

Alternatywnie do funkcji mastera lub slave'a CANopen, na sterowniku dostępny jest również czysty stos warstwy 2. Może być on używany, gdy funkcje CANopen nie są potrzebne. Zapewnia on wyższą przepustowość przy mniejszym obciążeniu CPU.

Można ustawić 127 filtrów odbiorczych z całkowitym buforem wynoszącym 127 telegramów lub pracować bez filtrów z buforem odbiorczym wynoszącym 255 telegramów.

Aby korzystać z tego rozwiązania w CODESYS V3, należy na magistrali CAN wybrać urządzenie WAGO CanLayer2. Funkcjonalność ta jest realizowana za pomocą biblioteki WagoAppCanLayer2.

3.8 Funkcje pamięci

3.8.1 Bezpieczeństwo danych

Z myślą o bezpieczeństwie i możliwości przywrócenia danych sterownik wyposażony jest w funkcję backupu i restore.

Odpowiednie ustawienia wprowadza się w WBM w zakładce „Configuration“ na stronach „Package Server“ > „Firmware Backup“ lub „Firmware Restore“.

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

Ponadto można wybrać dane, które mają zostać objęte kopią zapasową lub przywrócone:
- projekt CODESYS („PLC Runtime", projekt bootowalny, ustawienia CODESYS)
- ustawienia urządzenia („Settings“)
- system operacyjny sterownika oraz główny system plików („System“)
- wszystkie powyższe elementy („All“), widoczne tylko wtedy, gdy dane nie są zapisywane w sieci.

ⓘ Wskazówka

Należy uwzględnić wersję firmware'u!

Przywracanie systemu operacyjnego (opcja „System") jest dozwolone i możliwe tylko wtedy, gdy wersje oprogramowania firmware w momencie tworzenia kopii zapasowej i przywracania są identyczne.
W razie potrzeby należy zrezygnować z przywracania systemu operacyjnego lub wcześniej dostosować wersję firmware do wersji obowiązującej w momencie tworzenia kopii zapasowej.

3.8.1.1 Funkcja backupu

Przy pomocy funkcji backupu można podczas pracy zapisywać na karcie pamięci pliki wewnętrznej pamięci oraz ustawienia urządzeń.

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.

Jeśli jako nośnik docelowy została wybrana karta pamięci, dioda LED gniazda karty pamięci miga podczas zapisu na żółto/pomarańczowo.

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

Sterownik posiada 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 backupu z karty pamięci!

Z karty pamięci nie jest możliwy backup na wewnętrzną pamięć flash.

ⓘ Wskazówka

Należy uwzględnić czas tworzenia kopii zapasowych

Tworzenie plików backupu trwa kilka minut. Aby skrócić ten czas, należy przed rozpoczęciem backupu zatrzymać program CODESYS.

Funkcję backupu można realizować przez stronę WBM „Firmware Backup“ w zakładce „Configuration“, wybór „Package Server“ > „Firmware Backup“.

Tabela 98: Strona WBM „Firmware Backup“ – grupa „Firmware Backup“

Parametr	Znaczenie	
Boot Device	Nośnik pamięci, z którego przeprowadzony był rozruch.	
Destination	Miejsce zapisu kopii zapasowej	
	Memory Card	Dane zostają zapisane na karcie pamięci. Ta możliwość wyboru widoczna jest tylko wtedy, gdy wetknięta jest karta pamięci i nie był z niej przeprowadzony rozruch.
	Pamięć USB	Dane są zapisywane na pendrivie. Ta opcja jest dostępna tylko w produktach z portem USB. Opcja jest aktywna tylko wtedy, gdy podłączony jest nośnik USB i system nie został z tego nośnika uruchomiony.
	Network	Dane zapisywane są w systemie plików i udostępniane na PC do pobrania.
PLC Runtime Project	Zapisywanie projektu runtime PLC, projektu bootowalnego i ustawień CODESYS	
	☐	Bieżący projekt PLC zostaje niezabezpieczony
	☑	Bieżący projekt PLC zostaje zabezpieczony
Settings	Zabezpieczenie ustawień urządzenia	
	☐	Ustawienia urządzenia nie są zabezpieczone.
	☑	Ustawienia urządzenia zostają zabezpieczone.
System	Zapisywanie systemu operacyjnego urządzenia i głównego systemu plików	
	☐	System operacyjny urządzenia i główny system plików nie są zabezpieczone.
	☑	System operacyjny urządzenia i główny system plików są zabezpieczone.
Encryption	Tworzenie kopii zapasowej danych w postaci zaszyfrowanej	

Parametr	Znaczenie	
	☐	Dane są zapisywane bez szyfrowania.
	☑	Dane są zapisywane w postaci zaszyfrowanej
Encryption passphrase	Hasło szyfrowania Pole edycji widoczne jest tylko wtedy, gdy pole wyboru**Encryption** jest zaznaczone.	
Confirm passphrase	Hasło szyfrowania do kontroli Pole edycji widoczne jest tylko wtedy, gdy pole wyboru **Encryption** jest zaznaczone.	

3.8.1.2 Funkcja Restore

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

Jako medium źródłowe można wybrać sieć lub kartę pamięci (jeśli jest włożona).

Gdy jako medium źródłowe zostanie wybrana karta pamięci, wskaźnik LED gniazda karty pamięci będzie podczas ładowania migał na żółto/pomarańczowo.

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 uruchomieniu wykorzystana zostanie stara partycja.

Po restarcie zostaje automatycznie załadowany projekt bootowalny, a ustawienia zostają automatycznie aktywowane. Źródło ładowania projektu bootowalnego (Boot Project) z pamięci wewnętrznej lub karty pamięci jest określane przez ustawienie „Home directory on memory card enabled”. To ustawienie można realizować przez stronę WBM „PLC Runtime Configuration“ w zakładce „Configuration“, wybór „PLC Runtime“.

ⓘ 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

Odświeżenie możliwe tylko z wewnętrznej pamięci!

Jeśli produkt był uruchamiany z karty pamięci, nie jest możliwe odświeżenie firmware'u.

ⓘ Wskazówka

Reset przez odświeżenie

Reset można realizować przez odświeżenie systemu, ustawień lub CODESYS!

ⓘ Wskazówka

Utrata połączenia przez odświeżenie!

Jeśli w wyniku odświeżenia zmienią się parametry połączenia ETHERNET, WBM może nie być w stanie nawiązać połączenia z produktem.
WBM należy ponownie otworzyć za pomocą odpowiedniego adresu IP produktu w wierszu adresu.

ⓘ Wskazówka

Uwzględnić czas resetu

Proces restore wymaga ok. 2 ... 3 minut.
Po zakończeniu procesu restore sterownik uruchamiany jest ponownie i jest znowu gotowy do pracy.

Funkcję Restore można realizować przez stronę WBM „Firmware Restore" w zakładce „Configuration", wybór „Package Server" > „Firmware Restore".

Tabela 99: Strona WBM „Firmware Restore" – grupa „Firmware Restore"

Parametr	Znaczenie	
Source	Tu wybiera się źródło danych do odświeżenia.	
	Memory Card	Dane zostają odczytane z karty pamięci. Ta możliwość wyboru aktywna jest tylko wtedy, gdy wetknięta jest karta pamięci i nie był z niej przeprowadzony rozruch.
	Pamięć USB	Dane są odczytywane z pamięci USB. Ta opcja jest dostępna tylko w produktach z portem USB. Opcja jest aktywna tylko wtedy, gdy podłączony jest nośnik USB i system nie został z tego nośnika uruchomiony.
	Network	Dane do odświeżenia pobrane zostają z PC.
Boot Device	Nośnik pamięci, z którego przeprowadzony był rozruch.	
PLC Runtime Project	Nazwa pliku kopii zapasowej projektu CODESYS; Pole edycji aktywne jest tylko wtedy, gdy jako źródło danych wybrano sieć.	
Settings	Nazwa pliku kopii zapasowej ustawień; Pole edycji aktywne jest tylko wtedy, gdy jako źródło danych wybrano sieć.	
System	Nazwa pliku kopii zapasowej danych systemowych i głównego systemu plików (root); Pole edycji aktywne jest tylko wtedy, gdy jako źródło danych wybrano sieć.	
Decryption	Szyfrowanie danych	
	☐	Dane zostały zaszyfrowane.
	☑	Dane zostały zapisane bez szyfrowania.
Decryption passphrase	Hasło deszyfrujące; Pole edycji jest widoczne tylko wtedy, gdy zaznaczone jest pole **Decryption**.	

3.8.2 Funkcja karty pamięci

3.8.2.1 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/pomarańczowo.

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

3.8.2.2 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 dostępu na żółto/pomarańczowo.

Sterownik pracuje następnie bez karty pamięci.

3.8.2.3 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 bootowalny.

Przy pomocy WBM można przełożyć katalog Home dla systemu runtime na kartę pamięci, aby zyskać więcej pamięci dla dużego projektu bootowalnego lub innych plików.

Przedtem jednak należy spełnić kilka warunków.

- Bieżąca aplikacja IEC 61131 musi być zatrzymana i urządzenie musi zostać doprowadzone do stanu podstawowego przez zastosowanie funkcji „Reset". Istniejący ewentualnie projekt bootowalny zostaje usunięty.
- Jeśli katalog Home ma być przełożony na kartę pamięci, należy najpierw włożyć do urządzenia kartę sformatowaną przy pomocy wspieranego systemu plików. Tylko pierwsza partycja karty pamięci dostępna jest pod /media/sd i może zostać wykorzystana jako katalog Home.

Tylko jeśli spełnione są oba powyższe warunki, na stronie „PLC Runtime" w WBM można aktywować pole wyboru „Home directory on memory card enabled".
Ustawienie to zostanie zapisane po naciśnięciu przycisku **[Submit]** i zacznie obowiązywać po kolejnym restarcie.
Żadne pliki nie zostaną przeniesione ze starego do nowego katalogu Home.

Po przełączeniu projekt musi być załadowany na nowo i projekt bootowalny założony od nowa.

Należy pamiętać, że karta pamięci nie może być pod żadnym pozorem wyjmowana tak długo, jak długo znajduje się na niej katalog Home. Przy działającej aplikacji mogłoby to spowodować niekontrolowane zawieszenie się sterownika.

Przekładanie katalogu Home jest bezskuteczne, jeśli sterownik został uruchomiony z karty pamięci. Stan konfiguracji zostaje wprawdzie zapisany, ale zacznie być realizowany dopiero wtedy, gdy zawartość karty pamięci zostanie przekopiowana do pamięci wewnętrznej.

3.8.2.4 Ładowanie projektu bootowalnego

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

Tabela 100: 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 jest ładowany ...
nie	nie	nie	Nie, brak projektu bootowalnego.
		tak	Nie, brak projektu bootowalnego.
	tak	nie	Nie, w pamięci Flash urządzenia nie ma zapisanego projektu bootowalnego.
		tak	Tak, z karty pamięci
tak	nie	nie	Tak, z wewnętrznej pamięci flash
		(Tak) niedozwolona	Nie, to 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, to niedozwolona kombinacja, ponieważ dla tego ustawienia nie może istnieć projekt bootowalny w wewnętrznej pamięci flash.

3.9 Funkcje diagnostyczne

3.9.1 Diagnostyka za pomocą elementów sygnalizacyjnych

Różne elementy sygnalizacyjne na urządzeniu umożliwiają bezpośrednią diagnostykę, np. sygnalizacja LED zasilania, systemu, sieci obiektowej i sieci.

Liczba i rodzaj elementów sygnalizacyjnych zależy od produktu. Diagnostyka za pomocą tych elementów sygnalizacyjnych jest opisana w odpowiednich podręcznikach.

Sekwencje migania opisane w następnych akapitach dotyczą wszystkich produktów wymienionych w zakresie obowiązywania niniejszego dokumentu.

3.9.1.1 Diagnostyka za pomocą sekwencji migania

Przebieg sekwencji migania

Diagnostyka zakłócenia jest zawsze sygnalizowana cyklicznie trzema sekwencjami migania:

1. Pierwsza sekwencja wskazuje przez miganie (10 Hz) wyświetlanie kodu błędu i argumentu błędu.
2. Druga sekwencja migania (1 Hz) wskazuje kod błędu.
3. Trzecia sekwencja migania (1 Hz) wskazuje argument błędu.

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.

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.

3.9.1.1.1 Kody błędów LED I/O

Tabela 101: 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	Nieużywane
7	Niewspierany moduł I/O
8	Nieużywane
9	Błąd wyjątku CPU

Kod błędu 1 – Błąd sprzętu i konfiguracji

Tabela 102: Kod błędu 1 – Błąd sprzętu i konfiguracji: znaczenie kodów migania i środki zaradcze

Argument błędu	Przyczyna	Środek zaradczy
-	Nieprawidłowa suma kontrolna parametrów interfejsu magistrali systemowej	1. Wyłącz zasilanie sterownika. 2. Wymień sterownik. 3. Ponownie włącz zasilanie.
1	Podczas generowania kodu inline wewnętrzny bufor pamięci przekroczył maksymalną ilość danych.	1. Wyłącz zasilanie sterownika. 2. Zredukuj liczbę modułów I/O. 3. Ponownie włącz zasilanie.

Argument błędu	Przyczyna	Środek zaradczy
2	Moduł(y) I/O z niewspieranym typem danych	1. Aktualizuj firmware sterownika Jeśli błąd występuje nadal, przyczyna leży w module I/O. Można ją wykryć w następujący sposób: 2. Wyłącz zasilanie sterownika. 3. Umieść moduł końcowy w środku, między podłączonymi modułami I/O. 4. Ponownie włącz zasilanie. 5. Jeśli LED miga nadal na czerwono, wyłącz ponownie zasilanie, włóż moduł końcowy w środek pierwszej połowy węzła (patrząc od strony sterownika sieciowego). 6. Jeśli LED przestała migać, wyłącz zasilanie i włóż moduł końcowy w środek drugiej połowy węzła (patrząc od strony sterownika sieciowego). 7. Ponownie włącz zasilanie. 8. Powtarzaj procedurę do momentu, aż znajdziesz uszkodzony moduł I/O. Wymień uszkodzony moduł.
3	Nieznany typ modułu pamięci programu Flash	1. Wyłącz zasilanie sterownika. 2. Wymień sterownik. 3. Ponownie włącz zasilanie.
4	Wystąpił błąd przy zapisie w pamięci flash	1. Wyłącz zasilanie sterownika. 2. Wymień sterownik. 3. Ponownie włącz zasilanie.
5	Wystąpił błąd podczas usuwania sektora flash.	-
6	Konfiguracja modułów I/O po resecie magistrali systemowej nie zgadza się z konfiguracją modułów I/O po ostatnim uruchomieniu sterownika.	▪ Zrestartuj sterownik przez odłączenie zasilania i ponowne włączenie lub przy pomocy przycisku Reset na sterowniku.
7	Wystąpił błąd przy opisie szeregowego EEPROM	1. Wyłącz zasilanie sterownika. 2. Wymień sterownik. 3. Ponownie włącz zasilanie.
8	Niedozwolona kombinacja sprzętu i firmware'u	-
9	Nieprawidłowa suma testowa w szeregowym EEPROM	-
10	Inicjalizacja szeregowego EEPROM zakończona niepowodzeniem	-
11	Wystąpił błąd przy odczycie z szeregowego EEPROM	1. Wyłącz zasilanie sterownika. 2. Zredukuj liczbę modułów I/O. 3. Ponownie włącz zasilanie.
12	Przekroczony czas dostępu do szeregowego EEPROM	1. Wyłącz zasilanie sterownika. 2. Wymień sterownik. 3. Ponownie włącz zasilanie.
14	Przekroczona maksymalna liczba modułów bram lub modułów mailbox	1. Wyłącz zasilanie sterownika. 2. Zredukuj liczbę modułów bram lub modułów mailbox. 3. Ponownie włącz zasilanie.
16	Przekroczona maksymalna liczba modułów I/O	1. Wyłącz zasilanie sterownika. 2. Zredukuj liczbę modułów I/O. 3. Ponownie włącz zasilanie.

Kod błędu 2 – Błąd konfiguracji

Tabela 103: Kod błędu 2 – Błąd konfiguracji: znaczenie kodu migania i sposoby usuwania błędu

Argument błędu	Przyczyna	Środek zaradczy
2	Przekroczona maksymalna wielkość obrazu procesu	1. Wyłącz zasilanie sterownika. 2. Zredukuj liczbę modułów I/O. 3. Ponownie włącz zasilanie.

Kod błędu 3 – Błąd protokołu magistrali systemowej

Tabela 104: Kod błędu 3 – Błąd protokołu magistrali systemowej: znaczenie kodu migania i sposoby usuwania błędu

Argument błędu	Przyczyna	Środek zaradczy
-	Awaria komunikacji magistrali systemowej; nie można wykryć uszkodzonego modułu I/O.	✓ Jeśli do sterownika podłączony jest moduł zasilający (np. 750-602), należy sprawdzić jego prawidłowe działanie. Jeśli moduł zasilający nie jest wadliwy, przyczyna zakłócenia może leżeć w module I/O. Moduł I/O można wykryć w następujący sposób: 1. Wyłącz zasilanie sterownika. 2. Umieść moduł końcowy w środku, między podłączonymi modułami I/O. 3. Ponownie włącz zasilanie. 4. Jeśli LED I/O miga nadal na czerwono, wyłącz ponownie zasilanie, włóż moduł końcowy w środek pierwszej połowy węzła (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. Wymień uszkodzony moduł I/O lub sterownik. 1. Jeśli LED przestała migać, wyłącz zasilanie i włóż moduł końcowy w środek drugiej połowy węzła (patrząc od strony sterownika sieciowego). 2. Ponownie włącz zasilanie. 3. Powtarzaj procedurę do momentu, aż znajdziesz uszkodzony moduł I/O. Wymień uszkodzony moduł.

Kod błędu 4 – Fizyczny błąd magistrali systemowej

Tabela 105: Kod błędu 4 – Fizyczny błąd magistrali systemowej: znaczenie kodów migania i sposoby usuwania błędów

Argument błędu	Przyczyna	Środek zaradczy
-	Przekroczona dopuszczalna liczba modułów I/O	1. Wyłącz zasilanie sterownika. 2. Zredukuj liczbę modułów I/O do dopuszczalnej wartości. 3. Ponownie włącz zasilanie.
n*	Przerwanie magistrali systemowej po n-tym module I/O udostępniającym dane procesowe.	1. Wyłącz zasilanie sterownika. 2. Wymień moduł I/O (n+1) udostępniający dane procesowe. 3. Ponownie włącz zasilanie. *) Moduły I/O, które nie dostarczają danych, nie są liczone (np. moduł zasilający bez diagnostyki)

Kod błędu 5 – Błąd inicjalizacji magistrali systemowej

Tabela 106: Kod błędu 5 – Błąd inicjalizacji magistrali systemowej: znaczenie kodów migania i sposoby usuwania błędów

Argument błędu	Przyczyna	Środek zaradczy
n*	Błąd przy komunikacji rejestrowej w czasie inicjalizacji magistrali systemowej	1. Wyłącz zasilanie sterownika. 2. Wymień moduł I/O (n+1) udostępniający dane procesowe. 3. Ponownie włącz zasilanie. *) Moduły I/O, które nie dostarczają danych, nie są liczone (np. moduł zasilający bez diagnostyki)

Kod błędu 7 – Niewspierany moduł I/O

Tabela 107: Kod błędu 7 – Niewspierany moduł I/O: znaczenie kodów migania i sposoby usuwania błędów

Argument błędu	Przyczyna	Środek zaradczy
n	Pierwszy niewspierany moduł I/O na pozycji n	1. Wyłącz zasilanie sterownika. 2. Wymień n-ty moduł I/O udostępniający dane procesowe lub zredukuj liczbę modułów I/O na n-1. 3. Ponownie włącz zasilanie.

Kod błędu 9 – Błąd wyjątku CPU

Tabela 108: Kod błędu 9 – Błąd wyjątku CPU: znaczenie kodu migania i sposoby usuwania błędu

Argument błędu	Przyczyna	Środek zaradczy
1	Niewłaściwe przydzielenie programu	Zakłócenie przebiegu programu – ▪ Skontaktuj się ze wsparciem technicznym WAGO.
2	Nadmiar stosu	Zakłócenie przebiegu programu. ▪ Skontaktuj się ze wsparciem technicznym WAGO.
3	Niedomiar stosu	Zakłócenie przebiegu programu. ▪ Skontaktuj się ze wsparciem technicznym WAGO.
4	Nieprawidłowe zdarzenie (NMI)	Zakłócenie przebiegu programu. ▪ Skontaktuj się ze wsparciem technicznym WAGO.
5	Zadziałał watchdog magistrali lokalnej.	✓ W przypadku aplikacji CODESYS: ▪ Skontaktuj się ze wsparciem technicznym WAGO. ✓ W przypadku aplikacji C: ▪ Sprawdź ustawienia monitorowania czasu.

3.9.1.1.2 Kody błędów LED MS

Tabela 109: Przegląd kodów błędu LED „MS"

Kod błędu	Znaczenie
1	Błąd konfiguracji

Tabela 110: Kod błędu 1 – Błąd konfiguracji: znaczenie kodu migania i sposoby usuwania błędu

Argument błędu	Przyczyna	Środek zaradczy
5	Błąd przy synchronizacji konfiguracji sterowania z magistralą systemową	1. Sprawdź konfigurację sterownika CODESYS pod kątem zadeklarowanych modułów I/O. 2. Porównaj je do faktycznie zainstalowanych modułów I/O. 3. Ponownie skompiluj projekt. 4. Wgraj projekt ponownie do sterownika.

3.9.2 Diagnostyka poprzez WBM

Tabela 111: Strona WBM „Log Message Viewer“ – grupa „Refresh Options“

Parametr	Znaczenie	
Read only the last	Włączanie/wyłączanie ostatnich n komunikatów; wprowadzanie liczby wyświetlanych komunikatów	
Automatic refresh interval (sec)	Włączanie/wyłączanie cyklicznej aktualizacji; wprowadzanie czasu cyklu w sekundach, z jakim ma być wykonywana cykliczna aktualizacja; w zależności od statusu zmienia się etykieta przycisku ("Refresh"/"Start"/"Stop").	
Source	Wybór źródła komunikatów diagnostycznych; Dostępne opcje na liście rozwijanej zależą od aktualnie zalogowanego użytkownika:	
	User	Tylko standardowe komunikaty diagnostyczne
	admin	Standardowe komunikaty diagnostyczne i wszystkie dane logowania w folderze `/var/log/*`

Tabela 112: Strona WBM „Download" – grupa „Diagnostic Information"

Parametr	Znaczenie
[Download]	Pobieranie informacji diagnostycznych z urządzenia

Tabela 113: Strona WBM „Network Capture“ – grupa „State“

Parametr	Znaczenie
Current State	Aktualny status zapisu sieci
Last Captured Package Count	Zapisane pakiety sieciowe
Last Refresh Time	Tu wyświetlany jest czas ostatniej aktualizacji Current State i Last Captured Package Count.

Tabela 114: Strona WBM „Network Capture“ – grupa „Configuration“

Parametr	Znaczenie	
Enable	Włączanie/wyłączanie zapisu	
Rotate Log Files	Włączanie/wyłączanie rotacyjnego zapisu; Gdy ta opcja jest włączona, ruch sieciowy jest zapisywany w maksymalnie trzech plikach o określonym maksymalnym rozmiarze. Po osiągnięciu maksymalnego rozmiaru pierwszego pliku dane są nadal zapisywane w drugim pliku itd. Gdy również trzeci plik osiągnie maksymalny rozmiar, dane z pierwszego pliku zostają nadpisane.	
Max. Filesize	Wprowadzanie maksymalnego rozmiaru pliku dla zapisu danych	
Storage Location	Wybieranie lokalizacji zapisanych danych	
	Internal Flash	Dane są zapisywane w wewnętrznej pamięci.
	SD-Card	Dane zapisywane są na karcie pamięci. Jeśli wybrana jest opcja „SD-Card“, ale karta pamięci jest już wyjęta, opcja ta nie jest już aktywna i można wybrać tylko „Internal-Flash“.
Listen On Network Interface	Wybór interfejsu sieciowego, z którego ma być przechwytywany ruch sieciowy; do wyboru są dostępne interfejsy sieciowe urządzenia.	

Tabela 115: Strona WBM „Network Capture“ – grupa „Filter Configuration“

Parametr	Znaczenie
Capture Filter	Wprowadzenie filtrów zapisu; służą one do przechwytywania jedynie istotnego lub wybranego ruchu sieciowego. Na przykład możliwy jest zapis komunikacji tylko z określonego portu lub z konkretnego adresu IP. Więcej informacji na temat możliwych ustawień filtrów można znaleźć w objaśnieniach „Capture Filter" w dokumentacji „Wireshark.

Tabela 116: Strona WBM „Network Capture“ – grupa „Log Download“

Parametr	Znaczenie
Select Log File	Wybór zapisu, który ma zostać pobrany z urządzenia

4 Uruchamianie

4.1 Włączanie sterownika

Przed włączeniem sterownika należy upewnić się, że:
- sterownik został prawidłowo zamontowany (patrz rozdział „Montaż“),
- wszystkie potrzebne przewody danych (patrz rozdział „Złącza“) są podłączone do odpowiednich interfejsów, a ich złącza wtykowe zamocowane przy pomocy śrub,
- podłączone jest zasilanie magistrali systemowej i obiektowej (patrz opis systemu),
- podłączony jest moduł końcowy (patrz opis systemu),
- zostało zapewnione wyrównanie potencjałów (patrz opis systemu), oraz
- wykonane jest poprawne ekranowanie (patrz opis systemu).

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

Start sterownika sygnalizowany jest krótkim rozbłyskiem wszystkich wskaźników LED.

Po kilku sekundach wskaźniki LED SYS sygnalizują pomyślne zakończenie procesu bootowania sterownika.

Równocześnie zostaje uruchomiony system runtime CODESYS V3.

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).

4.2 Ustalanie adresu IP hosta

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

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

1. Otwórz okno poleceń. W polu edycji **Start** > **System Windows** >**Wykonaj** (Windows® 10) lub **Start** > **Wyszukaj Programy/Pliki** (Windows® 7) wpisz polecenie „cmd“.
2. Potwierdź przyciskiem **[OK]** lub klawiszem ***Enter***.
3. Wpisz polecenie „ipconfig“.
4. Potwierdź klawiszem ***Enter***.

➡ Pojawią się adres IP, maska podsieci i standardowa brama z przynależnymi parametrami.

4.3 Ustawianie adresu IP

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

Tabela 117: Fabryczne ustawienie dla adresowania IP interfejsu ETHERNET

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

- Aby PC i produkt mogły się komunikować ze sobą, należy przy pomocy jednego z narzędzi do konfiguracji (np. WBM lub WAGO Ethernet Settings) dopasować adresowanie IP do struktury systemu, patrz **Konfiguracja [▸ 87]**.

Przykład integracji produktu (192.168.1.17) w istniejącej sieci:

- Adres IP hosta to **192.168.1.2**.
- Produkt 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 produktu przy masce podsieci 255.255.255.0 muszą być zgodne.

Tabela 118: Maska sieci 255.255.255.0

Host PC	Przestrzeń adresowa dla produktu
192.168.1.2	**192.168.1.**1 lub **192.168.1.**3 … **192.168.1.**254

4.3.1 Połączenie IP przez USB (PFC300)

Aby przeprowadzić uruchomienie i czynności serwisowe, można nawiązać połączenie IP przez USB.

1. Należy podłączyć sterownik do komputera PC za pomocą złącza serwisowego USB i przewodu serwisowego USB.
2. W przypadku użycia systemu Windows® 10, należy przejść od razu do kroku 4.
   ⇨ W systemie Windows® 7 po podłączeniu sterownik zachowuje się jak zewnętrzny dysk. Na tym dysku zapisany jest sterownik dla połączenia IP przez USB.
3. Zainstalować ten sterownik.
   ⇨ Po instalacji możliwa jest komunikacja przez połączenie IP przez USB.
4. W przeglądarce otworzyć stały adres IP produktu 192.168.42.42.

➡ Otworzy się interfejs Web-Based Management sterownika.

➡ Umożliwia on wykonanie wszystkich niezbędnych ustawień sterownika.

4.3.2 Ustawianie adresu IP przez WMB

Adres IP sterownika można zmienić bezpośrednio w zainstalowanym WBM, bez użycia innych narzędzi.

1. Podłącz sterownik do PC przy użyciu odpowiedniego przewodu sieciowego.
2. Na PC otwórz przeglądarkę internetową.
3. Otwórz WMB w sterowniku. W tym celu na pasku adresu przeglądarki wpisz: „https://<adres IP>/wbm“.
4. Jeśli nie znasz adresu IP, ustal go w sposób opisany dalej.
   ⇨ Po tym pojawia się żądanie uwierzytelnienia.

5. Wpisz nazwę użytkownika „user“ i odpowiednie hasło (ustawienie fabryczne „user“).
   ⇨ Jeśli standardowe hasło nie zostało jeszcze zmienione, pojawi się żądanie jego zmiany w tym momencie.
6. Otwórz zakładkę „Configuration“.
7. Wybierz w nawigacji punkt „Networking“ i podpunkt „TCP/IP Configuration“.
8. W grupie „TCP/IP Configuration“ w polu wyboru „IP Source“ wybierz pozycję „Static IP“.
9. W polu „Static IP Address“ podaj żądany adres IP.
10. W polu „Subnet Mask“ podaj żądaną maskę podsieci.
11. Aby potwierdzić zmiany, kliknij przycisk **[Submit]**.
    ⇨ Przez zmianę adresu IP połączenie ze sterownikiem zostaje przerwane.
12. Utwórz nowe połączenie ze zmienionym adresem IP.

4.3.3 Przydzielanie adresu IP przy pomocy 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 DHCP.

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

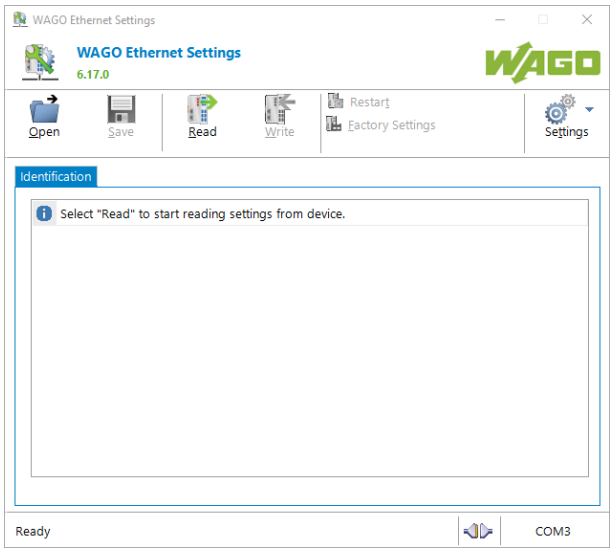
W połączeniu z serwerem DNC podłączonym do DHCP możliwe jest uzyskanie dostępu do urządzenia przez nazwę hosta. Składa się ona z przedrostka i adresu MAC lub jego części. Adres MAC produktu nadrukowany jest na etykiecie umieszczonej z boku.

4.3.4 Zmiana adresu IP przy użyciu „WAGO Ethernet Settings“

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

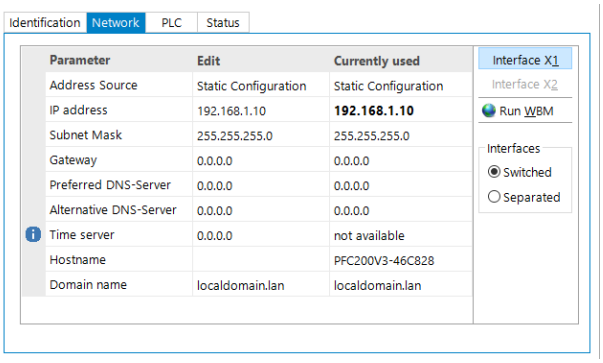
Do transmisji danych należy użyć przewodu serwisowego USB WAGO lub sieci IP.

1. Wyłącz napięcie robocze sterownika.
2. Nawiąż odpowiednie połączenie między sterownikiem i PC.
3. Włącz ponownie napięcie robocze sterownika.
4. Uruchom program „WAGO Ethernet Settings“.



Ilustracja 6: WAGO Ethernet Settings – ekran startowy (przykład)

5. Kliknij przycisk **[Lead]**, aby wczytać i zidentyfikować podłączony sterownik.
6. Wybierz zakładkę **„Network“**:



Ilustracja 7: WAGO Ethernet Settings – zakładka „Network“ (przykład)

7. Aby móc nadać stały adres, wybierz w punkcie **„Address Source“** w kolumnie **„Parameter“** wartość „Static Configuration“. Standardowo aktywowany jest BootP.
8. W kolumnie **„Parameter“** wpisz żądany adres IP oraz adresy podsieci i bramy.
9. Kliknij przycisk **[Write]**, aby przejąć adres do sterownika. („WAGO Ethernet Settings“ będzie za każdym razem powodował automatyczny restart sterownika. Może to potrwać ok. 30 sekund.)
10. Teraz możesz zamknąć „WAGO Ethernet Settings“, bądź w razie potrzeby wprowadzić dalsze ustawienia bezpośrednio w systemie zarządzania przez WWW (WBM). W tym celu kliknij przycisk **[Run WBM]** po prawej stronie okna.

4.3.5 Ustawianie domyślnego adresu IP za pomocą przełącznika adresów

W przypadku produktów z przełącznikiem adresów można za pomocą tego przełącznika zmienić ustawienia sieci.

Przełącznik adresów zawiera 8 pojedynczych wyłączników 1 ... 8 z wartościami 1 ... 128. Włącznik wyłączony ma wartość 0. Ustawiona wartość adresu wynika z sumy wartości wszystkich włączonych przełączników (przykład: przełącznik 7, 6 i 3 na "ON" odpowiada wartości adresu 64 + 32 + 4 = 100). Dzięki temu można ustawić wartość adresu na 0 ... 255.

Ustawienie przełącznika adresów jest odczytywane tylko przy restarcie sterownika. Zmiany położeń przełączników podczas pracy są ignorowane do następnego restartu.

Jeśli złącza ETHERNET X1 i X2 pracują w trybie separowanym, ustawienia mają wpływ tylko na interfejs X1. Dla interfejsu X2 wszystkie ustawienia pozostają bez zmian. Jeśli złącza ETHERNET X1 i X2 pracują w trybie switched, ustawienia dotyczą zarówno interfejsu X1, jak i X2.

Poniższa tabela przedstawia znaczenie wartości adresu przełącznika adresów.

Tabela 119: Przełączanie adresów

Adres	Znaczenie
0	Konfiguracja parametrów IP odbywa się za pomocą ustawień w systemie zarządzania opartym na przeglądarce (WBM) lub poprzez ustawienia fabryczne.
1 … 254	Przydzielany jest stały adres IP. Adres IP składa się z adresu sieciowego i ustawionej wartości adresu. Adres sieciowy konfiguruje się przez WBM i jest on ustawiony fabrycznie na 192.168.1.0 (maska podsieci 255.255.255.0, brama standardowa 0.0.0.0).
255	Adres IP przydziela się za pomocą protokołu DHCP.

Przykłady:

Ustawiony adres IP wynosi 192.168.129.129, przełącznik adresów jest ustawiony na wartość 203.

Jeśli maska sieci wynosi 255.255.255.0, cała czwarta wartość adresu IP zostaje zastąpiona:

Ustawiona maska sieci:	255.255.255.000
Ustawiony adres IP:	192.168.129.129
Wynikający adres sieciowy:	192.168.129.000
Wynikający adres urządzenia:	---.---.---.129
Przełącznik adresów:	---.---.---.203
Adres sieciowy po restarcie:	192.168.129.000
Adres urządzenia po restarcie:	---.---.---.203
Adres IP po restarcie:	192.168.129.203

Możliwe i konfigurowalne są 254 adresy (1 … 254).

Jeśli maska sieci jest większa (np. 255.255.255.240), wartość adresu jest ograniczona. Uwzględniana jest tylko część mikroprzełączników DIP przełącznika adresów. W poniższym przykładzie są to tylko przełączniki 1 … 4. Położenie przełącznika 5 … 8 jest ignorowane:

Ustawiona maska sieci:	255.255.255.240
Ustawiony adres IP:	192.168.129.129
Wynikający adres sieciowy:	192.168.129.128
Wynikający adres urządzenia:	---.---.---.001
Przełącznik adresów:	---.---.---.203
Adres sieciowy po restarcie:	192.168.129.128
Adres urządzenia po restarcie:	---.---.---.011
Adres IP po restarcie:	192.168.129.139

Możliwa jest konfiguracja 254 adresów (1…254), jednak dostępnych do użycia jest tylko 14 adresów (1…14).

Jeśli maska sieci jest mniejsza (np. 255.255.240.000), zwiększa się możliwa liczba urządzeń w podsieci, ale za pomocą przełącznika adresów można ustawić tylko część możliwych adresów urządzenia:

Ustawiona maska sieci:	255.255.240.000
Ustawiony adres IP:	192.168.129.129
Wynikający adres sieciowy:	192.168.128.000
Wynikający adres urządzenia:	---.---.--1 129
Przełącznik adresów:	---.---.---.203
Adres sieciowy po restarcie:	192.168.128.000
Adres urządzenia po restarcie:	---.---.---.203
Adres IP po restarcie:	192.168.128.203

Możliwe są 4094 adresy (1 ... 4094), ale można ustawić tylko 254 adresy (1 ... 254).

4.3.6 Tymczasowe ustawianie stałych adresów IP

W tym procesie adresy IP dla interfejsów sieciowych X1 ... X<n> ustawia się tymczasowo na stałe adresy IP.
Dla każdego zastosowanego bridge'a przypisywanym interfejsom nadawany jest osobny adres, przy czym bridge 1 otrzymuje adres IP "192.168.1.17", bridge 2 adres IP "192.168.2.17" itd.

Nie jest przeprowadzany reset.

Aby ustawić tymczasowo stałe adresy IP, należy postępować w następujący sposób:

1. Ustaw przełącznik trybu pracy w pozycji STOP.
2. Naciśnij przycisk resetu przez czas dłuższy niż 8 sekund.

➡ Wykonanie jest zasygnalizowane miganiem wskaźników LED „SYS“ na pomarańczowo.

Jeśli po aktywowaniu tymczasowych adresów IP dokonywane będą zmiany w konfiguracji IP brigde'a, nowe ustawienia będą stale przejmowane i natychmiast stosowane. Skonfigurowany bridge opuszcza tym samym tymczasowy tryb adresu IP. Inne bridge'e zachowują swoje tymczasowe adresy IP aż do restartu/resetu.

Aby anulować to ustawienie, postępuj w następujący sposób:

- przeprowadź reset oprogramowania,

lub

- wyłącz i ponownie włącz produkt.

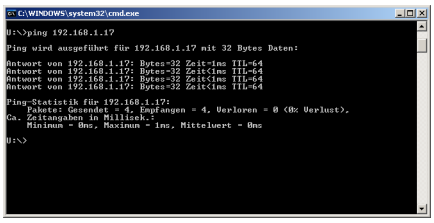
4.4 Testowanie połączenia sieciowego

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

1. Otwórz okno poleceń. W polu edycji **Start** > **System Windows** >**Wykonaj** (Windows® 10) lub **Start** > **Wyszukaj Programy/Pliki** (Windows® 7) wpisz polecenie „cmd“.
2. Potwierdź przyciskiem **[OK]** lub klawiszem ***Enter***.
3. Wpisz w oknie poleceń polecenie „ping“ i adres IP sterownika (np. ping 192.168.1.17).

4. Potwierdź klawiszem ***Enter***.

   ⇨ 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. W tym przypadku należy sprawdzić ustawienia sieci.



Ilustracja 8: Przykład testu działania

5. Zamknij wiersz polecenia, jeśli test zakończył się pomyślnie.

4.5 Zmiana haseł

ⓘ Wskazówka

Zmienić hasła!

Ustawione fabrycznie, standardowe hasła podane w niniejszej instrukcji obsługi nie stanowią wystarczającego zabezpieczenia!

- Należy zmienić te hasła stosownie do potrzeb.

ⓘ Wskazówka

Dopuszczalne znaki w hasłach

Hasło może zawierać tylko następujące znaki:
małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9) oraz znaki spcjalne (! " # $ % & ' ( ) * + , . / : ; < = > ? @ [ ] ^ _ ` { } | ~ –).

W celu zwiększenia bezpieczeństwa, hasła powinny zawierać kombinację małych liter, dużych liter, cyfr i znaków specjalnych.
W skład haseł nie powinny wchodzić nazwy popularne, daty urodzenia i inne łatwe do zgadnięcia informacje.

Dlatego przed uruchomieniem sterownika należy zmienić hasła standardowe!

Dla grupy użytkowników „Użytkownicy Linux®" zastosowano standardowe hasła i wymieniono je w tabeli **Użytkownik Linux® [▸ 34]**.

Aby zmienić te hasła poprzez WBM, należy postępować w sposób następujący:

1. Podłącz sterownik do PC przez jeden z interfejsów sieciowych (X1, X2).
2. Otwórz na PC przeglądarkę internetową i wywołaj WBM sterownika.
3. Zaloguj się w sterowniku jako użytkownik „root", „admin" lub „user" przy pomocy standardowego hasła.
4. Zmień hasło dla wszystkich zgłoszonych użytkowników na stronie WBM „Configuration of the users for the WBM".

5. W ten sposób można zmienić hasła dla wszystkich użytkowników.

Aby zmienić hasła przez program terminalowy, należy postępować w następujący sposób:

1. Podłącz sterownik do PC korzystając z interfejsu sieciowego X1.
2. Otwórz na PC program terminalowym.
3. Zaloguj się w sterowniku jako użytkownik „root" przy pomocy standardowego hasła.
4. Zmień hasło dla wszystkich użytkowników przy użyciu poleceń „passwd root", „passwd admin" i „passwd user".

4.6 Wyłączanie/restart

Aby wyłączyć sterownik, należy odłączyć zasilanie.

Aby przeprowadzić reset oprogramowania (restart) sterownika, należy nacisnąć przycisk Reset. Alternatywnie można wyłączyć i ponownie włączyć sterownik.

ⓘ Wskazówka

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

Aby zmiany parametrów zostały zrealizowane, wymagany jest restart sterownika. Zapis 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 przy użyciu programowej funkcji Reboot. Dzięki temu wszystkie procesy zapisu zostaną przeprowadzone poprawnie i w pełni zakończone.

5 Konfiguracja

5.1 Konfiguracja za pomocą WBM

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

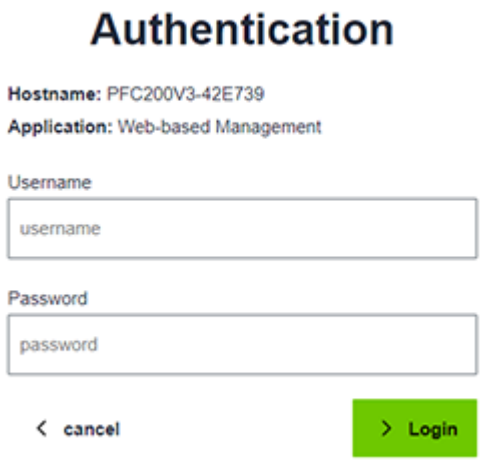
1. Podłącz sterownik do PC poprzez złącze ETHERNET X1 i sieć ETHERNET lub złącze serwisowe USB i przewód serwisowy USB.
2. Na PC należy otworzyć przeglądarkę internetową.
3. W pasku adresu przeglądarki internetowej wpisz „https://", a następnie adres IP sterownika, a po nim „/wbm", np. „https://192.168.1.17/wbm". Należy pamiętać, że PC i sterownik muszą znajdować się w tej samej podsieci, patrz .
   Jeśli nie znasz adresu IP i nie możesz go ustalić, przełącz sterownik czasowo na stały domyślny adres IP "192.168.1.17", patrz .

   ⓘ Wskazówka **Uwzględnić obciążenie przez program CODESYS**

   Jeśli sterownik obciążony jest 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 zatrzymaj zatem aplikację CODESYS.

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



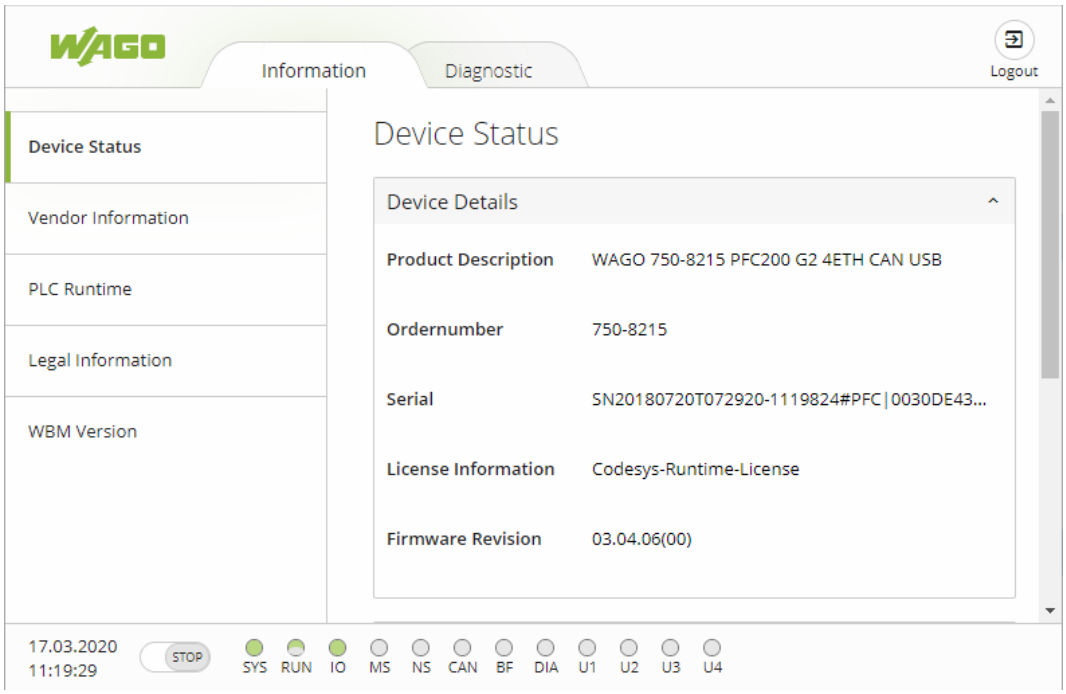
Ilustracja 9: Okno logowania

4. Wprowadź nazwę użytkownika i hasło.
5. Kliknij przycisk **[> Login]**.

➡ W zależności od wybranego użytkownika wyświetlane są 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. przy pomocy **[F5]**), należy się ponownie zalogować, gdyż w tym przypadku przeglądarka nie ma możliwości zapisania plików z danej sesji logowania.

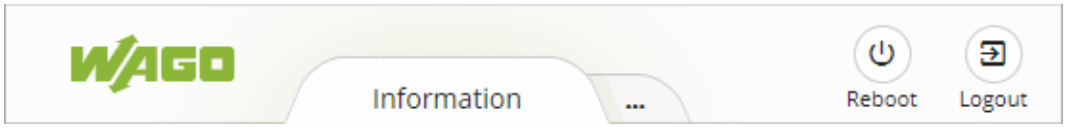
5.1.1 Ogólne informacje o stronie



Ilustracja 10: Okno przeglądarki WBM (przykład)

W wierszu nagłówkowym okna przeglądarki wyświetlane są zakładki różnych obszarów WBM i przyciski **[Reboot]** oraz **[Logout]**. Przycisk **[Reboot]** widoczny jest tylko wtedy, gdy zalogowany jest administrator. Naciśnięcie przycisku **[Reboot]** powoduje restart sterownika. Restart może potrwać kilka minut. Przycisk **[Logout]** służy do wylogowania aktualnego użytkownika. Pojawia się wtedy ponownie polecenie zalogowania.

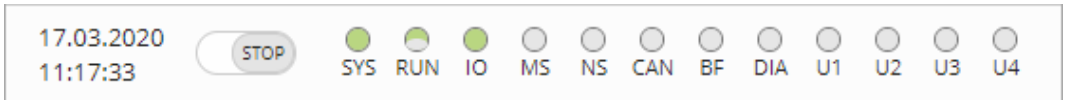
Gdy na wybranej szerokości okna nie mieszczą się wszystkie zakładki, w miejscu niewyświetlonej zakładki widoczna jest zakładka z symbolem (...). Dzięki temu poprzez listę rozwijalną można wybrać zakładki, które nie są wyświetlane.



Ilustracja 11: Wiesz nagłówkowy 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 12: Wiersz statusu WBM (przykład)

- Data i godzina – lokalny czas i lokalna data na urządzeniu
- Stan przełącznika trybu pracy
- Stany LED urządzenia:
  Diody LED są oznaczone odpowiednim opisem. Stany są symbolizowane za pomocą grafiki. Możliwe są następujące stany LED:
  – 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. Zawarty jest tu czas wysłania wiadomości.
Stany wyświetlone w WBM nie odpowiadają w każdym momencie aktualnym stanom na sterowniku. Transmisja danych wymaga określonego czasu, a odpytywanie następuje w określonych interwałach. Czas między odpytywaniami wynosi 30 sekund.

5.1.2 Przegląd stron WBM i prawa dostępu

Prawa dostępu do stron WBM zostały przedstawione w tabeli poniżej. Użytkownicy z niższymi uprawnieniami mogą nie mieć dostępu do stron lub mogą je tylko przeglądać.

Tabela 120: Prawa dostępu dla stron WBM

Zakładka	Nawigacja		Tytuł strony WBM	Użytkownik
Informacja	Device Status		Device Status	User
	Vendor Information		Vendor Information	User
	PLC Runtime		PLC Runtime Information	User
	Legal Information			
		WAGO Licenses	WAGO Software License Agreement	User
		Open Source Licenses	Open Source Licenses	User
		WBM Licenses	WBM Third Party License Information	User
		Trademarks Information	Trademarks Information	
	WBM Version		WBM Version Info	User
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 Domainname	User
		Routing	Routing	User
		STP/RSTP	Spanning Tree Protocol	User
	Clock		Clock Settings	User
	Administration			
		Serial Interface	Configuration of Serial Interface RS232/ RS485	admin
		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

Zakładka	Nawigacja		Tytuł strony WBM	Użytkownik
		DHCP Server	DHCP Server Configuration	admin
		DNS	Configuration of DNS Server	admin
	Cloud Connectivity			
		Status	Status Overview	admin
		Connection <n>	Configuration of Connection <n>	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 Parameters	admin
	Commissioning		Commissioning Settings	admin
	Docker		DockerSettings	admin
	Users		WBM User Configuration	admin
	modem		Configuration of internal 4G Modem	admin
Fieldbus	OPC UA		OPC UA Configuration	admin
	PROFIBUS DP		Configuration of PROFIBUS DP Slave	User
	BACnet			
		Status	BACnet Status	admin
		Configuration	BACnet Configuration	admin
		Data Link	BACnet Data Link	admin
		Storage Location	BACnet Storage Location	admin
		Info	BACnet Info	admin
Security	Open VPN/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
	Boot Mode		Boot Mode Configuration	admin
	TLS		Security Settings	admin
	Integrity		Advanced Intrusion Detection Environment (AIDE)	admin
	WAGO Device Access		WAGO Device Access	admin
Diagnostic	Log Message		Log Message Viewer	User
	Download		Download	admin
	Network Capture		Network Capture	admin

5.2 Konfiguracja przy pomocy „WAGO Ethernet Settings“

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

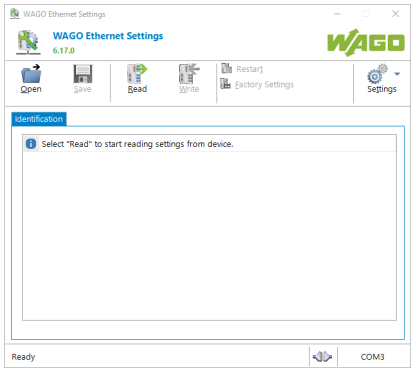
ⓘ Wskazówka

Zwrócić uwagę na wersję oprogramowania!

Przy konfiguracji sterownika należy korzystać co najmniej z wersji „WAGO Ethernet Settings" 06.15.01 z 2021-02-08.

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

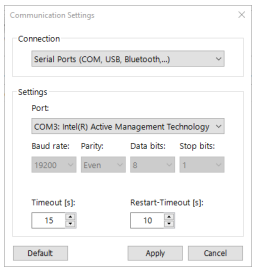
Do transmisji danych należy użyć odpowiedniego przewodu serwisowego USB-C lub sieci IP.



Ilustracja 13: „WAGO Ethernet Settings" – ekran startowy (przykład)

- Należy kliknąć na „Settings"" i potem na „Communication".

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



Ilustracja 14: „WAGO Ethernet Settings" – konfiguracja połączeń komunikacyjnych (przykład)

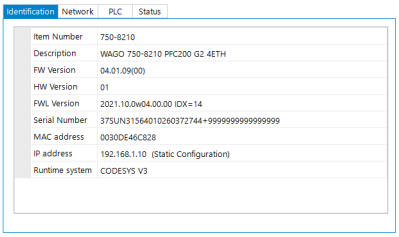
Po skonfigurowaniu „WAGO Ethernet Settings" i kliknięciu na **[Apply]**, automatycznie zostanie nawiązane połączenie ze sterownikiem.

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

5.2.1 Zakładka Identification

Tu zawarte są podstawowe informacje o podłączonym produkcie.

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

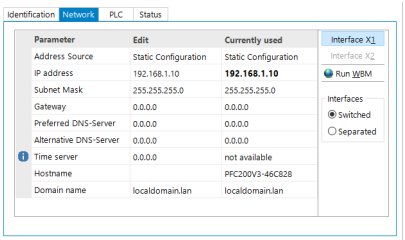


Ilustracja 15: „WAGO Ethernet Settings“ – zakładka Identification (przykład)

5.2.2 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.



Ilustracja 16: „WAGO Ethernet Settings“ – zakładka Network (przykład)

Producent

Tu decyduje się, w jaki sposób sterownik ma uzyskać adres IP: statycznie, przez DHCP lub przez BootP.

Adres IP, maska podsieci, brama

W przypadku konfiguracji statycznej tu wpisuje się parametry sieci.

ⓘ Wskazówka

Ograniczone ustawienia dla bram domyślnych!

Przy pomocy „WAGO Ethernet Settings“ można ustawić tylko bramę domyślną 1. Bramę domyślną 2 można ustawić wyłącznie w WBM!

Preferowany serwer DNS, alternatywny serwer DNS

Tu w razie potrzeby wpisuje się adres IP dostępnego serwera DNS, który może być wykorzystany w tłumaczeniu nazw w sieci.

Serwer czasowy

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

Nazwa hosta

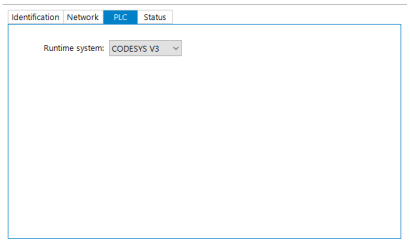
Tu wyświetlana jest nazwa hosta sterownika. W ustawieniach fabrycznych nazwa hosta składa się z ciągu „PFCx00-"i ostatnich 3 bajtów adresu MAC. Ta standardowa wartość jest stosowana zawsze wtedy, gdy wybrana samodzielnie nazwa usuwana jest w kolumnie „Edit“.

Nazwa domeny

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

5.2.3 Zakładka PLC

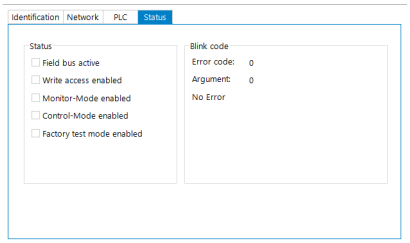
Tu można wybrać system runtime.



Ilustracja 17: „WAGO Ethernet Settings“ – zakładka Protokół (przykład)

5.2.4 Zakładka Status

Tu wyświetlane są ogólne informacje o statusie sterownika.



Ilustracja 18: „WAGO Ethernet Settings“ – zakładka Status (przykład)

6 Serwis

6.1 Zmiany firmware'u

UWAGA

Nie wyłączać sterownika!

Przerwanie procedury aktualizacji/aktualizacji wstecznej może uszkodzić sterownik.

- Dlatego podczas procedury aktualizacji/aktualizacji wstecznej nie należy wyłączać sterownika i nie odłączać zasilania!

Wskazówka

Należy uwzględnić wersję firmware'u!

Przy urządzeniach z fabryczną instalacją firmware'u >= FW 05 nie jest możliwa aktualizacja wsteczna do wersji <= FW 04!
Należy zastosować specjalny obraz aktualizacji wstecznej.

Wskazówka

Uwzględnić dokumentację odpowiednią do docelowej wersji firmware!

Dzięki zmianie firmware'u 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.

1. Dlatego po zmianie firmware'u należy korzystać z dokumentacji odpowiadającej docelowemu firmware'owi.
2. W razie pytań należy skontaktować się ze wsparciem WAGO.

Firmware można aktualizować na dwa różne sposoby:
- przy użyciu WAGOupload
- przy użyciu karty pamięci i WBM

6.1.1 Przeprowadzanie aktualizacji/aktualizacji wstecznej przy użyciu WAGOupload

1. Uruchom WAGOupload.
2. Kliknąć **[Update Firmware]**.
3. W oknie dialogowym „Select Target Controllers" przy opcji „Transfer via TCP/IP" wpisz adres IP sterownika.
4. Kliknij przycisk **[Find Controller]**.
   ⇨ Teraz na liście wyświetlony zostaje Twój sterownik.
5. Zaznacz wyświetlony sterownik i kliknij przycisk **[Next]**.
6. W oknie dialogowym „Select Update File" wybierz plik *.wup żądanego firmware'u.
7. Kliknij na **[Dalej]**.

8. Potwierdź listę przyciskiem **[Weiter]**.
9. Poczekaj, aż proces zostanie zakończony komunikatem o statusie i następnie kliknij przycisk **[Exit]**, aby zamknąć okno.

➡ Na sterowniku dostępny jest teraz nowo zainstalowany firmware.

6.1.2 Przeprowadzanie aktualizacji/aktualizacji wstecznej przy użyciu karty pamięci i WBM

1. Najpierw skopiuj plik obrazu firmware'u (plik *.img) na kartę pamięci za pomocą odpowiedniego narzędzia.
2. Zapisz aplikację i ustawienia sterownika.
3. Wyłącz sterownik.
4. Włóż kartę pamięci z instalowanym firmware'em do gniazda.
5. Włącz sterownik.

   ⇨ Sterownik zostaje uruchomiony z obrazem firmware'u, który ma być zainstalowany z karty pamięci.
6. Po uruchomieniu sterownika otwórz stronę WBM „Administration“ > „Create Boot Image“ (w tym celu należy zawsze zmienić tymczasowy adres IP).
7. Utwórz obraz boot w wewnętrznej pamięci. W tym celu kliknij przycisk **[Start Copy]**.
8. Po zakończeniu tej czynności wyłącz sterownik.
9. Usuń kartę pamięci.
10. Ponownie włącz sterownik.

➡ Sterownik jest teraz uruchamiany z nowo zainstalowaną wersją firmware z wewnętrznej pamięci.

6.2 Wyzwalanie funkcji RESET

Przy pomocy przełącznika trybu pracy i przycisku RESET można realizować różne funkcje resetu.

6.2.1 Gorący reset

Przy gorącym resecie resetowane są wszystkie aplikacje CODESYS V3. Wszystkie dane globalne ustawiane są na poziomie ich wartości inicjacyjnych. Odpowiada on poleceniu „Reset warm“ w środowisku CODESYS V3 IDE.

- 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.

6.2.2 Zimny reset

W tym przypadku resetowane są wszystkie aplikacje CODESYS V3. Wszystkie dane globalne i zmienne nieulotne ustawiane są na poziomie ich wartości inicjacyjnych. Odpowiada on poleceniu „Reset cold“ w środowisku CODESYS V3 IDE.

1. 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.

2. Następnie można puścić przełącznik trybu pracy.

6.2.3 Reset programowy (restart)

Przy resecie programowym produkt uruchamiany jest ponownie.

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

➡ Wykonanie sygnalizowane jest krótkim rozbłyskiem wszystkich wskaźników LED. Po kilku dodatkowych sekundach dioda „SYS" wskazuje, że sterownik został pomyślnie uruchomiony.

6.2.4 Reset sterownika

UWAGA

Nie wyłączać sterownika!

Przerwanie procedury aktualizacji wstecznej może uszkodzić sterownik.

- Dlatego podczas procedury Reset nie należy wyłączać sterownika i nie odłączać zasilania!

Wskazówka

Wszystkie parametry i hasła zostaną nadpisane!

Przy resecie wszystkie parametry i hasła zostaną nadpisane.
Zapisane projekty startowe, w tym istniejące dane wizualizacji internetowej, zostaną usunięte.
Niezainstalowane funkcje firmware nie zostaną nadpisane.
Licencje na oprogramowanie zostaną zachowane.

- W razie pytań należy skontaktować się ze wsparciem WAGO.

Aby przeprowadzić „Controller-Reset", należy postępować w następujący sposób:

1. Naciśnij i przytrzymaj przycisk resetu.
2. Przełącznik trybu pracy należy ustawić w pozycji „RESET" i przytrzymać w tej pozycji.
3. Przytrzymaj 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, puść przełącznik trybu pracy i przycisk Reset.

➡ Sterownik został zresetowany i wykonuje automatyczny restart.

Wskazówka

Nie przerywać procedury resetu!

Przy zbyt wczesnym puszczeniu przycisku resetu produkt uruchomi się ponownie, bez zrealizowania resetu sterownika.

6.3 Aktualizacja certyfikatów Root

Aby uaktualnić w sterowniku certyfikaty Root, należy postępować w następujący sposób:

1. Pobierz do sterownika aktualny plik Root CA bundle ze strony internetowej https://curl.haxx.se/ca.
2. Zmień nazwę pliku na „ca-certificates.crt“.
3. Prześlij plik za pomocą klienta SFTP lub FTP do folderu /etc/ssl/certs w sterowniku.
4. Zrestartuj sterownik. W tym celu należy skorzystać z funkcji Reboot w WBM.

7 Załącznik

7.1 Dialogi konfiguracyjne

7.1.1 Strony WBM

7.1.1.1 Przegląd stron WBM i prawa dostępu

Prawa dostępu do stron WBM zostały przedstawione w tabeli poniżej. Użytkownicy z niższymi uprawnieniami mogą nie mieć dostępu do stron lub mogą je tylko przeglądać.

Tabela 121: Prawa dostępu dla stron WBM

Zakładka	Nawigacja		Tytuł strony WBM	Użytkownik
Informacja	Device Status		Device Status	User
	Vendor Information		Vendor Information	User
	PLC Runtime		PLC Runtime Information	User
	Legal Information			
		WAGO Licenses	WAGO Software License Agreement	User
		Open Source Licenses	Open Source Licenses	User
		WBM Licenses	WBM Third Party License Information	User
		Trademarks Information	Trademarks Information	
	WBM Version		WBM Version Info	User
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 Domainname	User
		Routing	Routing	User
		STP/RSTP	Spanning Tree Protocol	User
	Clock		Clock Settings	User
	Administration			
		Serial Interface	Configuration of Serial Interface RS232/ RS485	admin
		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
		DHCP Server	DHCP Server Configuration	admin

Zakładka	Nawigacja		Tytuł strony WBM	Użytkownik
		DNS	Configuration of DNS Server	admin
	Cloud Connectivity			
		Status	Status Overview	admin
		Connection <n>	Configuration of Connection <n>	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 Parameters	admin
	Commissioning		Commissioning Settings	admin
	Docker		DockerSettings	admin
	Users		WBM User Configuration	admin
	modem		Configuration of internal 4G Modem	admin
Fieldbus	OPC UA		OPC UA Configuration	admin
	PROFIBUS DP		Configuration of PROFIBUS DP Slave	User
	BACnet			
		Status	BACnet Status	admin
		Configuration	BACnet Configuration	admin
		Data Link	BACnet Data Link	admin
		Storage Location	BACnet Storage Location	admin
		Info	BACnet Info	admin
Security	Open VPN/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
	Boot Mode		Boot Mode Configuration	admin
	TLS		Security Settings	admin
	Integrity		Advanced Intrusion Detection Environment (AIDE)	admin
	WAGO Device Access		WAGO Device Access	admin
Diagnostic	Log Message		Log Message Viewer	User
	Download		Download	admin
	Network Capture		Network Capture	admin

W kolejnych rozdziałach opisano parametry i możliwości ustawień dla stron WBM.

7.1.1.2 Zakładka „Information“

7.1.1.2.1 Strona „Device Status“

Na stronie „Device Status“ wyświetlane są dane identyfikacyjne produktu i najważniejsze właściwości sieci.

Grupa „Device Details“

W tej grupie wyświetlane są właściwości produktu.

Tabela 122: Strona WBM „Device Status“ – grupa „Device Details“

Parametr	Znaczenie
Product Description	Nazwa produktu
Numer zamówieniowy	Numer katalogowy produktu
Unique Item Identifier (UII)	Unikatowy numer identyfikacyjny produktu
License Information	Wskazanie, że system runtime CODESYS jest zainstalowany.
Firmware Revision	Stan firmware'u

Grupa „Network TCP/IP Details“

W tej grupie wyświetlane są właściwości sieci i interfejsów produktu.

Tabela 123: 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	
Interfejs <n>	Aktualnie skonfigurowany interfejs; Dla każdego skonfigurowanego interfejsu 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 **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
	external	Adres IP przypisywany jest ewentualnie przez aplikację sieciową; Ma to miejsce na przykład wtedy, gdy adres IP zarządzany jest przez aplikację.
IP Address	Aktualny adres IP produktu	
Subnet Mask	Aktualna maska podsieci produktu	

7.1.1.2.2 Strona „Vendor Information“

Na stronie „Vendor Information“ wyświetlane są nazwa i adres producenta.

7.1.1.2.3 Strona „PLC Runtime Information“

Na stronie „PLC Runtime Information“ znajdują się informacje o aktywowanym systemie runtime.
Ponadto jest tu link otwierający WebVisu.

Grupa „Runtime“

Tabela 124: Strona WBM „PLC Runtime Information” – grupa „Runtime“

Parametr	Znaczenie
Wersja	Aktualnie aktywowany system runtime Przy wyłączonym systemie runtime wyświetlana jest informacja „None".

Grupa „WebVisu“

Tu znajduje się link, którym można otworzyć WebVisu.

7.1.1.2.4 Strona „WAGO Software License Agreement“

Na stronie „WAGO Software License Agreement“ wyszczególnione są warunki licencji dla oprogramowania WAGO zastosowanego w produkcie.

7.1.1.2.5 Strona „Open Source Licenses“

Na stronie „Open Source Licenses“ wyszczególnione są (w kolejności alfabetycznej) warunki licencji dla oprogramowania Open Source zastosowanego w produkcie.

7.1.1.2.6 Strona „WBM Third Party License Information“

Na stronie „WBM Third Party License Information“ znajdują się teksty o licencji dla oprogramowania Open Source, dotyczące samego systemy WBM.

7.1.1.2.7 Strona „Trademarks Information“

Na stronie „Trademarks Information“ znajduje się lista praw ochronnych i znaków towarowych.

7.1.1.2.8 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.

7.1.1.3 Zakładka „Configuration“

7.1.1.3.1 Strona „PLC Runtime Configuration“

Na stronie „PLC Runtime Configuration“ znajdują się ustawienia projektu bootowalnego utworzonego w środowisku programistycznym i ustawienia do wizualizacji sieciowej utworzonej w systemie runtime.

Grupa „General PLC Runtime Configuration“

Zmiana systemu operacyjnego zostanie zrealizowana natychmiast.
Zmiana katalogu Home zostanie zrealizowana dopiero po następnym restarcie produktu. W tym celu należy skorzystać z funkcji Reboot WBM. Nie należy wyłączać produktu zbyt wcześnie!

Tabela 125: Strona WBM „PLC Runtime Configuration” – grupa „General PLC Runtime Configuration“

Parametr	Znaczenie
PLC Runtime Version	Wybór aktywnego systemu runtime PLC

Parametr	Znaczenie	
	none	Żaden system runtime nie jest aktywowany.
	CODESYS V3	System runtime CODESYS V3 jest aktywowany.
Home directory on memory card enabled	Wybór lokalizacji dla katalogu Home systemu runtime	
	☐	Katalog Home dla systemu operacyjnego zapisywany jest w wewnętrznej pamięci sterownika.
	☑	Katalog Home dla systemu operacyjnego zapisywany jest na karcie pamięci.
[Submit]	Zaakceptuj zmiany	

ⓘ Wskazówka

Przy przełączeniu systemu runtime usuwane są wszystkie dane!

Przy przełączeniu systemu runtime katalog Home dla systemu operacyjnego zostaje całkowicie usunięty.

ⓘ Wskazówka

Przed przełożeniem katalogu Home włożyć kartę pamięci!

Tylko pierwsza partycja karty pamięci dostępna jest pod /media/sd i może zostać wykorzystana jako katalog Home.

- Jeśli katalog Home ma być przełożony na kartę pamięci, należy najpierw włożyć do urządzenia kartę sformatowaną przy pomocy wspieranego systemu plików.

Grupa „Webserver Configuration"

Zmiana zostaje zrealizowana natychmiast.

Tabela 126: Strona WBM „PLC Runtime Configuration" – grupa „Webserver Configuration"

Parametr	Znaczenie	
CODESYS 3 Webserver State	Status (enabled/disabled) serwera WWW CODESYS V3	
Default Webserver	Wybór widoku strony przy wpisaniu samego adresu IP produktu	
	Web-Based-Management	Wyświetlany jest Web-Based-Management.
	WebVisu	Wyświetlana jest wizualizacja sieciowa systemu runtime.
[Submit]	Zaakceptuj zmiany	

W ustawieniu fabrycznym przy wpisaniu adresu IP otwierany jest 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 przy pomocy adresu „https://<adres IP>/wbm" oraz wizualizację sieciową przy pomocy adresu „https://<adres IP>/webvisu".

ⓘ Wskazówka

Możliwe komunikaty błędu przy otwieraniu wizualizacji sieciowej

Wskaźnik „500 - Internal Server Error" wskazuje, że serwer WWW nie jest włączony. Strona o tytule „WebVisu not available" wskazuje, że do produktu nie została załadowana aplikacja z wizualizacją sieciową.

7.1.1.3.2 Strona „TCP/IP Configuration"

Na stronie „TCP/IP Configuration" znajdują się ustawienia TCP/IP dla interfejsów sieci ETHERNET.

Grupa „Bridge Interfaces"

Dla każdego skonfigurowanego bridge'a właściwości są wyświetlane w osobnym obszarze.

Tabela 127: Strona WBM „TCP/IP Configuration" – grupa „Bridge Interfaces"

Parametr	Znaczenie	
Bridge <n>	Ustawienia dla wybranego bridge'a	
Current IP Address	Aktualny adres IP	
Current Subnet Mask	Aktualna maska podsieci	
Current Default Gateway	Adres IP aktualnej domyślnej bramy	
IP Source	Wybierz adres IP.	
	Static IP	Statyczne adresowanie IP
	DHCP	Dynamiczne adresowanie IP przez DHCP
	BootP	Dynamiczne adresowanie IP przez BootP
Static IP Address	Wprowadzanie statycznego adresu IP; adres IP jest aktywny, gdy w polu wyboru **IP Source** zaznaczona jest „Static IP".	
Subnet Mask	Wprowadzanie maski podsieci; maska podsieci jest aktywna, gdy w polu wyboru **IP Source** zaznaczona jest „Static IP".	
Default Gateway	Wprowadzanie adresu IP bramy domyślnej	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

Grupa „Dummy Interfaces"

Dla każdego skonfigurowanego interfejsu Dummy właściwości są wyświetlane w osobnym obszarze.

Tabela 128: Strona WBM „TCP/IP Configuration" – grupa „Dummy Interfaces"

Parametr	Znaczenie	
Dummy <n>	Ustawienia dla wybranego interfejsu Dummy	
Current IP Address	Aktualny adres IP	
Current Subnet Mask	Aktualna maska podsieci	
IP Source	Wybierz adres IP.	
	Static IP	Statyczne adresowanie IP
Static IP Address	Wprowadzanie statycznego adresu IP; adres IP jest aktywny, gdy w polu wyboru **IP Source** zaznaczona jest „Static IP".	
Subnet Mask	Wprowadzanie maski podsieci; maska podsieci jest aktywna, gdy w polu wyboru **IP Source** zaznaczona jest „Static IP".	

Parametr	Znaczenie
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

Grupa „VLAN Interfaces“

Dla każdego skonfigurowanego interfejsu VLAN właściwości są wyświetlane w osobnym obszarze.

Tabela 129: Strona WBM „TCP/IP Configuration“ – grupa „VLAN Interfaces“

Parametr	Znaczenie	
VLAN <n>	Ustawienia wybranego interfejsu VLAN	
Current IP Address	Aktualny adres IP	
Current Subnet Mask	Aktualna maska podsieci	
IP Source	Wybierz adres IP.	
	Static IP	Statyczne adresowanie IP
	DHCP	Dynamiczne adresowanie IP
Static IP Address	Wprowadzanie statycznego adresu IP; adres IP jest aktywny, gdy w polu wyboru **IP Source** zaznaczona jest „Static IP".	
Subnet Mask	Wprowadzanie maski podsieci; maska podsieci jest aktywna, gdy w polu wyboru **IP Source** zaznaczona jest „Static IP".	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

Grupa „DNS Server“

Tabela 130: Strona WBM „TCP/IP Configuration“ – grupa „DNS Server“

Parametr	Znaczenie
Active	Aktywny serwer DNS; Indeks odzwierciedla kolejność zapytań.
Assigned by DHCP	Serwery DNS przypisane przez DHCP (lub BootP); Jeśli żaden serwer DNS nie został przypisany przez DHCP (lub BootP), wyświetli się komunikat „no DNS Servers assigned by DHCP“.
Assigned by user	Adresy serwerów DNS wprowadzonych przez użytkownika; Jeśli nie został wprowadzony żaden serwer, pojawi się komunikat „no DNS Servers configured".
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.
New Server IP	Wprowadzanie innych adresów serwera DNS; Możliwe są maksymalnie 3 adresy.
[Add]	Dodaj nowy wpis.

7.1.1.3.3 Strona „Ethernet Configuration“

Na stronie „Ethernet Configuration“ znajdują się ustawienia dla sieci ETHERNET.

Grupa „Bridge Configuration“

Tabela 131: Strona WBM „Ethernet Configuration“ – grupa „Bridge Configuration“

Parametr	Znaczenie
Bridge 1 ... <n>	Przyporządkowanie fizycznych portów X1 ... X<n> do logicznego bridge'a, kliknij odpowiedni przycisk opcji. Przyporządkowanie zostaje zaznaczone kolorem. Jeden port może być przyporządkowany do tylko jednej bramy.

Parametr	Znaczenie
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

Grupa „Dummy Interfaces“

Tabela 132: Strona WBM „Ethernet Configuration“ – grupa „Dummy Interfaces“

Parametr	Znaczenie
Name	Nazwa wybranego interfejsu Dummy
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.
Add Dummy Interface	Tworzenie nowego interfejsu Dummy
Name	Wprowadzanie nazwy nowego interfejsu Dummy
[Add]	Dodaj nowy wpis.

Grupa „VLAN Interfaces“

Tabela 133: Strona WBM „Ethernet Configuration“ – grupa „VLAN Interfaces“

Parametr	Znaczenie
Name	Nazwa wybranego interfejsu VLAN
VLAN-ID	VLAN-ID wybranego interfejsu VLAN
Link	Przyporządkowany bridge wybranego interfejsu VLAN
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.
Add VLAN Interface	Tworzenie nowego interfejsu VLAN
Name	Wprowadzanie nazwy nowego interfejsu VLAN
VLAN-ID	Wprowadzanie VLAN-ID; dopuszczalne wartości to 3 … 4094.
Link	Wybór przyporządkowanego bridge'a
[Add]	Dodaj nowy wpis.

Grupa „Port Mirror Settings“

PFC100 G2, PFC200 G2 - 2-Port, PFC300

Tabela 134: Strona WBM „Ethernet Configuration“ – grupa „Port Mirror Settings“

Parametr	Znaczenie	
Enabled	Włączanie/wyłączanie funkcji mirroringu (kopiowania) ruchu sieciowego pomiędzy portami	
	☐	Ruch sieciowy nie jest kopiowany (ustawienie fabryczne).
	☑	Ruch sieciowy jest kopiowany pomiędzy wybranymi portami.
Source	Port źródłowy kopiowanego ruchu sieciowego (X1 … X<n>)	
Destination	Port docelowy kopiowanego ruchu sieciowego (X1 … X<n>)	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

Grupa „Port Mirror“ nie jest dostępna w produktach PFC200 G2 - 4-Port.

Grupa „Strom Control Settings“

PFC100 G2, PFC200 G2 - 2-Port

Tabela 135: Strona WBM „Ethernet Configuration“ – grupa „Storm Control Settings“

Parametr	Znaczenie	
Broadcast Protection	Wartość graniczna dla pakietów typu Broadcast; Wartość domyślna: 1% maksymalnej przepustowości łącza	
Multicast Protection	Określa, czy ograniczenie ruchu dotyczy wyłącznie pakietów Broadcast, czy też łącznie pakietów Broadcast i Multicast.	
	☐	Ograniczenie liczby pakietów dotyczy wyłącznie pakietów Broadcast.
	☑	Ograniczenie liczby pakietów dotyczy łącznie pakietów Broadcast i Multicast.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

PFC200 G2 - 4-Port

Tabela 136: Strona WBM „Ethernet Configuration“ – grupa „Storm Control Settings“

Parametr	Znaczenie
Broadcast Protection	Wartość graniczna dla pakietów typu Broadcast; Wartość domyślna: 1 Mb
Multicast Protection	Wartość graniczna dla pakietów typu Multicast; Wartość domyślna: 1 Mb

PFC300

Tabela 137: Strona WBM „Ethernet Configuration“ – grupa „Storm Control Settings“

Parametr	Znaczenie
Broadcast Protection	Wartość graniczna dla pakietów typu Broadcast; Wartość domyślna: 20 000 pakietów na sekundę
Multicast Protection	Wartość graniczna dla pakietów typu Multicast; Wartość domyślna: 20 000 pakietów na sekundę
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

Grupa „Ethernet Interface Configuration“

PFC100 G2, PFC200 G2 - 2-Port

Tabela 138: Strona WBM „Ethernet Configuration“ – grupy „Ethernet Interface Configuration“

Parametr	Znaczenie	
Interface X<n>	Dla każdego interfejsu zintegrowanego w sterowniku wyświetlany jest osobny obszar.	
Enabled	Aktywacja/dezaktywacja interfejsu	
	☐	Interfejs jest dezaktywowany.
	☑	Interfejs jest aktywny.
MAC Learning	Aktywacja/dezaktywacja funkcji "MAC Learning" dla interfejsu	
	☐	Funkcja „MAC Learning" jest dezaktywowana.
	☑	Funkcja „MAC Learning" jest aktywna.
Broadcast Protection Enabled	Aktywacja/dezaktywacja Broadcast-Protection	
	☐	Broadcast Protection jest dezaktywowany.
	☑	Broadcast Protection jest aktywowany.

Parametr	Znaczenie
Current Speed/Duplex	Aktualna prędkość transmisji i aktualny typ transmisji
Speed/Duplex	Wybór prędkości transmisji oraz i typu transmisji; Lista dostępnych opcji jest generowana w zależności od urządzenia i interfejsu. Przy aktywowanej opcji „Autonegotiation“ tryby łączeniowe negocjowane są automatycznie z urządzeniem przeciwstawnym.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

PFC200 G2 - 4-Port, PFC300

Tabela 139: Strona WBM „Ethernet Configuration“ – grupy „Ethernet Interface Configuration“

Parametr	Znaczenie	
Interface X<n>	Dla każdego interfejsu zintegrowanego w sterowniku wyświetlany jest osobny obszar.	
Enabled	Aktywacja/dezaktywacja interfejsu	
	☐	Interfejs jest dezaktywowany.
	☑	Interfejs jest aktywny.
MAC Learning	Aktywacja/dezaktywacja funkcji "MAC Learning" dla interfejsu	
	☐	Funkcja „MAC Learning" jest dezaktywowana.
	☑	Funkcja „MAC Learning" jest aktywna.
Broadcast Protection Enabled	Aktywacja/dezaktywacja Broadcast-Protection.	
	☐	Broadcast Protection jest dezaktywowany.
	☑	Broadcast Protection jest aktywowany.
Multicast Protection Enabled	Aktywacja/dezaktywacja Multicast Protection.	
	☐	Multicast Protection jest dezaktywowany.
	☑	Multcast Protection jest aktywowany.
Current Speed/Duplex	Aktualna prędkość transmisji i aktualny typ transmisji	
Speed/Duplex	Wybierz prędkość i metodę transmisji; Lista wyboru jest generowana w zależności od urządzenia i interfejsu. Przy aktywowanej opcji „Autonegotiation“ tryby łączeniowe negocjowane są automatycznie z urządzeniem przeciwstawnym.	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

7.1.1.3.4 Strona „Configuration of Host and Domain Name“

Na tej stronie można ustawić nazwy hosta i domeny.

Grupa „Hostname“

Tabela 140: Strona WBM „Configuration of Host and Domain Name“ – grupa „Hostname“

Parametr	Znaczenie
Currently used	Aktualna nazwa hosta
Configured	Wprowadzanie opcjonalnej nazwy hosta
[Clear]	Usuwanie opcjonalnej nazwy hosta i przywracanie wartości domyślnej
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

Gdy nazwa hosta jest dostarczana przez odpowiedź DHCP, staje się aktywna w systemie. W przypadku kilku interfejsów sieciowych korzystających z DHCP zawsze obowiązuje ostatnio otrzymana nazwa hosta.
Jeśli ma obowiązywać tylko nazwa hosta skonfigurowana tutaj, należy tak dostosować konfigurację serwerów DHCP, aby w odpowiedzi DHCP nie były wysyłane nazwy hosta.

Grupa „Domain Name“

Tabela 141: Strona WBM „Configuration of Host and Domain Name“ – grupa „Domain Name“

Parametr	Znaczenie
Currently used	Aktualnie używana nazwa domeny
Configured	Wprowadzanie opcjonalnej nazwy domeny
[Clear]	Usuwanie opcjonalnej nazwy domeny
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

Gdy nazwa domeny jest dostarczana przez odpowiedź DHCP, staje się aktywna w systemie. W przypadku kilku interfejsów sieciowych korzystających z DHCP zawsze obowiązuje ostatnio otrzymana nazwa domeny.
Jeśli ma obowiązywać tylko nazwa domeny skonfigurowana tutaj, należy tak dostosować konfigurację serwerów DHCP, aby w odpowiedzi DHCP nie były wysyłane nazwy domeny.

7.1.1.3.5 Strona „Routing“

Na stronie „Routing“ znajdują się ustawienia i informacje dotyczące rutingu między interfejsami sieciowymi.

Grupa „IP Forwarding through multiple interfaces“

Tabela 142: Strona WBM „Routing“ – grupa „IP Forwarding through multiple interfaces“

Parametr	Znaczenie	
Enabled	Umożliwia przekazywanie pakietów danych IP pomiędzy różnymi interfejsami sieciowymi	
	☐	Ustawienia w sekcji „Static Routes” są stosowane również wtedy, gdy pakiety IP docierające do sterownika przez jeden interfejs sieciowy nie mogą być przekazywane dalej przez inny interfejs.
	☑	Pakiety IP mogą być przekazywane między interfejsami. Mogą być wymagane dodatkowe ustawienia.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

Grupa „Custom Routes“

Dla każdej skonfigurowanej trasy statycznej wyświetlany jest osobny obszar. Gdy nie zostały wprowadzone statyczne trasy, wyświetlana jest informacja „(no custom routes)“.

Tabela 143: Strona WBM „Routing“ – grupa „Custom Routes“

Parametr	Znaczenie	
Enabled	Zastosowanie wybranej trasy	
	☐	Trasa nie jest zastosowana.
	☑	Trasa jest zastosowana.
Destination Address	Adres docelowy urządzenia	

Parametr	Znaczenie	
	Default	Dostępni są dowolni uczestnicy komunikacji sieciowej.
	Network address	Dostępne jest tylko określone urządzenie lub urządzenie z danej puli adresów.
Destination Mask	Maska podsieci urządzenia Jeśli Destination Address jest zdefiniowany jako „default“, należy tu wpisać wartość „0.0.0.0“.	
Gateway Address	Adres bramy Jeśli pole „Interface“ jest puste, należy tu wpisać wartości. Jeśli w polu „Interface“ wpisana jest wartość, wypełnienie tego pola jest opcjonalne.	
Gateway Metric	Metryka trasy 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. Najmniejsza wartość wynosi 0. Największa wartość to $2^{32} - 1 = 4.294.967.295$.	
Interfejs	Interfejs, przez który prowadzone są pakiety kierowane do Destination Address. Można użyć bridge'ów (br0 … br3), modemu (wwan0) lub nazwy interfejsu VPN. Jeśli pole „Gateway Address" jest puste, należy je wypełnić. Jeśli w polu „Gateway Address“ wpisana jest wartość, wypełnienie tego pola jest opcjonalne.	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.	
[Add]	Dodaj nowy wpis.	

Grupa „Dynamic Routes (assigned by DHCP)“

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 144: Strona WBM „Routing“ – grupa „IP-Masquerading“

Parametr	Znaczenie	
Enabled	Stosowanie IP-Masquerading	
	☐	IP-Masquerading nie jest zastosowany.
	☑	IP-Masquerading jest zastosowany.
Interfejs	Wybierz jedną z podanych nazw dla interfejsu sieciowego Przy wybraniu opcji „other" możliwa jest dowolna nazwa interfejsu sieciowego.	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.	
[Add]	Dodaj nowy wpis.	

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 145: Strona WBM „Routing“ – grupa „Port Forwarding“

Parametr	Znaczenie	
Enabled	Użyj przekierowania portów	
	☐	Port Forwarding nie jest zastosowany.
	☑	Port Forwarding jest zastosowany.
Interfejs	Wybierz jedną z podanych nazw dla interfejsu sieciowego Przy wybraniu opcji „other" możliwa jest dowolna nazwa interfejsu sieciowego.	
Port	Wybór portu, po którym przesyłane pakiety danych mają dotrzeć do produktu.	
Protocol	Wybierz protokół, który ma być uwzględniony dla Port-Forwarding; Do wyboru są TCP, UDP lub oba protokoły.	
Destination Address	Wybierz adres sieciowy urządzenia docelowego Ten adres zastępuje pierwotny adres docelowy pakietu danych.	
Destination Port	Wybierz numer portu urządzenia docelowego Wartość ta zastępuje pierwotny port docelowy pakietu danych.	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.	
[Add]	Dodaj nowy wpis.	

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.

7.1.1.3.6 Strona „Spanning Tree Protocol“

Na stronie „Spanning Tree Protocol" znajdują się ustawienia dla STP/RSTP.

Grupa „Status“

W grupie „Status“ wyświetlane są aktualne wartości aktywnej konfiguracji STP/RSTP.

Tabela 146: Strona WBM „Spanning Tree Protocol" – grupa „Status"

Parametr	Znaczenie	
Current Status	Aktualny status	
	☐	STP/RSTP nie jest aktywny.
	☑	STP/RSTP jest aktywny.
Current Bridge	Wybrany bridge	
Current Mode	Aktualny protokół	
	STP	Spanning Tree Protocol jest aktywny.
	RSTP	Rapid Spanning Tree Protocol jest aktywny.
Current Priority	Aktualny priorytet bridge'a	
Current Hello Time (sec)	Aktualny czas „Hello" w sekundach	

Parametr	Znaczenie	
Current Forward Delay (sec)	Aktualny czas „Forward Delay" w sekundach	
Current Max Age (sec)	Aktualny czas „Max Age" w sekundach	
Current Max Hops	Aktualny Max Hops	
Current Path Cost	Aktualny Path Cost	
Port X[n]	Dla każdego portu X[n] wybranego bridge'a wyświetlany jest osobny obszar. Ustawienia portu wyświetlane są dopiero po pomyślnym włączeniu STP/RSTP.	
Current Bpdu Filter	Aktualny status „Bpdu Filter"	
	☐	Filtr Bpdu nie jest aktywny.
	☑	Filtr Bpdu jest aktywny.
Current Bpdu Guard	Aktualny status „Bpdu Guard"	
	☐	Bpdu-Guard nie jest aktywny.
	☑	Bpdu-Guard jest aktywny.
Current Edge Port	Aktualny status portu	
	☐	Port nie jest portem Edge.
	☑	Port jest portem Edge.
Current Root Guard	Aktualny status „Root Guard"	
	☐	Root-Guard nie jest aktywny.
	☑	Root-Guard jest aktywny.
Current Path Cost	Aktualny koszt ścieżki	
Current Priority	Aktualny priorytet	
Current Role	Aktualna rola portu	
	Designated	Port wybrany w każdym segmencie sieci LAN, który zapewnia najniższe koszty ścieżki głównej. Im wyższa prędkość połączenia, tym niższa cena.
	Disabled	Port jest dezaktywowany.
Current Status	Aktualny status portu	
	Forwarding	Port może wysyłać i odbierać dane, uczyć się adresów MAC i przesyłać dane do miejsca docelowego.
	Discarding	Port nie przekazuje danych do innych switchy w sieci i nie aktualizuje tabel adresów MAC.

Grupa „Parameter Settings"

W grupie „Parameter Settings" można zmienić ustawienia dla konfiguracji STP/RSTP.

Tabela 147: Strona WBM „Spanning Tree Protocol" – grupa „Parameter Settings"

Parametr	Znaczenie	
Enabled	Aktywacja/dezaktywacja Spanning Tree Protocol	
	☐	Spanning Tree Protocol nie jest aktywny.
	☑	Spanning Tree Protocol jest aktywny.
Bridge	Wybierz bridge.	
Mode	Wybierz protokół;	
	STP	Spanning Tree Protocol
	RSTP	Rapid Spanning Tree Protocol

Parametr	Znaczenie	
Priority	Ustawianie priorytetu bridge'a; dopuszczalne wartości: 1 … 15	
Hello Time	Ustawianie Hello Time; dopuszczalne wartości: 1 … 19	
Forward Delay	Ustawienie Forward Delay; dopuszczalne wartości: 4 … 30	
Max Age	Ustawienie maks. wieku; dopuszczalne wartości: 6 … 40	
Max Hops	Ustawienie maksymalnej liczby przeskoków; dopuszczalne wartości: 6 … 40	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	
Port X[n]	Dla każdego portu X[n] wyświetlany jest osobny obszar. Ustawienia portu są dostępne dopiero po pomyślnym włączeniu STP/RSTP.	
Filtr Bpdu	Aktywacja/dezaktywacja filtra Bpdu	
	☐	Filtr Bpdu nie jest aktywny.
	☑	Filtr Bpdu jest aktywny.
Bpdu Guard	Aktywacja/dezaktywacja Bpdu Guard	
	☐	Bpdu Guard nie jest aktywny.
	☑	Bpdu Guard jest aktywny.
Port Edge	Aktywacja/dezaktywacja portu jako portu Edge	
	☐	Port nie jest portem Edge.
	☑	Port to Edge.
Funkcja Root Guard	Aktywacja/dezaktywacja funkcji Root Guard	
	☐	Funkcja Root Guard nie jest aktywna.
	☑	Funkcja Root Guard jest aktywna.
Path Cost	Ustawianie Path Cost; dopuszczalne wartości: 0 … 65535	
Priority	Ustawienie priorytetu; Dopuszczalne wartości: 0 … 15, Default = 8	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

7.1.1.3.7 Strona „Clock Settings“

Na tej stronie można wprowadzić ustawienia daty i godziny.

Grupa „Timezone and Format“

Tabela 148: Strona WBM „Clock“ – grupa „Timezone and Format“

Parametr	Znaczenie	
Timezone	Wybierz strefę czasową, ustawienia 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

Parametr	Znaczenie	
	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	Powyżej niemożliwy wybór strefy czasowej: podanie nazwy strefy czasowej, kraju i miasta Ustalenie prawidłowej nazwy strefy czasowej: **http://www.timeandda-te.com/time/map/**	
Time Format	Format czasowy: 12h / 24h	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

Grupa „UTC Time and Date“

Tabela 149: Strona WMB „Clock“ – grupa „UTC Time and Date“

Parametr	Znaczenie
UTC Date	Data
UTC Time	Czas GMT
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

Grupa „Local Time and Date“

Tabela 150: Strona WMB „Clock“ – grupa „Local Time and Date“

Parametr	Znaczenie
Local Date	Data lokalna
Local Time	Zegar lokalny
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

7.1.1.3.8 Strona „Configuration of Serial Interface“

Na tej stronie dostępne są ustawienia dotyczące interfejsu komunikacyjnego.

7.1.1.3.8.1 PFC100/PFC200

Grupa „Current Serial Interface Configuration"

W tej grupie wyświetlana jest aplikacja, do której aktualnie przypisany jest interfejs szeregowy oraz aktualny tryb interfejsu.

Tabela 151: Strona WBM „Configuration of Serial Interface" – grupa „Current Serial Interface Configuration"

Parametr	Znaczenie	
Assigned to	Przypisanie interfejsu komunikacyjnego	
	Unassigned (usage by Applications, Libraries, PLC Runtime)	Interfejs komunikacyjny nie jest przypisany do żadnej aplikacji. Dzięki temu np. program CODESYS może uzyskać do niego dostęp za pomocą bloków funkcyjnych.
	Linux Console	Interfejs komunikacyjny jest przypisany do konsoli Linux.
Mode	Tryb interfejsu komunikacyjnego	
	RS232	Interfejs komunikacyjny pracuje w trybie RS-232.

Parametr	Znaczenie	
	RS485	Interfejs komunikacyjny pracuje w trybie RS-485.

UWAGA

Szkody materialne wynikające z przełączania właściciela lub trybu!

Podczas przełączania podłączone urządzenia RS-232/RS-485 mogą zostać uszkodzone.

- Przed przełączeniem należy te urządzenia usunąć!

Grupa „Assign Owner of Serial Interface“

Tutaj można wybrać aplikację, do której po następnym ponownym uruchomieniu sterownika zostanie przypisany interfejs komunikacyjny.

Tabela 152: Strona WBM „Configuration of Serial Interface“ – grupa „Assign Mode of Serial Interface“

Parametr	Znaczenie
RS232	Interfejs komunikacyjny pracuje w trybie RS-232.
RS485	Interfejs komunikacyjny pracuje w trybie RS-485.
[Submit]	Akceptacja zmiany; zmiana zostanie zrealizowana dopiero po następnym restarcie.

Grupa „Assign Mode of Serial Interface“

Tu można wybrać tryb pracy złącza komunikacyjnego.

Tabela 153: Strona WBM „Configuration of Serial Interface“ – grupa „Assign Owner of Serial Interface“

Parametr	Znaczenie
Unassigned (usage by Applications, Libraries, PLC Runtime)	Interfejs komunikacyjny nie jest przypisany do żadnej aplikacji.
Linux Console	Interfejs komunikacyjny jest przypisany do konsoli Linux.
[Submit]	Akceptacja zmiany; zmiana zostanie zrealizowana dopiero po następnym restarcie.

7.1.1.3.8.2 PFC300

Grupa „Current Serial Interface Configuration"

W tej grupie wyświetlany jest aktualny tryb interfejsu.

Tabela 154: Strona WBM „Configuration of Serial Interface" – grupa „Current Serial Interface Configuration"

Parametr	Znaczenie	
Mode	Tryb interfejsu komunikacyjnego	
	RS485	Interfejs komunikacyjny pracuje w trybie RS-485.

Grupa „Bus Termination"

Tutaj można włączyć lub wyłączyć terminację magistrali dla interfejsu komunikacyjnego.

Tabela 155: Strona WBM „Configuration of Serial Interface" – grupa "Bus Termination"

Parametr	Znaczenie	
Termination enabled	Aktywacja/dezaktywacja terminacji	
	☐	Terminacja dezaktywowana
	☑	Terminacja magistrali jest aktywowana.

Parametr	Znaczenie
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

Grupa „Bias Network"

Tutaj można skonfigurować sieć Bias dla interfejsu komunikacyjnego.

Tabela 156: Strona WBM „Configuration of Serial Interface" – grupa "Bias Network"

Parametr	Znaczenie
Off	Brak aktywnej magistrali
Niski	Aktywna terminacja 1 (640Ohm)
Wysoki	Aktywna terminacja 2 (1210Ohm)
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

7.1.1.3.9 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 157: Strona WBM „Configuration of Service Interface“ – grupa „ Assign Owner of Service Interface“

Parametr	Znaczenie
WAGO Service Communication	Złącze serwisowe wykorzystywane jest do komunikacji serwisowej WAGO lub komunikacji z systemem runtime.
Linux Console	Złącze serwisowe jest przypisane do konsoli Linux.
Unassigned (usage by Applications, Libraries, PLC Runtime)	Złącze serwisowe nie jest przypisane do żadnej aplikacji. Dzięki temu np. program CODESYS może uzyskać do niego dostęp za pomocą bloków funkcyjnych.
[Submit]	Akceptacja zmiany; zmiana zostanie zrealizowana dopiero po następnym restarcie.

7.1.1.3.10 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 158: Strona WBM „Create bootable Image“ – grupa „Create bootable image from boot device“

Parametr	Znaczenie
Boot Device	Wyświetla nośnik pamięci, z którego przeprowadzony był rozruch.
Destination	Wybór miejsca docelowego dla tworzonego obrazu; W zależności od nośnika, z którego uruchomiono system, po zakończeniu rozruchu dostępne są następujące miejsca docelowe dla tworzonego obrazu rozruchowego (bootable image):

Parametr	Znaczenie	
	System rozruchowy:	Partycja docelowa dla „bootable image“
	Karta pamięci	Internal Flash
	Pamięć wewnętrzna	Memory Card
[Start Copy]	Rozpocznij proces kopiowania ▪ Po pozytywnym wyniku testu proces rozpoczyna się od razu. ▪ Jeśli zostały wykryte błędy, wyświetlany jest odpowiedni komunikat i proces nie jest realizowany. ▪ Jeśli istnieją ostrzeżenia, są one jeszcze raz wyświetlane i należy potwierdzić, że mimo to chcesz kontynuować proces.	

- 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!

7.1.1.3.11 Strona „Firmware Backup“

Na stronie „Firmware Backup“ znajdują się ustawienia dotyczące zabezpieczenia danych sterownika.

Grupa „Firmware Backup“

Tabela 159: Strona WBM „Firmware Backup“ – grupa „Firmware Backup“

Parametr	Znaczenie	
Boot Device	Nośnik pamięci, z którego przeprowadzony był rozruch.	
Destination	Miejsce zapisu kopii zapasowej	
	Memory Card	Dane zostają zapisane na karcie pamięci. Ta możliwość wyboru widoczna jest tylko wtedy, gdy wetknięta jest karta pamięci i nie był z niej przeprowadzony rozruch.
	Pamięć USB	Dane są zapisywane na pendrivie. Ta opcja jest dostępna tylko w produktach z portem USB. Opcja jest aktywna tylko wtedy, gdy podłączony jest nośnik USB i system nie został z tego nośnika uruchomiony.
	Network	Dane zapisywane są w systemie plików i udostępniane na PC do pobrania.
PLC Runtime Project	Zapisywanie projektu runtime PLC, projektu bootowalnego i ustawień CODESYS	
	☐	Bieżący projekt PLC zostaje niezabezpieczony
	☑	Bieżący projekt PLC zostaje zabezpieczony
Settings	Zabezpieczenie ustawień urządzenia	
	☐	Ustawienia urządzenia nie są zabezpieczone.
	☑	Ustawienia urządzenia zostają zabezpieczone.
System	Zapisywanie systemu operacyjnego urządzenia i głównego systemu plików	
	☐	System operacyjny urządzenia i główny system plików nie są zabezpieczone.

Parametr	Znaczenie	
	☑	System operacyjny urządzenia i główny system plików są zabezpieczone.
Encryption	Tworzenie kopii zapasowej danych w postaci zaszyfrowanej	
	☐	Dane są zapisywane bez szyfrowania.
	☑	Dane są zapisywane w postaci zaszyfrowanej
Encryption passphrase	Hasło szyfrowania Pole edycji widoczne jest tylko wtedy, gdy pole wyboru**Encryption** jest zaznaczone.	
Confirm passphrase	Hasło szyfrowania do kontroli Pole edycji widoczne jest tylko wtedy, gdy pole wyboru **Encryption** jest zaznaczone.	
[Create Backup]	Rozpocznij proces backupu	

ⓘ Wskazówka

Należy uwzględnić wersję firmware'u!

Przywracanie systemu operacyjnego (opcja „System") jest dozwolone i możliwe tylko wtedy, gdy wersje oprogramowania firmware w momencie tworzenia kopii zapasowej i przywracania są identyczne.
W razie potrzeby należy zrezygnować z przywracania systemu operacyjnego lub wcześniej dostosować wersję firmware do wersji obowiązującej 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 backupu z karty pamięci!

Z karty pamięci nie jest możliwy backup na wewnętrzną pamięć flash.

ⓘ Wskazówka

Należy uwzględnić czas tworzenia kopii zapasowych

Tworzenie plików backupu trwa kilka minut. Aby skrócić ten czas, należy przed rozpoczęciem backupu zatrzymać program CODESYS.

7.1.1.3.12 Strona „Firmware Restore"

Na stronie „Firmware Restore" znajdują się ustawienia do odświeżenia firmware'u.

Grupa „Firmware Restore“

Tabela 160: Strona WBM „Firmware Restore“ – grupa „Firmware Restore“

Parametr	Znaczenie	
Source	Tu wybiera się źródło danych do odświeżenia.	
	Memory Card	Dane zostają odczytane z karty pamięci. Ta możliwość wyboru aktywna jest tylko wtedy, gdy wetknięta jest karta pamięci i nie był z niej przeprowadzony rozruch.
	Pamięć USB	Dane są odczytywane z pamięci USB. Ta opcja jest dostępna tylko w produktach z portem USB. Opcja jest aktywna tylko wtedy, gdy podłączony jest nośnik USB i system nie został z tego nośnika uruchomiony.
	Network	Dane do odświeżenia pobrane zostają z PC.
Boot Device	Nośnik pamięci, z którego przeprowadzony był rozruch.	
PLC Runtime Project	Nazwa pliku kopii zapasowej projektu CODESYS; Pole edycji aktywne jest tylko wtedy, gdy jako źródło danych wybrano sieć.	
Settings	Nazwa pliku kopii zapasowej ustawień; Pole edycji aktywne jest tylko wtedy, gdy jako źródło danych wybrano sieć.	
System	Nazwa pliku kopii zapasowej danych systemowych i głównego systemu plików (root); Pole edycji aktywne jest tylko wtedy, gdy jako źródło danych wybrano sieć.	
Decryption	Szyfrowanie danych	
	☐	Dane zostały zaszyfrowane.
	☑	Dane zostały zapisane bez szyfrowania.
Decryption passphrase	Hasło deszyfrujące; Pole edycji jest widoczne tylko wtedy, gdy zaznaczone jest pole **Decryption**.	
[Restore]	Rozpocznij proces przywracania	

ⓘ Wskazówka

Należy uwzględnić wersję firmware'u!

Przywracanie systemu operacyjnego (opcja „System") jest dozwolone i możliwe tylko wtedy, gdy wersje oprogramowania firmware w momencie tworzenia kopii zapasowej i przywracania są identyczne.
W razie potrzeby należy zrezygnować z przywracania systemu operacyjnego lub wcześniej dostosować wersję firmware do wersji obowiązującej w momencie tworzenia kopii zapasowej.

ⓘ 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

Odświeżenie możliwe tylko z wewnętrznej pamięci!

Jeśli produkt był uruchamiany z karty pamięci, nie jest możliwe odświeżenie firmware'u.

ⓘ Wskazówka

Reset przez odświeżenie

Reset można realizować przez odświeżenie systemu, ustawień lub CODESYS!

ⓘ Wskazówka

Utrata połączenia przez odświeżenie!

Jeśli w wyniku odświeżenia zmienią się parametry połączenia ETHERNET, WBM może nie być w stanie nawiązać połączenia z produktem.
WBM należy ponownie otworzyć za pomocą odpowiedniego adresu IP produktu w wierszu adresu.

ⓘ Wskazówka

Uwzględnić czas resetu

Proces restore wymaga ok. 2 ... 3 minut.
Po zakończeniu procesu restore sterownik uruchamiany jest ponownie i jest znowu gotowy do pracy.

7.1.1.3.13 Strona „Active System“

Na tej stronie możliwe są ustawienia do wyboru partycji, z której ma być uruchamiany system.

Grupa „Boot Device“

Tabela 161: Strona WBM „Active System“ – grupa „Boot Device"

Parametr	Znaczenie
Booted from	Nośnik pamięci, z którego przeprowadzony był rozruch

Grupa „System <n> (Internal Flash)"

Tabela 162: Strona WBM „Active System“ – grupa „System <n> (Internal Flash)“

Parametr	Znaczenie	
Active	Aktywność systemu	
Configured	Aktywność systemu po następnym procesie Reboot	
State	Status systemu	
	good	Obowiązujący system
	bad	Nieaktualny system, używany tylko do testów
[Activate]	Uruchom system przy następnym procesie Reboot.	

ⓘ Wskazówka

Przygotować system bootowalny!

W systemie bootowalnym musi istnieć backup firmware'u!

7.1.1.3.14 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 znalezionego nośnika pamięci wyświetlany jest obszar z informacjami o tym nośniku.

Tabela 163: Strona WBM „Mass Storage“ – grupa „Devices"

Parametr	Znaczenie
<Device>	Nośnik pamięci
Boot Device	Tu wyświetlana jest informacja, czy z tego nośnika pamięci przeprowadzony był rozruch.
Volume name	Nazwa nośnika pamięci

Grupa „Create new Filesystem on Memory Card“

ⓘ Wskazówka

Dane zostają usunięte!

Przy formatowaniu dane zapisane na dysku pamięci zostają usunięte!

Tabela 164: Strona WBM „Mass Storage“ – grupa "Create new Filesystem on Memory Card“

Parametr	Znaczenie	
IP Source	Wybieranie formatu, 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	Wprowadzanie nazwy, którą ma otrzymać nośnik pamięci przy formatowaniu	
[Start]	Formatuj nośnik pamięci	

7.1.1.3.15 Strona „Software Uploads“

Na stronie „Software Uploads“ można zainstalować na produkcie pakiety oprogramowania pobrane z komputera.

Tabela 165: Strona WBM „Software Uploads“ – grupa „Upload new Software“

Parametr	Znaczenie
Software File	Nazwa wybranego pakietu oprogramowania, dopóki nie zostanie on przesłany do produktu; Jeśli pakiet nie został jeszcze wybrany, pojawia się tekst "Choose ipk file ...". W tym przypadku należy kliknąć pole edycji i wybrać na komputerze plik z pakietem.

Parametr	Znaczenie
Force install	
[Install]	Zainstaluj wybrany pakiet; Po zakończeniu instalacji plik z pakietem oprogramowania zostanie usunięty z produktu. Jeśli nie jest to możliwe na skutek błędu w trakcie przetwarzania, usunięcie nastąpi najpóźniej przy kolejnym restarcie produktu.

7.1.1.3.16 Strona „Configuration of Network Services“

Na tej stronie można wprowadzać ustawienia dla różnych usług.

ⓘ Wskazówka

Zamknąć nieużywane porty i usługi!

Przez otwarte porty i usługi osoby nieuprawnione mogą uzyskać dostęp do systemu automatyki.

1. 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 i port 11740 dla CODESYS V3).
2. Porty i usługi dobrze jest otwierać tylko na czas uruchamiania lub konfiguracji.

Grupa „FTP“

Tabela 166: Strona WBM „Configuration of Network Services“ – grupa „FTP“

Parametr	Znaczenie	
Service active	Aktywacja/dezaktywacja serwera FTP	
	☐	Usługa FTP jest nieaktywna; Ustawienia fabryczne
	☑	Usługa FTP jest aktywna.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

Grupa „FTPES (explicit FTPS)“

Tabela 167: Strona WBM „Configuration of Network Services“ – grupa „FTPES (explicit FTPS)“

Parametr	Znaczenie	
Service active	Aktywacja/dezaktywacja usługi FTPES (explicit FTPS);	
	☐	Usługa FTPES jest nieaktywna; Ustawienia fabryczne
	☑	Usługa FTPES jest aktywna.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

Grupa „HTTP“

Tabela 168: Strona WBM „Configuration of Network Services“ – grupa „HTTP“

Parametr	Znaczenie	
Service active	Aktywacja/dezaktywacja serwisu HTTP	
	☐	Serwis HTTP jest dezaktywowany; Ustawienia fabryczne
	☑	Serwis HTTP jest aktywowany.

Parametr	Znaczenie
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

Wskazówka

Utrata połączeń przy dezaktywacji

Przy dezaktywacji serwisu połączenie z produktem może zostać przerwane.

- Należy ponownie otworzyć stronę.

Grupa „HTTPS“

Tabela 169: Strona WBM „Configuration of Network Services“ – grupa „HTTPS“

Parametr	Znaczenie	
Service active	Status serwisu HTTPS	
	☐	Usługa HTTPS jest nieaktywna.
	☑	Serwis HTTPS jest aktywowany.

Grupa „I/O-*CHECK*“

Tabela 170: Strona WBM „Configuration of Network Services“ – grupa „I/O-CHECK“

Parametr	Znaczenie	
Service active	Aktywowanie/dezaktywowanie serwisu WAGO I/O-*CHECK*	
	☐	Serwis WAGO I/O-*CHECK* jest dezaktywowany; nastawa fabryczna
	☑	Serwis WAGO I/O-*CHECK* jest aktywowany.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

7.1.1.3.17 Strona „Configuration of NTP Client“

Na stronie „Configuration of NTP Client“ znajdują się ustawienia dla usługi NTP.

Grupa „NTP Client Configuration“

Tabela 171: Strona WBM „Configuration of NTP Client“ – grupa „NTP Client Configuration“

Parametr	Znaczenie	
Service enabled	Automatyczna aktualizacja czasu; aktywacja/dezaktywacja	
	☐	Aktualizacja czasu jest nieaktywna; ustawienia fabryczne
	☑	Aktualizacja czasu jest aktywna.
Update Interval (sec)	Wprowadzenie interwału odświeżania serwera czasowego.	
Time Server <n>	Wprowadzenie adresów IP serwerów czasu; możliwe są maksymalnie 4 serwery czasu.	
Additionally assigned (DHCP)	Serwer NTP przydzielony przez DHCP; Jeśli nie został przydzielony serwer czasu, wyświetlana jest informacja „No additional servers assigned".	
[update time]	Aktualizacja godziny	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

7.1.1.3.18 Strona „PLC Runtime Services“

Na stronie „PLC Runtime Services“ znajdują się ustawienia dla różnego typu usług systemu runtime.

Grupa „CODESYS V3“

Tabela 172: Strona WBM „PLC Runtime Services“ – grupa „CODESYS V3“

Parametr	Znaczenie	
CODESYS V3 State	Status systemu runtime	
	disabled	System runtime jest dezaktywowany.
	enabled	System runtime jest aktywowany.
Webserver Enabled	Aktywacja i dezaktywacja serwera WWW dla wizualizacji WWW	
	☐	Serwer WWW jest nieaktywny.
	☑	Serwer WWW jest aktywny.
Separated WebVisu Ports (8080/8081)	Ustawianie portów CODESYS WebVisu dla HTTP/HTTPS	
	☐	CODESYS WebVisu jest udostępniany na portach 80/443 (standard jak WBM).
	☑	CODESYS WebVisu jest dostępny na portach 8080/8081.
Port Authentication Enabled	Aktywacja/dezaktywacja logowania w celu połączenia z urządzeniem	
	☐	Logowanie nie jest wymagane dla połączenia.
	☑	Połączenie wymaga logowania. Domyślną nazwą użytkownika jest admin, a hasłem jest hasło podane w „General Configuration".
Webserver Port Authentication Enabled	Aktywacja/dezaktywacja logowania w celu wywołania wizualizacji internetowej aplikacji Codesys	
	☐	Logowanie nie jest wymagane do wywołania wizualizacji internetowej.
	☑	Do wywołania wizualizacji internetowej wymagane jest zalogowanie. Standardowa nazwa użytkownika to admin, a hasłem jest hasło podane w „General Configuration".
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

7.1.1.3.19 Strona „SSH Server Settings“

Na stronie „SSH Server Settings“ znajdują się ustawienia dla usługi SSH.

Grupa „SSH Server“

Tabela 173: Strona WBM „SSH Server Settings“ – grupa „SSH Server“

Parametr	Znaczenie	
Service active	Aktywacja/dezaktywacja usługi serwera SSH	
	☐	Usługa serwera SSH jest nieaktywna.
	☑	Usługa serwera SSH jest aktywna.
Port Number	Wprowadzanie numeru portu.	
Allow root login	Blokada lub zezwolenie na dostęp do katalogu głównego	
Allow password login	Aktywowanie/dezaktywowanie pytania o hasło	

Parametr	Znaczenie
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

7.1.1.3.20 Strona „DHCP Server Configuration“

Na stronie „DHCP Server Configuration“ znajdują się ustawienia dla usługi DHCP.

Dla każdego skonfigurowanego bridge'a wyświetlana jest osobna grupa.

Grupa „DHCP Server Configuration Bridge <n>“

Tabela 174: Strona WBM „DHCP Server Configuration“ – grupa „DHCP Configuration Bridge <n>“

Parametr	Znaczenie	
Service active	Aktywacja/dezaktywacja usługi serwera DHCP dla bridge <n>	
	☐	Usługa serwera DHCP dla bridge <n> nie jest aktywowana.
	☑	Usługa serwera DHCP dla bridge <n> jest aktywowana.
Start IP for Range	Wprowadzanie wartości początkowej dostępnego zakresu adresów IP.	
End IP for Range	Wprowadzanie wartości końcowej dostępnego zakresu adresów IP.	
Lease time (min)	Wprowadzanie czasu dzierżawy w minutach. Ustawienia fabryczne: 120 minut	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	
Static Hosts	Statyczne przypisania identyfikatorów MAC-ID lub nazw hostów do adresów IP; Jeśli brak przypisania, wyświetlany jest komunikat "No static hosts configured".	
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.	
Add Static Host	Dodawanie statycznych przyporządkowań adresów MAC lub nazw hosta do adresów IP; możliwe jest maks. 15 przyporządkowań.	
MAC Address or Hostname	Wpisywanie adresu MAC lub nazwy hosta; np. "01:02:03:04:05:06=192.168.1.20"lub "hostname=192.168.1.20".	
IP Address	Wprowadzanie adresu IP	
[Add]	Dodaj nowy wpis.	

7.1.1.3.21 Strona „Configuration of DNS Server“

Na tej stronie możliwe są ustawienia usługi DNS.

Grupa „DNS Server“

Tabela 175: Strona WBM „Configuration of DNS Server“ – grupa „DNS Server“

Parametr	Znaczenie	
Service active	Aktywacja/dezaktywacja usługi serwera DNS	
	☐	Usługa serwera DNS jest nieaktywna.
	☑	Usługa serwera DNS jest aktywowana.
Mode	Ustawianie trybu pracy;	
	Proxy	Zapytania buforowane są w celu optymalizacji przepustowości komunikacji.
	Relay	Wszystkie zapytania są przesyłane bezpośrednio dalej.

Parametr	Znaczenie
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.
Static Hosts	Statyczne przyporządkowanie nazw hostów do adresów IP; Jeśli nie ma przyporządkowania, wyświetlana jest informacja „No static hosts configured".
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.
Add Static Host	Statyczne przyporządkowywanie adresów IP do nazw hosta; możliwe jest maks. 10 przyporządkowań.
IP Address	Wprowadzanie adresu IP; np. "192.168.1.20:hostname"
Hostname	Wprowadzanie nazwy hosta.
[Add]	Dodaj nowy wpis.

7.1.1.3.22 Strona „Status overview"

Na stronie „Status overview" znajdują się informacje dotyczące dostępu do chmury.

Grupa „Connection <n>"

Dla każdego dostępu do chmury wyświetlana jest osobna grupa.

Tabela 176: Strona WBM „Overview" – grupa „Connection <n>"

Parametr	Znaczenie
Operation	Status aplikacji z połączeniem z chmurą
Data from PLC Runtime	Liczba kolekcji danych (Data-Collections), które zostały zarejestrowane przez aplikację IEC w celu przesyłania danych do chmury.
Cloud Connection	Status połączenia z chmurą
Heartbeat	Aktualnie skonfigurowany interwał heartbeat w sekundach
Telemetry data transmission	Status transmisji danych
Cache fill level (QoS 1 and 2)	Stan zapełnienia pamięci dla wiadomości wychodzących, wyrażony w procentach.

7.1.1.3.23 Strona „Configuration of Connection <n>"

Na tej stronie można wprowadzać 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 przedstawione są w osobnej tabeli.

Tabela 177: Strona WBM „Configuration of Connection <n>" – grupa „Configuration"

Parametr	Znaczenie
Enabled	Aktywacja/dezaktywacja funkcji Cloud Connectivity
Cloud platform	Platforma chmury
Hostname	Nazwa hosta lub adres IP dla wybranej platformy chmury
ID Scope	Punkt końcowy dla usługi Azure Device Provisioning Service (DPS).
Registration ID	ID rejestru dla usługi Azure Device Provisioning Service (DPS).

Parametr	Znaczenie
Port number	Numer portu, do którego ma być utworzone połączenie. Wartości typowe: ▪ 8883 dla połączeń szyfrowanych ▪ 1883 dla połączeń nieszyfrowanych
Device ID	Device ID dla wybranej platformy chmury
Client ID	Client ID dla wybranej platformy chmury
Authentication	Metoda uwierzytelniania, np. „Shared Key Acces", „X.509 Certificate"
Activation Key	Kod aktywacji dla wybranej platformy chmury
Clean Session	Aktywacja Clean-Session przy połączeniu z usługą chmury Clean Session jest aktywna: informacje i wiadomości dotyczące tego połączenia z usługą chmury nie są zapisywane.
TLS	Aktywacja/dezaktywacja szyfrowania TLS dla połączenia z platformą chmury Amazon Web Services (AWS) stosuje TLS.
CA file	Ścieżka do pliku zakodowanego w formacie PEM, który zawiera zaufany certyfikat CA używany do nawiązania szyfrowanego połączenia. Wartość standardowa: certyfikat CA /etc/ssl/certs/ca-certificates.crt
User	Nazwa użytkownika
Password	Hasło
Certification file	Tu wpisuje się ścieżkę do pliku zakodowanego w formacie PEM, wykorzystywanego do uwierzytelnienia usługi chmury.
Key file	Ścieżka do pliku zakodowanego w formacie PEM, który zawiera prywatny kod do uwierzytelnienia usługi chmury.
Use websockets	Aktywacja/dezaktywacja połączenia z platformą chmury za pomocą protokołu Websocket przez port 443 Jeśli dezaktywowane: połączenie z platformą chmury za pomocą protokołu MQTT przez port 8883
HTTP Proxy Host	Nazwa hosta lub adres IP serwera proxy
HTTP Proxy Port	Numer portu serwera proxy
HTTP Proxy User	Nazwa użytkownika proxy
HTTP Proxy Password	Hasło użytkownika proxy
Use compression	Aktywacja/dezaktywacja kompresji danych za pomocą kompresji GZIP
Data Protocol	Protokół danych
Cache mode	Lokalizacja pamięci podręcznej dla telegramów danych Pole wyboru jest aktywne tylko wtedy, gdy wetknięta jest prawidłowo sformatowana karta SD. Więcej informacji znaleźć można w instrukcji A500920.
Last Will	Aktywacja/dezaktywacja komunikatu Last Will Po aktywacji pojawią się kolejne pola edycji
(Last Will) Topic	Tu wpisuje się temat dla wysyłanej wiadomości Last Will.
(Last Will) Message	Wiadomość, która ma być wysłana jako wiadomość Last Will
(Last Will) QoS	„Quality of Service" (QoS) wiadomości Last Will
(Last Will) Retain	Aktywacja/dezaktywacja ostatniej wiadomości Last-Will wysłanej przez brokera pod danym tematem jako wiadomości zapisanej (Retained Message).
Device info	Aktywacja/dezaktywacja wiadomości Device Info, informującej usługę chmury o podstawowej konfiguracji sterownika. Więcej informacji znaleźć można w instrukcji A500920.
Device status	Aktywacja/dezaktywacja wiadomości Device State informująca usługę chmury o zmianach przełącznika trybu pracy i wskaźników LED. Więcej informacji znaleźć można w instrukcji A500920.

Parametr	Znaczenie
Standard commands	Aktywacja/dezaktywacja zintegrowanych komend standardowych Więcej informacji znaleźć można w instrukcji A500920. Jeśli nieaktywne: wspierane są tylko komendy zdefiniowane w programie IEC.
Application property template	Tworzenie własności dla poszczególnych wiadomości MQTT do chmury Azure Ten parametr jest opcjonalny, tzn. gdy pole pozostawione jest puste, ta własność nie jest wysyłana. Miejsce na tworzenie: ▪ <m>: Message type ▪ <p>: Protocol version ▪ <d>: DeviceId Przykłady: ▪ MyKey=HelloWorld_<m> ▪ TestKey=<m>/<p>/<d> ▪ DeviceId=<d>
[Submit]	Akceptacja zmiany; zmiana zostanie zrealizowana dopiero po następnym restarcie.

Poniższe tabele przedstawiają zależności między polami wyboru i edycji a poszczególnymi platformami chmury oraz możliwe ustawienia.

Tabela 178: Zależności między polami wyboru i edycji a poszczególnymi platformami chmury

Pole wyboru lun edycji	Platforma chmury					
	WAGO Cloud	Azure	MQTT AnyCloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
Enabled	x	x	x	x	x	x
Cloud platform	x	x	x	x	x	x
Hostname	x	x	x	x	x	
Port Number			x	(X)	x	
Device ID	x	x				
Client ID			x	x	x	
Authentication		x				x
Activation Key	x	X2				X2
Clean Session			x	(X)	x	
TLS			x	(X)	x	
CA file			x	x	x	x
User			x			
Password			x			
Certification file		X2	x	x	x	
Key file		X2	x	x	x	
Use websockets	x	X1				x
Proxy Type	X4	X4				X4
HTTP Proxy Host	X5	X5				X5
HTTP Proxy Port	X5	X5				X5
HTTP Proxy User	X5	X5				X5
HTTP Proxy Password	X5	X5				X5
Data Protocol		x	x	x	(X)	x
Use compression	x	X1	X1			X1
Cache mode	x	x	x	x	x	x

Pole wyboru lun edycji	Platforma chmury					
	WAGO Cloud	Azure	MQTT AnyCloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
Last Will			x	x	x	
Last Will Topic			X3	X3	X3	
Last Will Message			X3	X3	X3	
Last Will QoS			X3	X3	X3	
Last Will Retain			X3	(X3)	X3	
Device info		X1	X1	X1		X1
Device status		X1	X1	X1		X1
Standard commands		X1	X1	X1		X1
Application property template		X1				X1
X: Widoczne i aktywne						
(X): Widoczne, ale nieaktywne						
X1: Widoczne i aktywne, zależnie od wybranego protokołu danych						
X2: Widoczne i aktywne, zależnie od wybranego uwierzytelnienia						
X3: Widoczne i aktywne, gdy włączony jest „Last Will“.						
(X3): Widoczne ale nieaktywne, gdy włączony jest „Last Will“.						
X4: Aktywne, gdy włączony jest „Use websockets“.						
X5: Widoczne i aktywne, gdy włączony jest „Use websockets“ i gdy jako „Proxy Type“ ustawiony jest „HTTP“.						

Tabela 179: Możliwość wyboru protokołu danych dla poszczególnych platform chmury

Protokół danych	Platforma chmury					
	WAGO Cloud	Azure	MQTT AnyCloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
WAGO Protocol		x	x	x		x
WAGO Protocol 1.5		x	x	x		x
Native MQTT			x	x	(X)	
Sparkplug payload B		x	x	x		
X: Możliwość wyboru						
(X): Stała konfiguracja						

Tabela 180: Zależności między polami wyboru i edycji a poszczególnymi protokołami danych

Pole wyboru lub edycji	Protokół danych			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
Client ID	x	x	x	x
Use compression	x	x	x	
Device info	x	x		
Device status	x	x		
Standard commands	x	x		
Application property template	x	x		
X: Widoczne i aktywne				

Tabela 181: Możliwość wyboru trybu pamięci podręcznej zależnie od wybranego protokołu danych

Tryb pamięci podręcznej	Protokół danych			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
RAM	x	x	x	(X)
SD-Card	X1	X1	X1	
X: Możliwość wyboru				
X1: Możliwość wyboru tylko wtedy, gdy nie jest włączona opcja „Compression“				
(X): Stała konfiguracja				

Tabela 182: Zależności między polami wyboru i edycji a poszczególnymi uwierzytelnieniami

Pole wyboru lub edycji	Uwierzytelnienie	
	Shared Access Key	X.509 Certificate
Activation Key	x	
Certification file		x
Key file		x
X: Widoczne i aktywne		

7.1.1.3.24 Strona „Controls Settings“

Na stronie „Controls Settings“ w zakładce „Configuration“ dostępne są ustawienia oraz informacje dotyczące aktywacji i dezaktywacji przełącznika trybu pracy oraz przycisku Reset.

Tabela 183: Strona WBM „Controls Settings“ – grupa „OMS Controls“

Parametr	Znaczenie	
Current Mode	Aktualny stan funkcjonalności przełącznika trybu pracy oraz przycisku Reset	
	Inactive	Sterownik ignoruje każde użycie przełącznika trybu pracy i przycisku Reset.
	Active	Sterownik reaguje na użycie przełącznika trybu pracy i przycisku Reset.
Activate	Aktywacja/dezaktywacja przełącznika trybu pracy oraz przycisku Reset	
	☐	Wyłącz przełącznik trybu pracy i przycisk Reset.
	☑	Włącz przełącznik trybu pracy i przycisk Reset.
[Submit]	Akceptacja zmiany; zmiana zostanie zrealizowana dopiero po następnym restarcie.	

ⓘ Wskazówka

Przy wyłączonym przełączniku trybu pracy załadowany projekt bootowalny (CODESYS Boot Project) jest automatycznie uruchamiany po ponownym uruchomieniu urządzenia!

Zatrzymanie i zresetowanie działającej aplikacji przy wyłączonym przełączniku trybu pracy jest możliwe wyłącznie za pomocą środowiska programistycznego CODESYS.

7.1.1.3.25 Strona „Configuration of general SNMP parameters“

Na tej stronie można ustawić ogólne ustawienia SNMP.

Grupa „General SNMP Configuration“

Tabela 184: Strona WBM „Configuration of General SNMP Parameter“ – grupa „General SNMP Configuration“

Parametr	Znaczenie	
Service active	Aktywowanie/dezaktywowanie usługi SNMP	
	☐	Usługa SNMP jest dezaktywowana.
	☑	Usługa SNMP jest aktywna.
Name of Device	Wprowadzanie nazwy produktu (sysName)	
Description	Wprowadzanie opisu produktu (sysDescription).	
Physical Location	Wprowadzanie lokalizacji produktu (sysLocation).	
Contact	Wprowadzanie kontaktowego adresu e-mail (sysContact)	
ObjectID	Wprowadzanie Object ID.	
[Submit]	Akceptacja zmiany; zmiana zostanie zrealizowana dopiero po następnym restarcie.	

7.1.1.3.26 Strona „Configuration of SNMP v1/v2c Parameters“

Na stronie „Configuration of SNMP v1/v2c Parameters“ znajdują się ustawienia dla SNMP v1/v2c.

Grupa „Communities“

Tabela 185: Strona WBM „Configuration of SNMP v1/v2c Parameters“ – grupa „Communities“

Parametr	Znaczenie
Name	Nazwa Społeczności do konfiguracji managera SNMP
Access	Prawa dostępu dla Społeczności; Możliwe wartości to: ▪ ReadOnly ▪ ReadWrite
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.
[Add]	Dodaj nowy wpis.

Grupa „Trap Receivers“

Tabela 186: Strona WBM „Configuration of SNMP v1/v2cparameters" – grupa „Trap Receivers"

Parametr	Znaczenie
Host	Nazwa hosta lub adres IP nowego odbiorcy komunikatów trap (Management-station)
Community Name	Nazwa Społeczności do konfiguracji odbiorcy komunikatów trap
Wersja	Wersja SNMP, przez którą powinny być wysyłane komunikaty trap; Możliwe wartości: ▪ v1 ▪ v2c
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.
[Add]	Dodaj nowy wpis.

7.1.1.3.27 Strona „Configuration of SNMP v3 Parameters“

Na stronie „Configuration of SNMP v3 Parameters“ znajdują się ustawienia dla SNMP v3.

Grupa „Users“

Tabela 187: Strona WBM „Configuration of SNMP v3 Parameters“ – grupa „User“

Parametr	Znaczenie
Security Authentication Name	Nazwa użytkownika
Authentication Type	Typ uwierzytelnienia dla pakietów SNMP v3; Możliwe wartości: ▪ Brak uwierzytelnienia („None“) ▪ Message Digest 5 ("MD5") ▪ Secure Hash Algorithm ("SHA", "SHA224", "SHA256", "SHA384", "SHA512")
Authentication Key	Hasło do uwierzytelnienia
Privacy	Algorytm szyfrowania dla wiadomości SNMP; Możliwe wartości: ▪ Brak szyfrowania („None“) ▪ Data Encryption Standard ("DES") ▪ Advanced Encryption Standard ("AES", "AES128", "AES192", "AES192C", "AES256", "AES256C")
Privacy Key	Kod szyfrowania
Access	Prawa dostępu dla użytkownika v3; Możliwe wartości: ▪ ReadOnly ▪ ReadWrite
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.
[Add]	Dodaj nowy wpis.

Grupa „Trap Receivers“

Tabela 188: Strona WBM „Configuration of SNMP v3 Parameters“ – grupa „Trap Receivers“

Parametr	Znaczenie
Security Authentication Name	Nazwa użytkownika
Authentication Type	Typ uwierzytelnienia dla pakietów SNMP v3; Możliwe wartości: ▪ Brak uwierzytelnienia („None“) ▪ Message Digest 5 ("MD5") ▪ Secure Hash Algorithm ("SHA", "SHA224", "SHA256", "SHA384", "SHA512")
Authentication Key	Hasło do uwierzytelnienia
Privacy	Algorytm szyfrowania dla wiadomości SNMP; Możliwe wartości: ▪ Brak szyfrowania („None“) ▪ Data Encryption Standard ("DES") ▪ Advanced Encryption Standard ("AES", "AES128", "AES192", "AES192C", "AES256", "AES256C")
Privacy Key	Kod szyfrowania
Host	Nazwa hosta lub adres IP odbiorcy komunikatów trap v3
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.
[Add]	Dodaj nowy wpis.

7.1.1.3.28 Strona „Commissioning Settings“

Na stronie „Commissioning Settings" znajdują się informacje i ustawienia dotyczące usługi „Commissioning Agent".

Grupa „Commissioning“

Tabela 189: Strona WBM „Commissioning Settings" – grupa „Commissioning"

Parametr	Znaczenie	
Service Enabled	Aktywacja/dezaktywacja usługi „Commissioning Agent"	
	☐	Usługa „Commissioning Agent" jest nieaktywna.
	☑	Usługa „Commissioning Agent" jest aktywowana.
Commissioning State	Aktualny status usługi „Commissioning Agent"	
	inactive	Usługa nie jest aktywna.
	searching	Usługa szuka serwera.
	requesting	Usługa znalazła serwer i próbuje się połączyć.
	awaiting response	Usługa czeka na akceptację przez serwer.
	no server found	Usługa nie znalazła poprawnego serwera w podanym czasie pięciu minut. Aby ponownie rozpocząć wyszukiwanie, należy ponownie uruchomić urządzenie.
	processing	Usługa uruchamia instalację pakietów otrzymanych z serwera.
	error exit	Usługa przerwała instalację z powodu wewnętrznego błędu.
	success	Usługa pomyślnie zakończyła instalację.
Connected Server	Domena serwera, do którego podłączony jest produkt; Jeśli produkt nie jest podłączony, wyświetlana jest informacja "-".	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

7.1.1.3.29 Strona „Docker Settings“

Na stronie „Docker Settings“ znajdują się ustawienia dla usługi „Docker®“.

Grupa „Docker Status“

Tabela 190: Strona WBM „Docker Settings“ – grupa „Docker Status“

Parametr	Znaczenie	
Current State	Aktualny status usługi „Docker®"	
	stopped	Usługa „Docker®" została zatrzymana.
	running	Usługa „Docker®“ jest aktywna.
Service Enabled	Aktywacja/dezaktywacja usługi Docker®	
	☐	Usługa „Docker®" jest nieaktywna.
	☑	Usługa „Docker®" jest aktywna.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

7.1.1.3.30 Strona „WBM User Configuration“

Na stronie „WBM User Configuration“ można znaleźć ustawienia dla User-Aministration.

Grupa „Change Passwords“

Wskazówka

Zmienić hasła!

Ustawione fabrycznie, standardowe hasła podane w niniejszej instrukcji obsługi nie stanowią wystarczającego zabezpieczenia!

- Należy zmienić te hasła stosownie do potrzeb.

Wskazówka

Dopuszczalne znaki w hasłach

Hasło może zawierać tylko następujące znaki:
małe litery (a ... z), duże litery (A ... Z), cyfry (0 ... 9) oraz znaki spcjalne (! " # $ % & ' ( ) * + , . / : ; < = > ? @ [ ] ^ _ ` { } | ~ –).

Wskazówka

W hasłach WBM używać dopuszczalnych znaków!

Jeśli poza WBM (np. przez CBM) tworzone są hasła zawierające znaki niedopuszczalne w WBM, dostęp do stron WBM nie będzie możliwy!

Tabela 191: Strona WMB „Users Configuration“ – grupa „Change Passwords“

Parametr	Znaczenie
Old Password	Wprowadzanie aktualnie używanego hasła do uwierzytelnienia.
New Password	Wprowadzanie nowego hasła.
Confirm Password	Wprowadzanie nowego hasła do kontroli.
[Set Password]	Zastosuj nowe hasło

Wskazówka

Rozszerzone uprawnienia użytkowników WBM

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

7.1.1.4 Zakładka „Fieldbus“

7.1.1.4.1 Strona „OPC UA Configuration“

Na stronie „OPC UA Configuration“ znajdują się ustawienia dla usługi OPA UA.

Grupa „OPC UA Server Configuration“

Tabela 192: Strona WBM „OPC UA Configuration“ – grupa „OPC UA Server Configuration“

Parametr	Znaczenie	
Enabled	Aktywowanie/dezaktywowanie serwera OPC UA	
	☐	Serwer OPC UA jest dezaktywowany.

Parametr	Znaczenie	
	☑	Serwer OPC UA jest aktywowany.
Log Level	Wybór poziomu logowania; Wybrany poziom logowania wpływa na czas reakcji serwera. Dlatego należy wybrać najniższy niezbędny poziom, np. „Debug" dla dogłębnych analiz. Do ustawienia są następujące wartości:	
	Error	Wyświetlane są tylko komunikaty o błędach.
	Warning	Wyświetlane są komunikaty o błędach i ostrzeżenia.
	Info	Wyświetlane są komunikaty o błędach, ostrzeżenia i komunikaty o statusie.
	Debug	Wyświetlane są komunikaty o błędach, komunikaty ostrzegawcze, komunikaty o statusie oraz komunikaty debugowania.
Ctrl Configuration name	Wrowadzanie nazwy konfiguracji, którą otrzymuje sterownik wewnątrz PLC Open Device Set.	
[Submit]	Akceptacja zmiany; zmiana zostanie zrealizowana dopiero po następnym restarcie.	

Grupa „OPC UA Server Security Settings"

Tabela 193: Strona WBM „OPC UA Configuration" – grupa „OPC UA Server Security Settings"

Parametr	Znaczenie	
Anonymous Access	Zablokuj/Zezwól na anonimowy dostęp do serwera.	
	☐	Dostęp anonimowy jest niedozwolony.
	☑	Dostęp anonimowy jest dozwolony; pod warunkiem że uwierzytelnianie portu runtime jest również wyłączone.
Allow Password On Plaintext	Transmisja hasła w czytelnym formacie	
	☐	
	☑	
Security Modes	Tryb bezpieczeństwa serwera OPC UA; W zależności od wybranego trybu pracy dostępne są różne punkty końcowe OPC UA do nawiązania połączenia.	
	None	Zaznaczona tylko opcja OPC UA Endpoint **None**. Umożliwia nawiązanie niezabezpieczonego połączenia z serwerem OPC UA.
	None + Sign + SignAndEncrypt	Punkty końcowe **None**, **Sign** i **SignAndEncrypt** są dostępne. **Sign** udostępnia punkt końcowy, który jest chroniony hasłem. **SignAndEncrypt** udostępnia punkt końcowy, który oprócz hasła udostępnia również szyfrowanie.
	Sign + SignAndEncrypt	Punkty końcowe **Sign** i **SignAndEncrypt** są dostępne.
	SignAndEncrypt	Tylko Endpoint **SignAndEncrypt** jest dostępny.
Security Policies	Wybór polityki bezpieczeństwa; Tu ustawia się moc szyfrowania serwera OPC UA. Do wyboru są: Aes128Sha256RsaOaep and better, Basic256Sha256 and better, Aes256Sha256RsaPss.	
[Submit]	Akceptacja zmiany; zmiana zostanie zrealizowana dopiero po następnym restarcie.	

7.1.1.4.2 Strona „BACnet Status“

Na stronie „BACnet Status” wyświetlane są informacje o produkcie specyficzne dla sieci obiektowej BACnet i licencji BACnet.

Grupa „BACnet Information“

Tabela 194: Strona WBM „BACnet Status” – grupa „BACnet Information“

Parametr	Znaczenie	
State	Status sieci obiektowej BACnet	
	☐	Sieć BACnet jest dezaktywowana.
	☑	Sieć BACnet jest aktywowana.
Mode	Tryb pracy BACnet	
	ip	Komunikacja poprzez BACnet/IP
	sc	Komunikacja poprzez BACnet/SC
Wersja	Zainstalowana wersja BACnet	
Status Info	Status sieci obiektowej BACnet	
Device-ID	Aktualny Device ID produktu	

Grupa „BACnet License“

Tabela 195: Strona WBM „BACnet Status” – grupa „BACnet License“

Parametr	Znaczenie
Type	Wyświetlanie licencji dla BACnet
User Objects	Wyświetlanie liczby istniejących obiektów oraz liczby obiektów możliwych do użycia na podstawie licencji BACnet

Grupa „BACnet Data Link

Tabela 196: Strona WBM „BACnet Status" – grupa „BACnet Data Link"

Parametr	Znaczenie
Connection Info	Wskaźnik statutu płączenia

7.1.1.4.3 Strona „BACnet Configuration“

Na tej stronie można wprowadzić ustawienia specyficzne dla sieci obiektowej BACnet.

Grupa „Restart"

Tabela 197: Strona WBM „BACnet Data Link" – grupa „BACnet Restart"

Parametr	Znaczenie
[Restart]	Restart usługi BACnet

Grupa „BACnet Service“

Tabela 198: Strona WBM „BACnet Configuration” – grupa „BACnet Service“

Parametr	Znaczenie	
Service active	Aktywowanie/dezaktywowanie sieci obiektowej BACnet	
	☐	Sieć BACnet jest dezaktywowana.
	☑	Sieć BACnet jest aktywowana.
Mode	Tu wybiera się tryb pracy BACnet.	
	ip	Komunikacja poprzez BACnet/IP

Parametr	Znaczenie	
	sc	Komunikacja poprzez BACnet/SC
Who-Is online interval time (sec)	Odstęp czasowy między zapytaniami sterownika dla sieci obiektowej, które inne urządzenia są dostępne online (minimalny: 60 s).	
Broadcast I-Am answer	Umożliwia aktywację/dezaktywację wysyłania przez urządzenie komunikatów I-Am na broadcast BACnet.	
	☐	Wiadomości I-AM nie są wysyłane na adres BACnet Broadcast.
	☑	Wiadomości I-AM są wysyłane na adres BACnet Broadcast.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana dopiero po następnym restarcie sterownika lub restarcie BACnet.	

Grupa „BACnet Data"

Tabela 199: Strona WBM „BACnet Configuration" – grupa „BACnet Data"

Parametr	Znaczenie
Delete Persistence Data	Trwałe dane BACnet zostaną usunięte podczas następnego uruchomienia.
Reset all BACnet Data and Settings to Default	Przy kolejnym restarcie specyficzne ustawienia i dane BACnet zostają zresetowane do ustawień fabrycznych.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana dopiero po następnym restarcie sterownika lub restarcie BACnet.
override. xmlChose file ...	Wybór pliku na PC
[Upload]	Przesyłanie wybranego pliku z PC do sterownika

Grupa „BACnet Log Level"

Tabela 200: Strona WBM „BACnet Configuration" – grupa „BACnet Log Level"

Parametr	Znaczenie	
Error	Aktywacja/dezaktywacja edycji dziennika błędów	
	☐	Wpisy do dziennika błędów nie są wyświetlane.
	☑	Wyświetlane są wpisy do dziennika błędów.
Warning	Aktywacja/dezaktywacja wyjścia dziennika ostrzeżeń	
	☐	Wpisy do dziennika ostrzeżeń nie są wyświetlane.
	☑	Wyświetlane są wpisy do dziennika ostrzeżeń.
Info	Aktywacja/dezaktywacja edycji dziennika zdarzeń	
	☐	Wpisy do dziennika zdarzeń nie są wyświetlane.
	☑	Wyświetlane są wpisy do dziennika zdarzeń.
Debug	Aktywacja/dezaktywacja wyjścia dziennika błędów	
	☐	Wpisy w dzienniku debugowania nie są wyświetlane.
	☑	Wyświetlane są wpisy do dziennika błędów.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana dopiero po następnym restarcie sterownika lub restarcie BACnet.	

Grupa „BACnet Network Capture"

Tabela 201: Strona WBM „BACnet Configuration" – grupa „BACnet Network Capture"

Parametr	Znaczenie	
Enable	Aktywacja/dezaktywacja rejestrowania ruchu sieciowego przy użyciu odpowiednich filtrów BACnet	
	☐	Ruch sieciowy nie jest rejestrowany.
	☑	Rejestracja ruchu sieciowego
Log pre-master secrets	Aktywacja/dezaktywacja zapisu secrets w celu odszyfrowania ruchu sieciowego BACnet/SC	
	☐	Secrets nie są zapisywane.
	☑	Secrets są zapisywane.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana dopiero po następnym restarcie sterownika lub restarcie BACnet.	
BACnet Network Capture Archive **[Download]**	Za pomocą przycisku [Download] można pobrać z urządzenia zarejestrowany ruch sieciowy, w tym dane uwierzytelniające, jeśli ta opcja jest włączona.	

7.1.1.4.4 Strona „BACnet Data Link"

Grupa „Restart"

Tabela 202: Strona WBM „BACnet Data Link" – grupa „BACnet Restart"

Parametr	Znaczenie
[Restart]	Restart usługi BACnet

Grupa „BACnet/IP"

Tabela 203: Strona WBM „BACnet Data Link" – grupa „BACnet/IP"

Parametr	Znaczenie
Port Number	Wprowadzanie portu dla komunikacji BACnet/IP
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana dopiero po następnym restarcie sterownika lub restarcie BACnet.

Grupa „BACnet/SC"

Tabela 204: Strona WBM „BACnet Data Link" – grupa „BACnet/SC"

Parametr	Znaczenie	
Mode	Wybór trybu pracy BACnet/SC	
	regular	Urządzenie pracuje jako BACnet/SC Node.
	primary	Urządzenie pracuje jako BACnet/SC Primary HUB.
	failover	Urządzenie pracuje jako BACnet/SC Failover HUB.
Port Number	Wprowadzanie portu dla komunikacji BACnet/SC	
Primary Hub URI	Wpisanie URI dla głównego HUB-a (Primary HUB); wss://<IP-Adresse>:<Port HUBs> lub wss://<Domainname>:<Port HUBs> (np. wss://192.168.178.19:47808 lub wss://PFC200V3-XXXXXX.localdomain.lan:47808)	
Failover Hub URI	Wpisanie URI dla HUB przełączania awaryjnego; wss://<adres IP>:<Port HUBs> lub wss://<Domainname>:<Port HUBs> (np. wss://192.168.178.19:47808 lub wss://PFC200V3-XXXXXX.localdomain.lan:47808)	

Parametr	Znaczenie
Allow self signed Certificates	Aktywuj/dezaktywuj, czy komunikacja może być nawiązywana za pomocą certyfikatów z sygnaturą własną.
Allow expired Certificates	Aktywuj/dezaktywuj, czy komunikacja przez wygasłe certyfikaty może być nawiązana.
Allow any Certificates	Aktywuj/dezaktywuj, czy komunikacja może być nawiązywana przez dowolne certyfikaty.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana dopiero po następnym restarcie sterownika lub restarcie BACnet.

Grupa „BACnet/SC Certificate Authority (CA)"

Tabela 205: Strona WBM „BACnet Data Link" – grupa „BACnet/SC Certificate Authority (CA)"

Parametr	Znaczenie
Chose file ...	Wybór certyfikatu CA na komputerze w celu przesłania do urządzenia
[Upload]	Przesłanie wybranego certyfikatu CA do urządzenia; Po restarcie certyfikat ten jest używany jako certyfikat CA do komunikacji BACnet/SC.

Grupa „BACnet/SC Certificate"

Tabela 206: Strona WBM „BACnet Data Link" – grupa „BACnet/SC Certificate"

Parametr	Znaczenie
Chose file ...	Wybór certyfikatu urządzenia na komputerze w celu przesłania do urządzenia
[Upload]	Przesłanie wybranego certyfikatu urządzenia na urządzenie; Po restarcie certyfikat ten jest używany do komunikacji BACnet/SC.

Grupa „BACnet/SC Certificate Signing Request (CSR)"

Tabela 207: Strona WBM „BACnet Configuration" – grupa „BACnet/SC Certificate Signing Request (CSR)"

Parametr	Znaczenie
Country	Wprowadzanie nazwy kraju dla CSR lub certyfikatu urządzenia (dwie litery)
State	Dane dotyczące państwa dla CSR lub certyfikatu urządzenia
Locality	Wprowadzanie lokalizacji dla CSR lub certyfikatu urządzenia.
Organization	Wprowadzanie nazwy firmy lub organizacji dla CSR lub certyfikatu urządzenia.
Organizational Unit	Wprowadzanie nazwy działu dla CSR lub certyfikatu urządzenia.
Common Name	Wprowadzanie nazwy urządzenia dla CSR lub certyfikatu urządzenia.
[Generate]	Tworzenie na urządzeniu CSR i nowego klucza prywatnego
[Download]	Pobieranie CSR z urządzenia

Grupa „BACnet/SC Default Certificates"

Tabela 208: Strona WBM „BACnet Data Link" – grupa „BACnet/SC Default Certificates"

Parametr	Znaczenie
[Generate]	Tworzenie nowego certyfikatu

7.1.1.4.5 Strona „BACnet Storage Location“

Na stronie „BACnet Storage Location“ można wprowadzić ustawienia dla zapisu parametrów specyficznych dla BACnet.

Grupa „BACnet Persistence“

Tabela 209: Strona WBM „BACnet Storage Location” – grupa „BACnet Persistence“

Parametr	Znaczenie	
Storage Location	Wybierz lokalizację dla danych trwałych; wybór możliwy jest tylko wtedy, gdy oba nośniki są dostępne.	
	Internal Flash	Dane są zapisywane w wewnętrznej pamięci sterownika.
	SD-Card	Dane zapisywane są na karcie pamięci. Jeśli wybrana jest opcja „SD-Card“, ale karta pamięci jest już wyjęta, opcja ta nie jest już aktywna i można wybrać tylko „Internal-Flash“.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

Grupa „BACnet Trendlog”

Tabela 210: Strona WBM „BACnet Storage Location” – grupa „BACnet Trendlog“

Parametr	Znaczenie	
Storage Location	Wybierz lokalizację danych trendów; wybór jest możliwy tylko wtedy, gdy oba nośniki są dostępne.	
	Internal Flash	Dane są zapisywane w wewnętrznej pamięci sterownika.
	SD-Card	Dane zapisywane są na karcie pamięci. Jeśli wybrana jest opcja „SD-Card“, ale karta pamięci jest już wyjęta, opcja ta nie jest już aktywna i można wybrać tylko „Internal-Flash“.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

Grupa „BACnet Eventlog”

Tabela 211: Strona WBM „BACnet Storage Location” – grupa „BACnet Eventlog“

Parametr	Znaczenie	
Storage Location	Wybierz lokalizację dla danych dziennika zdarzeń; Wybór możliwy jest tylko wtedy, gdy oba nośniki są dostępne.	
	Internal Flash	Dane są zapisywane w wewnętrznej pamięci sterownika.
	SD-Card	Dane zapisywane są na karcie pamięci. Jeśli wybrana jest opcja „SD-Card“, ale karta pamięci jest już wyjęta, opcja ta nie jest już aktywna i można wybrać tylko „Internal-Flash“.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

7.1.1.4.6 Strona „BACnet Info"

Na stronie "BACnet Info"znajdują się ustawienia do wyświetlania informacji specyficznych dla BACnet.

Grupa „Refresh Options“

Tabela 212: Strona WBM „BACnet Info" – grupa „Refresh Options"

Parametr	Znaczenie
Automatic refresh interval (sec)	Włączanie/wyłączanie cyklicznej aktualizacji; wprowadzanie czasu cyklu w sekundach, z jakim ma być wykonywana cykliczna aktualizacja; w zależności od statusu zmienia się etykieta przycisku ("Refresh"/"Start"/"Stop").

Parametr	Znaczenie
[Refresh]	Aktualizacja wyświetlania; Przycisk jest widoczny tylko wtedy, gdy cykliczna aktualizacja nie jest włączona.
[Start]	Uruchomienie cyklicznej aktualizacji; Przycisk ten jest widoczny tylko wtedy, gdy cykliczna aktualizacja jest włączona, ale jeszcze nie została uruchomiona.
[Stop]	Zakończenie cyklicznej aktualizacji; Przycisk widoczny jest tylko wtedy, gdy cykliczna aktualizacja jest aktywna.

Cykliczną aktualizację można przeprowadzić tylko tak długo, jak otwarta jest strona „BACnet Info". Przy zmianie strony WBM aktualizacja zostaje zatrzymana do momentu, aż strona „BACnet Info" zostanie ponownie otwarta.

Grupa „BACnet/IP Statistics"

Tabela 213: Strona WBM „BACnet Info" – grupa „BACnet/IP Statistics"

Parametr	Znaczenie
BACnet/IP Statistics	BACnet/IP Statistik Jeśli brak danych, wyświetlana jest informacja „no data available or retrieved".

Grupa „BACnet/SC Statistics"

Tabela 214: Strona WBM „BACnet Info" – grupa „BACnet/SC Statistics"

Parametr	Znaczenie
BACnet/SC Statistics	BACnet/SC Statistics Jeśli brak danych, wyświetlana jest informacja „no data available or retrieved".

BACnet/SC Connections"

Tabela 215: Strona WBM „BACnet Info" – grupa „BACnet/SC Connections"

Parametr	Znaczenie
BACnet/SC Connections	BACnet/SC Connections Jeśli brak danych, wyświetlana jest informacja „no data available or retrieved".

7.1.1.5 Zakładka „Security“

7.1.1.5.1 Strona „OpenVPN / IPsec“

Wskazówka

Potencjalna luka bezpieczeństwa w protokołach VPN!

Protokoły VPN domyślnie umożliwiają uruchamianie skryptów Hook. To stanowi potencjalną lukę bezpieczeństwa.

1. Jeśli nie korzystasz z możliwości używania protokołów Hook, wyłącz je w konfiguracji. Dostosuj w tym celu odpowiedni plik konfiguracyjny.
2. Aby wyłączyć korzystanie z poleceń typu Hook w OpenVPN, należy w pliku konfiguracyjnym „openvpn.conf“ użyć polecenia `--script-security level 1`.
   Więcej informacji można znaleźć na stronie **www.openvpn.net/community-resources/reference-manual-for-openvpn-2-5/#scripting-integration**.
3. Aby wyłączyć korzystanie z poleceń typu Hook w IPsec, należy w pliku konfiguracyjnym „ipsec.conf“ użyć polecenia `--disable-updown`.
   Więcej informacji można znaleźć na stronie **www.wiki.strongswan.org/projects/strongswan/wiki/Updown/**.

Na stronie „OpenVPN / IPsec“ znajdują się ustawienia OpenVPN i IPsec.

Grupa „OpenVPN“

Tabela 216: Strona WBM „OpenVPN / IPsec" – grupa „OpenVPN"

Parametr	Znaczenie	
Current State	Aktualny status usługi OpenVPN	
	stopped	Usługa nie jest aktywna.
	running	Usługa jest aktywna.
OpenVPN enabled	Aktywowanie/dezaktywowanie usługi OpenVPN.	
openvpn.conf	Tu wybiera się plik konfiguracyjny OpenVPN, który należy przesłać z PC do produktu lub na odwrót.	
[Submit]	Akceptacja zmiany; zmiana zostanie zrealizowana dopiero po następnym restarcie.	
Choose file ...	Wybierz plik na produkcie lub komputerze	
[Upload]	Przesyłanie wybranego pliku z PC do produktu	
[Download]	Przesyłanie wybranego pliku z produktu do PC	

Grupa „IPsec“

Tabela 217: Strona WBM „OpenVPN / IPsec" – grupa „IPsec"

Parametr	Znaczenie	
Current State	Aktualny status usługi IPsec	
	stopped	Usługa nie jest aktywna.
	running	Usługa jest aktywna.
IPsec enabled	Aktywowanie/dezaktywowanie usługi OpenVPN.	
ipsec.conf	Tu wybiera się plik konfiguracyjny IPsec, który należy przesłać z PC do produktu lub na odwrót.	
ipsec.secrets	Wybierz plik IPsec Secrets, który należy przesłać z PC do produktu lub na odwrót	

Parametr	Znaczenie
[Submit]	Akceptacja zmiany; zmiana zostanie zrealizowana dopiero po następnym restarcie.
Choose file ...	Wybierz plik na produkcie lub komputerze
[Upload]	Przesyłanie wybranego pliku z PC do produktu
[Download]	Przesyłanie wybranego pliku z produktu do PC

7.1.1.5.2 Strona „General Firewall Configuration"

Na stronie „General Firewall Configuration" można znaleźć globalne ustawienia dla funkcji Firewall.

Grupa „Global Firewall Parameter"

Tabela 218: Strona WBM „General Firewall Configuration" – grupa „Global Firewall Parameter"

Parametr	Znaczenie
Firewall enabled entirely	Aktywacja/dezaktywacja pełnej funkcjonalności firewalla. To ustawienie ma najwyższy priorytet. Gdy firewall jest wyłączony, wszystkie inne ustawienia nie mają bezpośredniego znaczenia. Konfiguracja innych parametrów jest mimo to możliwa, aby przed włączeniem funkcji Firewall można było prawidłowo ustawić jej parametry. To ustawienie jest niezależne od ustawienia opcji „Filter enabled" w grupie „MAC address filter state Bridge <n>" na stronie „MAC address filter state Bridge".
ICMP echo broadcast protection	Aktywacja/dezaktywacja zabezpieczenia „ICMP echo broadcast"
Max. UDP connections per second	Wprowadzanie maksymalnej liczby połączeń UDP na sekundę
Max. TCP connections per second	Wprowadzanie maksymalnej liczby połączeń TCP na sekundę
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

ⓘ Wskazówka

Usługi CODESYS są odrzucane przy włączonej zaporze sieciowej, jeśli nie skonfigurowano filtrów użytkownika!

Jeśli wykorzystywane są usługi CODESYS (np. Modbus, OPC-UA, SNMP lub IIOT), w konfiguracji firewalla należy utworzyć odpowiednie filtry użytkownika dla tych usług. Filtry użytkownika muszą być skonfigurowane w taki sposób, aby odpowiednie porty były akceptowane.

7.1.1.5.3 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 219: Strona WBM „Interface Configuration" – grupa „Firewall Configuration Bridge <n> / VPN / WAN"

Parametr	Znaczenie
Firewall enabled for Interface	Aktywowanie/dezaktywowanie funkcji Firewall dla poszczególnych interfejsów

Parametr	Znaczenie
ICMP echo protection	Aktywacja/dezaktywacja zabezpieczenia „ICMP echo“ dla poszczególnych interfejsów
ICMP echo limit per second	Wprowadzanie maksymalnej liczby „ICMP pings" na sekundę. „0“ = „Disabled“
ICMP burst limit (0=disabled)	Wprowadzanie maksymalnej liczby „ICMP echo burst" na sekundę
Service Configuration	Aktywacja/dezaktywacja funkcji firewall dla poszczególnych usług
FTP/FTPES	Nie każda z przedstawionych tu usług jest dostępna dla każdego produktu. Same usługi muszą być włączane i wyłączane osobno przez stronę „Ports and Services“.
FTPS (implicit)	
HTTP	
HTTPS	
I/O Check	
PLC Runtime	
WebVisu – HTTP (port 8080)	
WebVisu – HTTPS (port 8081)	
SSH	
SNMP	
OPC UA (port 4840)	
BACnet (port 47808)	
PROFINET IO	
DNP3 (port 20000)	
IEC60870-5-104 (port 2404)	
IEC61850 (port 102)	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

W przypadku sterowników z funkcjonalnością telesterowania otwierane są standardowo porty Firewall wymienione w tabeli poniżej. Przez te porty mogą być realizowane odpowiednie usługi telesterowania, bez blokowania ich komunikacji przez Firewall.

Tabela 220: Porty dla funkcjonalności telecontrol

Protokół	Port
DNP3	20000
IEC60870-5-104	2404
IEC 61850	102

7.1.1.5.4 Strona „Configuration of MAC address filter“

Na tej stronie ustawia się konfigurację funkcji Firewall na poziomie sieci ETHERNET.

„MAC Address Filter Whitelist“ otrzymuje dwa domyślne wpisy o następujących wartościach:

- Opis: Wszystkie urządzenia WAGO
  Adres MAC: 00:30:DE:00:00:00
  Maska MAC: ff:ff:ff:00:00:00
- Opis: Enable docker bridges
  Adres MAC: 02:42:00:00:00:00
  Maska MAC: ff:ff:00:00:00:00

Po włączeniu pierwszego domyślnego wpisu można komunikować ze sobą w sieci różne produkty WAGO.

ⓘ 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 potem uzyskać dostępu do produktu przez sieć ETHERNET. Dotyczy to również innych usług używanych przez Twój produkt, np. konfiguracji IP przez DHCP.
Jeśli adres MAC Twojego serwera DHCP nie znajduje się na „białej liście filtrowania adresów MAC" (MAC Address Filter Whitelist), produkt po kolejnym cyklu aktualizacji utraci swoje ustawienia IP i również stanie się niedostępny. .
Dopóki w „MAC Address Filter Whitelist" nie będzie zawarty żaden wpis, załączenie filtra jest zablokowane.
Jeśli został wpisany co najmniej jeden dozwolony adres, przed aktywacją filtra pojawi się odpowiednie ostrzeżenie, które należy potwierdzić.
Opisany powyżej test jest przeprowadzany tylko w WBM, a nie w CBM!

Grupa „Global MAC address filter state"

Tabela 221: Strona WBM „Configuration of MAC address filter" – grupa „Global MAC address filter state"

Parametr	Znaczenie
Filter enabled	Aktywowanie/dezaktywowanie globalnego filtra adresów MAC
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

Grupa „MAC address filter state Bridge <n>"

Dla każdego skonfigurowanego bridge'a wyświetlana jest osobna grupa.

Tabela 222: Strona WBM „Configuration of MAC address filter" – grupa „MAC address filter state Bridge <n>"

Parametr	Znaczenie
Filter enabled	Aktywacja/dezaktywacja filtra adresu MAC dla danego bridge'a; To ustawienie jest niezależne od ustawienia „Firewall enabled entirely" w grupie „Global Firewall Parameter" na stronie „General Firewall Configuration".
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

Grupa „MAC address filter whitelist"

Tabela 223: Strona WBM „Configuration of MAC address filter" – grupa „MAC address filter whitelist"

Parametr	Znaczenie
Description	Opis urządzeń lub obszary, które przy ogólnie aktywowanym firewallu można odblokować przez aktywację filtra. Opis widoczny jest tylko przy wpisach, które pojawiły się w ustawieniu fabrycznym.
MAC address	Adres MAC pozycji na liście
MAC mask	Maska MAC pozycji na liście
Filter enabled	Aktywacja/dezaktywacja filtra dla pozycji na liście
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.
[Add]	Dodaj nowy wpis.

7.1.1.5.5 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 224: Strona WBM „Configuration of User Filter“ – grupa „User filter“

Parametr	Znaczenie	
Policy	Zezwól/wyłącz urządzenie sieciowe przez filtr	
	Allow	Urządzenie sieciowe jest dopuszczone.
	Drop	Urządzenie sieciowe jest wykluczone.
Source IP address	Źródłowy adres IP dla filtra	
Source Netmask	Maska sieci źródłowej dla filtra	
Source Port	Numer portu źródłowego dla filtra	
Destination IP address	Docelowy adres IP dla filtra	
Destination Netmask	Maska sieci docelowej dla filtra	
Destination Port	Numer portu docelowego dla filtra	
Protocol	Protokoły dla filtra	
	TCP/UDP	Serwisy TCP i UDP są filtrowane.
	TCP	Serwis TCP jest filtrowany.
	UDP	Serwis UDP jest filtrowany.
Input interface	Interfejsy do filtra	
	Any	Wszystkie interfejsy są filtrowane.
	Bridge <n>	Filtrowane są interfejsy przypisane do bridge'a <n>. Wyświetlane są tylko skonfigurowane bridge.
	VPN	Interfejs VPN jest filtrowany.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

ⓘ Wskazówka

Usługi CODESYS są odrzucane przy włączonej zaporze sieciowej, jeśli nie skonfigurowano filtrów użytkownika!

Jeśli wykorzystywane są usługi CODESYS (np. Modbus, OPC-UA, SNMP lub IIOT), w konfiguracji firewalla należy utworzyć odpowiednie filtry użytkownika dla tych usług. Filtry użytkownika muszą być skonfigurowane w taki sposób, aby odpowiednie porty były akceptowane.

7.1.1.5.6 Strona „Certificates“

Na tej stronie znajdują się ustawienia certyfikatów.

Grupa „Installed Certificates“

Tabela 225: Strona WBM „Certificates" – grupa „Installed Certificates"

Parametr	Znaczenie
<certificate name>	Załadowane certyfikty; Jeśli nie załadowano żadnego certyfikatu, wyświetlany jest komunikat „No certificates existing“.

Parametr	Znaczenie
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.
Choose file ...	Wybierz plik na PC
[Upload]	Przesyłanie wybranego pliku z PC do produktu

Certyfikaty są zapisywane w katalogu „/etc/certificates/".

Grupa „Installed Private Keys"

Tabela 226: Strona WBM „Certificates" – grupa „Installed Private Keys"

Parametr	Znaczenie
<private key name>	Załadowane klucze; Jeśli nie załadowano żadnego klucza, wyświetlany jest komunikat „No privace keys existing".
[Delete]	Usuń wybraną pozycję; Przycisk widoczny jest tylko wtedy, gdy istnieją wpisy.
Choose file ...	Wybierz plik na PC
[Upload]	Przesyłanie wybranego pliku z PC do produktu

Klucze są zapisywane w katalogu „/etc/certificates/keys/".

7.1.1.5.7 Strona „Boot mode configuration"

Na stronie „Boot mode configuration" znajdują się ustawienia opcji bootowania.

ⓘ Wskazówka

Przy wymuszeniu bootowania z wewnętrznej pamięci flash urządzenie nie może być uruchomione z karty pamięci!

Jeśli z powodu problemów lub nieprawidłowej konfiguracji połączenie przez ETHERNET nie jest już możliwe, można ponownie uzyskać dostęp do produktu poprzez złącze serwisowe i „WAGO Ethernet Settings".

Grupa „Force internal boot"

Tabela 227: Strona WBM „Boot mode configuration" – grupa „Force internal boot"

Parametr	Znaczenie	
Boot Mode	Ustawienie opcji rozruchu urządzenia	
	Memory card or internal flash	Urządzenie może być uruchamiane z pamięci Flash wewnętrznej lub z karty pamięci.
	Internal flash only	Urządzenie może być uruchamiane wyłącznie z pamięci Flash wewnętrznej.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

7.1.1.5.8 Grupa „Security Settings"

Na tej stronie znajdują się ustawienia dotyczące bezpieczeństwa sieci.

Grupa „TLS Configuration“

Tabela 228: Strona WBM „Security Settings“ – grupa „TLS Configuration“

Parametr	Znaczenie	
TLS Configuration	Ustawianie dozwolonych wersji TLS i procedur kryptograficznych dla HTTPS	
	standard	Serwer WWW zezwala na wersje TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 oraz innych algorytmów kryptograficznych, które obecnie nie są już uznawane za bezpieczne.
	Strong	Serwer WWW zezwala tylko na wersję TLS 1.2, TLS 1.3 i na silne algorytmy.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

ⓘ Wskazówka

Techniczna dyrektywa TR-02102 BSI

Zasady dotyczące ustawienia „Strong“ są oparte na wytycznej technicznej TR-02102 Federalnego Urzędu ds. Bezpieczeństwa Informacji. Wytyczne znajdują się na stronie:
↗ **www.bsi.bund.de**.

7.1.1.5.9 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 229: Strona WBM „Advanced Intrusion Detection Environment (AIDE)“ – grupa „Run AIDE check at startup“

Parametr	Znaczenie	
Service active	Aktywowanie/dezaktywowanie „AIDE check“ przy starcie sterownika	
	☐	„AIDE check" nie jest aktywny przy starcie.
	☑	„AIDE check" jest aktywny przy starcie.
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

Grupa „Control AIDE and show log"

Tabela 230: Strona WBM „Advanced Intrusion Detection Environment (AIDE)“ – grupa „Control AIDE and show log“

Parametr	Znaczenie	
Select Action	Wybierz 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	Włączanie/wyłączanie ostatniego n komunikatów; wprowadzanie liczby wyświetlanych komunikatów.	

Parametr	Znaczenie
Automatic refresh interval (sec)	Włączanie/wyłączanie cyklicznej aktualizacji; wprowadzanie czasu cyklu w sekundach, z jakim ma być wykonywana cykliczna aktualizacja; w zależności od statusu zmienia się etykieta przycisku ("Refresh"/"Start"/"Stop").
[Refresh]	Aktualizacja wyświetlania; Przycisk jest widoczny tylko wtedy, gdy cykliczna aktualizacja nie jest włączona.
[Start]	Uruchomienie cyklicznej aktualizacji; Przycisk ten jest widoczny tylko wtedy, gdy cykliczna aktualizacja jest włączona, ale jeszcze nie została uruchomiona.
[Stop]	Zakończenie cyklicznej aktualizacji; Przycisk widoczny jest tylko wtedy, gdy cykliczna aktualizacja jest aktywna.

Cykliczną aktualizację można przeprowadzać tak długo, jak długo 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 wyświetlane są pod ustawieniami.

7.1.1.5.10 Strona „WAGO Device Access“

Na stronie „WAGO Device Access“ znajdują się ustawienia do uwierzytelniania przy skanowaniu węzła.

ⓘ Wskazówka

Beta-Status

W niniejszej wersji firmware'u funkcjonalność „WAGODevice Access“ znajduje się jeszcze w statusie beta!

Grupa „Unauthenticated Requests“

Tabela 231: Strona WBM „WAGO Device Access“ – grupa „Unauthenticated Requests“

Parametr	Znaczenie
Allow unauthenticated Device Scan	Tu definiuje się, czy możliwe jest skanowanie węzła bez uwierzytelnienia. W ustawieniach domyślnych uwierzytelnianie jest wyłączone. W celu zwiększenia poziomu bezpieczeństwa można wymusić uwierzytelnianie podczas skanowania węzła. W obecnym statusie beta podczas skanowania wykrywane są tylko jednostki główne (head stations), natomiast moduły I/O nie są rozpoznawane!
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

Grupa „CORS Configuration“

Tabela 232: Strona WBM „WAGO Device Access“ – grupa „CORS Configuration“

Parametr	Znaczenie	
CORS Policy	Wybór, z których źródeł (Origin) dozwolone jest wykonywanie zapytań „Cross-Origin“ do interfejsu REST API.	
	Allow all	Dostęp „Cross-Origin“ do REST API jest dozwolony ze wszystkich źródeł.

Parametr	Znaczenie	
	Allow all origins and null	Oprócz wszystkich standardowych wartości źródeł (Origin) dozwolona jest również wartość „null". Niektóre przeglądarki wykorzystują ją do oznaczenia, że strona internetowa jest hostowana z lokalnego systemu plików.
	Allow origins from whitelist	Dostęp do REST API powinien być możliwy wyłącznie z tych źródeł (Origins), które zostały ujęte na białej liście (whitelist). Uwaga: przy tym ustawieniu konieczne jest dodanie źródła (Origin) Twojej aplikacji do listy dozwolonych (Whitelist), w przeciwnym razie przeglądarka zablokuje dostęp do REST-API.
	None	Serwer WWW instruuje przeglądarkę, aby w ogóle nie wykonywała żadnych zapytań typu „Cross-Origin".
CORS Whitelist	Należy wpisać źródła (Origins) aplikacji, które mają mieć prawo do wykonywania zapytań typu „Cross-Origin" do interfejsu REST API. To pole edycji jest aktywne tylko wtedy, gdy jako wartość „CORS Policy" zaznaczono „Allow origins from whitelist".	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

7.1.1.6 Zakładka „Diagnostic"

7.1.1.6.1 Strona „Log Message Viewer"

Na stronie „Log Message Viewer" znajdują się ustawienia do wyświetlania komunikatów diagnostycznych.

Tabela 233: Strona WBM „Log Message Viewer" – grupa „Refresh Options"

Parametr	Znaczenie	
Read only the last	Włączanie/wyłączanie ostatnich n komunikatów; wprowadzanie liczby wyświetlanych komunikatów	
Automatic refresh interval (sec)	Włączanie/wyłączanie cyklicznej aktualizacji; wprowadzanie czasu cyklu w sekundach, z jakim ma być wykonywana cykliczna aktualizacja; w zależności od statusu zmienia się etykieta przycisku ("Refresh"/"Start"/"Stop").	
Source	Wybór źródła komunikatów diagnostycznych; Dostępne opcje na liście rozwijanej zależą od aktualnie zalogowanego użytkownika:	
	User	Tylko standardowe komunikaty diagnostyczne
	admin	Standardowe komunikaty diagnostyczne i wszystkie dane logowania w folderze `/var/log/*`
[Refresh]	Aktualizacja wyświetlania; Przycisk jest widoczny tylko wtedy, gdy cykliczna aktualizacja nie jest włączona.	
[Start]	Uruchomienie cyklicznej aktualizacji; Przycisk ten jest widoczny tylko wtedy, gdy cykliczna aktualizacja jest włączona, ale jeszcze nie została uruchomiona.	
[Stop]	Zakończenie cyklicznej aktualizacji; Przycisk widoczny jest tylko wtedy, gdy cykliczna aktualizacja jest aktywna.	

Cykliczną aktualizację można przeprowadzić tylko tak długo, jak otwarta jest strona „Diagnostic Information". Przy zmianie strony WBM aktualizacja zostaje zatrzymana do momentu, aż strona „Diagnostic" zostanie ponownie otwarta.

Komunikaty wyświetlane są pod ustawieniami.

7.1.1.6.2 Strona „Download“

Na stronie „Download" można pobrać dane diagnostyczne produktu.

Tabela 234: Strona WBM „Download" – grupa „Diagnostic Information"

Parametr	Znaczenie
[Download]	Pobieranie informacji diagnostycznych z urządzenia

Utworzony plik archiwum zawiera komunikaty dziennika zdarzeń, wersję firmware'u i listę zainstalowanych pakietów.

7.1.1.6.3 Strona „Network Capture“

Na stronie „Network Capture“ znajdują się ustawienia niezbędne do rejestracji i pobierania komunikacji sieciowej na urządzeniu. Wyświetlany jest aktualny status rejestracji sieci.

Grupa „State“

Tabela 235: Strona WBM „Network Capture“ – grupa „State“

Parametr	Znaczenie
Current State	Aktualny status zapisu sieci
Last Captured Package Count	Zapisane pakiety sieciowe
Last Refresh Time	Tu wyświetlany jest czas ostatniej aktualizacji Current State i Last Captured Package Count.

Grupa „Configuration“

Tabela 236: Strona WBM „Network Capture“ – grupa „Configuration“

Parametr	Znaczenie	
Enable	Włączanie/wyłączanie zapisu	
Rotate Log Files	Włączanie/wyłączanie rotacyjnego zapisu; Gdy ta opcja jest włączona, ruch sieciowy jest zapisywany w maksymalnie trzech plikach o określonym maksymalnym rozmiarze. Po osiągnięciu maksymalnego rozmiaru pierwszego pliku dane są nadal zapisywane w drugim pliku itd. Gdy również trzeci plik osiągnie maksymalny rozmiar, dane z pierwszego pliku zostają nadpisane.	
Max. Filesize	Wprowadzanie maksymalnego rozmiaru pliku dla zapisu danych	
Storage Location	Wybieranie lokalizacji zapisanych danych	
	Internal Flash	Dane są zapisywane w wewnętrznej pamięci.
	SD-Card	Dane zapisywane są na karcie pamięci. Jeśli wybrana jest opcja „SD-Card“, ale karta pamięci jest już wyjęta, opcja ta nie jest już aktywna i można wybrać tylko „Internal-Flash“.
Listen On Network Interface	Wybór interfejsu sieciowego, z którego ma być przechwytywany ruch sieciowy; do wyboru są dostępne interfejsy sieciowe urządzenia.	
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.	

Grupa „Filter Configuration“

Tabela 237: Strona WBM „Network Capture“ – grupa „Filter Configuration“

Parametr	Znaczenie
Capture Filter	Wprowadzenie filtrów zapisu; służą one do przechwytywania jedynie istotnego lub wybranego ruchu sieciowego. Na przykład możliwy jest zapis komunikacji tylko z określonego portu lub z konkretnego adresu IP. Więcej informacji na temat możliwych ustawień filtrów można znaleźć w objaśnieniach „Capture Filter" w dokumentacji „Wireshark.
[Check]	Sprawdzenie poprawności filtra przechwytywania „Capture Filter“
[Submit]	Zaakceptuj zmianę; zmiana zostanie zrealizowana natychmiast.

Grupa „Log Download“

Tabela 238: Strona WBM „Network Capture“ – grupa „Log Download“

Parametr	Znaczenie
Select Log File	Wybór zapisu, który ma zostać pobrany z urządzenia
[Download]	Pobieranie wybranego zapisu z urządzenia
[Download All]	Pobieranie wszystkich dostępnych zapisów z urządzenia

Spis tabel

Tabela 1 Strona WBM „Device Status“ – grupa „Device Details“ 14
Tabela 2 Strona WBM „Device Status“ – grupa „Network TCP/IP Details“ 14
Tabela 3 Strona WBM „PLC Runtime Information“ – grupa „Runtime“ 15
Tabela 4 Strona WBM „Clock“ – grupa „Timezone and Format“ 15
Tabela 5 Strona WBM „Configuration of NTP Client“ – grupa „NTP Client Configuration“ 15
Tabela 6 Priorytety CODESYS V3 17
Tabela 7 Strona WBM „PLC Runtime Configuration” – grupa „General PLC Runtime Configuration“ 17
Tabela 8 Strona WBM „PLC Runtime Configuration” – grupa „Webserver Configuration“ 18
Tabela 9 Strona WBM „PLC Runtime Services“ – grupa „CODESYS V3“ 18
Tabela 10 Strona WBM „Controls Settings“ – grupa „OMS Controls“ 19
Tabela 11 Strona WBM „Configuration of Serial Interface" – grupa „Current Serial Interface Configuration" 21
Tabela 12 Strona WBM „Configuration of Serial Interface” – grupa „Assign Owner of Serial Interface“ 21
Tabela 13 Strona WBM „Configuration of Serial Interface“ – grupa „Assign Mode of Serial Interface“ 21
Tabela 14 Strona WBM „Configuration of Serial Interface" – grupa „Current Serial Interface Configuration" 22
Tabela 15 Strona WBM „Configuration of Serial Interface" – grupa "Bus Termination" 22
Tabela 16 Strona WBM „Configuration of Serial Interface" – grupa "Bias Network" 22
Tabela 17 Strona WBM „Configuration of Service Interface” – grupa „ Assign Owner of Service Interface“ 23
Tabela 18 Strona WBM „Ethernet Configuration“ – grupa „Bridge Configuration“ 24
Tabela 19 Strona WBM „Ethernet Configuration“ – grupa „Dummy Interfaces“ 24
Tabela 20 Strona WBM „Ethernet Configuration“ – grupa „VLAN Interfaces“ 24
Tabela 21 Strona WBM „Ethernet Configuration“ – grupa „Port Mirror Settings“ 25
Tabela 22 Strona WBM „Ethernet Configuration“ – grupa „Storm Control Settings“ 25
Tabela 23 Strona WBM „Ethernet Configuration“ – grupa „Storm Control Settings“ 25
Tabela 24 Strona WBM „Ethernet Configuration“ – grupa „Storm Control Settings“ 25
Tabela 25 Strona WBM „Ethernet Configuration“ – grupy „Ethernet Interface Configuration“ 25
Tabela 26 Strona WBM „Ethernet Configuration“ – grupy „Ethernet Interface Configuration“ 26
Tabela 27 Strona WBM „TCP/IP Configuration“ – grupa „Bridge Interfaces“ 27
Tabela 28 Strona WBM „TCP/IP Configuration“ – grupa „Dummy Interfaces“ 27
Tabela 29 Strona WBM „TCP/IP Configuration“ – grupa „VLAN Interfaces“ 27
Tabela 30 Strona WBM „TCP/IP Configuration“ – grupa „DNS Server“ 28
Tabela 31 Strona WBM „Configuration of Host and Domain Name“ – grupa „Hostname“ 28
Tabela 32 Strona WBM „Configuration of Host and Domain Name“ – grupa „Domain Name“ 29
Tabela 33 Strona WBM „Routing“ – grupa „IP Forwarding through multiple interfaces“ 30
Tabela 34 Strona WBM „Routing“ – grupa „Custom Routes“ 31

Tabela 35 Strona WBM „Routing" – grupa „Dynamic Routes (assigned by DHCP)" ... 32
Tabela 36 Strona WBM „Routing" – grupa „IP-Masquerading" ... 33
Tabela 37 Strona WBM „Routing" – grupa „Port Forwarding" ... 33
Tabela 38 Usługi i użytkownicy ... 34
Tabela 39 Użytkownik Linux® ... 34
Tabela 40 Strona WMB „Users Configuration" – grupa „Change Passwords" ... 35
Tabela 41 Strona WBM „Security Settings" – grupa „TLS Configuration" ... 36
Tabela 42 Strona WBM „General Firewall Configuration" – grupa „Global Firewall Parameter" ... 37
Tabela 43 Strona WBM „Interface Configuration" – grupa „Firewall Configuration Bridge <n> / VPN / WAN" ... 37
Tabela 44 Porty dla funkcjonalności telecontrol ... 38
Tabela 45 Strona WBM „Configuration of MAC address filter" – grupa „Global MAC address filter state" ... 38
Tabela 46 Strona WBM „Configuration of MAC address filter" – grupa „MAC address filter state Bridge <n>" ... 38
Tabela 47 Strona WBM „Configuration of MAC address filter" – grupa „MAC address filter whitelist" ... 38
Tabela 48 Strona WBM „Configuration of User Filter" – grupa „User filter" ... 39
Tabela 49 Lista parametrów wysyłanych przez DHCP ... 40
Tabela 50 Strona WBM „DHCP Server Configuration" – grupa „DHCP Configuration Bridge <n>" ... 41
Tabela 51 Strona WBM „Configuration of DNS Server" – grupa „DNS Server" ... 42
Tabela 52 Strona WBM „Configuration of General SNMP Parameter" – grupa „General SNMP Configuration" ... 42
Tabela 53 Strona WBM „Configuration of SNMP v1/v2c Parameters" – grupa „Communities" ... 43
Tabela 54 Strona WBM „Configuration of SNMP v1/v2cparameters" – grupa „Trap Receivers" ... 43
Tabela 55 Strona WBM „Configuration of SNMP v3 Parameters" – grupa „User" ... 44
Tabela 56 Strona WBM „Configuration of SNMP v3 Parameters" – grupa „Trap Receivers" ... 45
Tabela 57 Strona WBM „Configuration of Network Services" – grupa „FTP" ... 45
Tabela 58 Strona WBM „Configuration of Network Services" – grupa „FTPES (explicit FTPS)" ... 45
Tabela 59 Strona WBM „Configuration of Network Services" – grupa „HTTP" ... 45
Tabela 60 Strona WBM „Configuration of Network Services" – grupa „HTTPS" ... 46
Tabela 61 Strona WBM „Configuration of Network Services" – grupa „I/O-CHECK" ... 46
Tabela 62 Strona WBM „SSH Server Settings" – grupa „SSH Server" ... 46
Tabela 63 Strona WBM „Docker Settings" – grupa „Docker Status" ... 46
Tabela 64 Komponenty pakietu oprogramowania Cloud Connectivity ... 48
Tabela 65 Strona WBM „Overview" – grupa „Connection <n>" ... 48
Tabela 66 Strona WBM „Configuration of Connection <n>" – grupa „Configuration" ... 48
Tabela 67 Zależności między polami wyboru i edycji a poszczególnymi platformami chmury ... 50
Tabela 68 Możliwość wyboru protokołu danych dla poszczególnych platform chmury ... 51
Tabela 69 Zależności między polami wyboru i edycji a poszczególnymi protokołami danych ... 51

Tabela 70 Możliwość wyboru trybu pamięci podręcznej zależnie od wybranego protokołu danych 51
Tabela 71 Zależności między polami wyboru i edycji a poszczególnymi uwierzytelnieniami..... 52
Tabela 72 Strona WBM „OPC UA Configuration“ – grupa „OPC UA Server Configuration“..... 52
Tabela 73 Strona WBM „OPC UA Configuration“ – grupa „OPC UA Server Security Settings“..... 52
Tabela 74 Strona WBM „BACnet Status” – grupa „BACnet Information“..... 53
Tabela 75 Strona WBM „BACnet Status” – grupa „BACnet License“..... 54
Tabela 76 Strona WBM „BACnet Status" – grupa „BACnet Data Link" 54
Tabela 77 Strona WBM „BACnet Configuration“ – grupa „PLC Runtime“ 54
Tabela 78 Strona WBM „BACnet Configuration” – grupa „BACnet Service“ 54
Tabela 79 Strona WBM „BACnet Configuration“ – grupa „BACnet Data“..... 54
Tabela 80 Strona WBM „BACnet Configuration" – grupa „BACnet Log Level" 55
Tabela 81 Strona WBM „BACnet Configuration“ – grupa „BACnet Network Capture“ 55
Tabela 82 Strona WBM „BACnet Data Link" – grupa „BACnet Restart"..... 55
Tabela 83 Strona WBM „BACnet Data Link" – grupa „BACnet/IP" 55
Tabela 84 Strona WBM „BACnet Data Link" – grupa „BACnet/SC" 56
Tabela 85 Strona WBM „BACnet Data Link" – grupa „BACnet/SC Certificate Authority (CA)"..... 56
Tabela 86 Strona WBM „BACnet Data Link" – grupa „BACnet/SC Certificate"..... 56
Tabela 87 Strona WBM „BACnet Configuration" – grupa „BACnet/SC Certificate Signing Request (CSR)" 56
Tabela 88 Strona WBM „BACnet Data Link" – grupa „BACnet/SC Default Certificates"..... 57
Tabela 89 Strona WBM „BACnet Storage Location” – grupa „BACnet Persistence“ 57
Tabela 90 Strona WBM „BACnet Storage Location” – grupa „BACnet Trendlog“..... 57
Tabela 91 Strona WBM „BACnet Storage Location” – grupa „BACnet Eventlog“ 57
Tabela 92 Przegląd adresów w katalogu obiektów..... 58
Tabela 93 Indeksowanie zmiennych „IEC 61131-3“ w katalogu obiektów 63
Tabela 94 Dostęp od strony sieci obiektowej do danych wyjściowych PFC..... 64
Tabela 95 Przykłady dla dostępów w CODESYS do zmiennych PFC..... 65
Tabela 96 Maksymalne indeksy i subindeksy zmiennych „IEC 61131-3“ 65
Tabela 97 Przykład dla zmiennych wyjściowych „IEC 61131-3“..... 66
Tabela 98 Strona WBM „Firmware Backup“ – grupa „Firmware Backup“ 68
Tabela 99 Strona WBM „Firmware Restore“ – grupa „Firmware Restore“..... 70
Tabela 100 Ładowanie projektu bootowalnego..... 72
Tabela 101 Przegląd kodów błędu LED „I/O“..... 73
Tabela 102 Kod błędu 1 – Błąd sprzętu i konfiguracji: znaczenie kodów migania i środki zaradcze 73
Tabela 103 Kod błędu 2 – Błąd konfiguracji: znaczenie kodu migania i sposoby usuwania błędu 75
Tabela 104 Kod błędu 3 – Błąd protokołu magistrali systemowej: znaczenie kodu migania i sposoby usuwania błędu 75
Tabela 105 Kod błędu 4 – Fizyczny błąd magistrali systemowej: znaczenie kodów migania i sposoby usuwania błędów 75

Tabela 106 Kod błędu 5 – Błąd inicjalizacji magistrali systemowej: znaczenie kodów migania i sposoby usuwania błędów ... 76
Tabela 107 Kod błędu 7 – Niewspierany moduł I/O: znaczenie kodów migania i sposoby usuwania błędów ... 76
Tabela 108 Kod błędu 9 – Błąd wyjątku CPU: znaczenie kodu migania i sposoby usuwania błędu ... 76
Tabela 109 Przegląd kodów błędu LED „MS" ... 76
Tabela 110 Kod błędu 1 – Błąd konfiguracji: znaczenie kodu migania i sposoby usuwania błędu ... 76
Tabela 111 Strona WBM „Log Message Viewer" – grupa „Refresh Options" ... 77
Tabela 112 Strona WBM „Download" – grupa „Diagnostic Information" ... 77
Tabela 113 Strona WBM „Network Capture" – grupa „State" ... 77
Tabela 114 Strona WBM „Network Capture" – grupa „Configuration" ... 77
Tabela 115 Strona WBM „Network Capture" – grupa „Filter Configuration" ... 78
Tabela 116 Strona WBM „Network Capture" – grupa „Log Download" ... 78
Tabela 117 Fabryczne ustawienie dla adresowania IP interfejsu ETHERNET ... 80
Tabela 118 Maska sieci 255.255.255.0 ... 80
Tabela 119 Przełączanie adresów ... 83
Tabela 120 Prawa dostępu dla stron WBM ... 89
Tabela 121 Prawa dostępu dla stron WBM ... 98
Tabela 122 Strona WBM „Device Status" – grupa „Device Details" ... 100
Tabela 123 Strona WBM „Device Status" – grupa „Network TCP/IP Details" ... 100
Tabela 124 Strona WBM „PLC Runtime Information" – grupa „Runtime" ... 101
Tabela 125 Strona WBM „PLC Runtime Configuration" – grupa „General PLC Runtime Configuration" ... 101
Tabela 126 Strona WBM „PLC Runtime Configuration" – grupa „Webserver Configuration" ... 102
Tabela 127 Strona WBM „TCP/IP Configuration" – grupa „Bridge Interfaces" ... 103
Tabela 128 Strona WBM „TCP/IP Configuration" – grupa „Dummy Interfaces" ... 103
Tabela 129 Strona WBM „TCP/IP Configuration" – grupa „VLAN Interfaces" ... 104
Tabela 130 Strona WBM „TCP/IP Configuration" – grupa „DNS Server" ... 104
Tabela 131 Strona WBM „Ethernet Configuration" – grupa „Bridge Configuration" ... 104
Tabela 132 Strona WBM „Ethernet Configuration" – grupa „Dummy Interfaces" ... 105
Tabela 133 Strona WBM „Ethernet Configuration" – grupa „VLAN Interfaces" ... 105
Tabela 134 Strona WBM „Ethernet Configuration" – grupa „Port Mirror Settings" ... 105
Tabela 135 Strona WBM „Ethernet Configuration" – grupa „Storm Control Settings" ... 106
Tabela 136 Strona WBM „Ethernet Configuration" – grupa „Storm Control Settings" ... 106
Tabela 137 Strona WBM „Ethernet Configuration" – grupa „Storm Control Settings" ... 106
Tabela 138 Strona WBM „Ethernet Configuration" – grupy „Ethernet Interface Configuration" ... 106
Tabela 139 Strona WBM „Ethernet Configuration" – grupy „Ethernet Interface Configuration" ... 107
Tabela 140 Strona WBM „Configuration of Host and Domain Name" – grupa „Hostname" ... 107
Tabela 141 Strona WBM „Configuration of Host and Domain Name" – grupa „Domain Name" ... 108

Tabela 142 Strona WBM „Routing“ – grupa „IP Forwarding through multiple interfaces“ 108
Tabela 143 Strona WBM „Routing“ – grupa „Custom Routes“ 108
Tabela 144 Strona WBM „Routing“ – grupa „IP-Masquerading“ 109
Tabela 145 Strona WBM „Routing“ – grupa „Port Forwarding“ 110
Tabela 146 Strona WBM „Spanning Tree Protocol" – grupa „Status" 110
Tabela 147 Strona WBM „Spanning Tree Protocol" – grupa „Parameter Settings" 111
Tabela 148 Strona WBM „Clock“ – grupa „Timezone and Format“ 112
Tabela 149 Strona WMB „Clock“ – grupa „UTC Time and Date“ 113
Tabela 150 Strona WMB „Clock“ – grupa „Local Time and Date“ 113
Tabela 151 Strona WBM „Configuration of Serial Interface" – grupa „Current Serial Interface Configuration" 113
Tabela 152 Strona WBM „Configuration of Serial Interface“ – grupa „Assign Mode of Serial Interface“ 114
Tabela 153 Strona WBM „Configuration of Serial Interface” – grupa „Assign Owner of Serial Interface“ 114
Tabela 154 Strona WBM „Configuration of Serial Interface" – grupa „Current Serial Interface Configuration" 114
Tabela 155 Strona WBM „Configuration of Serial Interface" – grupa "Bus Termination" 114
Tabela 156 Strona WBM „Configuration of Serial Interface" – grupa "Bias Network" 115
Tabela 157 Strona WBM „Configuration of Service Interface” – grupa „ Assign Owner of Service Interface“ 115
Tabela 158 Strona WBM „Create bootable Image” – grupa „Create bootable image from boot device“ 115
Tabela 159 Strona WBM „Firmware Backup“ – grupa „Firmware Backup“ 116
Tabela 160 Strona WBM „Firmware Restore“ – grupa „Firmware Restore“ 118
Tabela 161 Strona WBM „Active System“ – grupa „Boot Device" 119
Tabela 162 Strona WBM „Active System“ – grupa „System <n> (Internal Flash)“ 119
Tabela 163 Strona WBM „Mass Storage“ – grupa „Devices" 120
Tabela 164 Strona WBM „Mass Storage“ – grupa "Create new Filesystem on Memory Card“ 120
Tabela 165 Strona WBM „Software Uploads“ – grupa „Upload new Software“ 120
Tabela 166 Strona WBM „Configuration of Network Services“ – grupa „FTP“ 121
Tabela 167 Strona WBM „Configuration of Network Services“ – grupa „FTPES (explicit FTPS)“ 121
Tabela 168 Strona WBM „Configuration of Network Services“ – grupa „HTTP“ 121
Tabela 169 Strona WBM „Configuration of Network Services“ – grupa „HTTPS“ 122
Tabela 170 Strona WBM „Configuration of Network Services“ – grupa „I/O-CHECK“ 122
Tabela 171 Strona WBM „Configuration of NTP Client“ – grupa „NTP Client Configuration“ 122
Tabela 172 Strona WBM „PLC Runtime Services“ – grupa „CODESYS V3“ 123
Tabela 173 Strona WBM „SSH Server Settings“ – grupa „SSH Server“ 123
Tabela 174 Strona WBM „DHCP Server Configuration“ – grupa „DHCP Configuration Bridge <n>“ 124
Tabela 175 Strona WBM „Configuration of DNS Server“ – grupa „DNS Server“ 124
Tabela 176 Strona WBM „Overview“ – grupa „Connection <n>“ 125
Tabela 177 Strona WBM „Configuration of Connection <n>“ – grupa „Configuration“ 125

Tabela 178 Zależności między polami wyboru i edycji a poszczególnymi platformami chmury 127
Tabela 179 Możliwość wyboru protokołu danych dla poszczególnych platform chmury 128
Tabela 180 Zależności między polami wyboru i edycji a poszczególnymi protokołami danych 128
Tabela 181 Możliwość wyboru trybu pamięci podręcznej zależnie od wybranego protokołu danych 129
Tabela 182 Zależności między polami wyboru i edycji a poszczególnymi uwierzytelnieniami 129
Tabela 183 Strona WBM „Controls Settings“ – grupa „OMS Controls“ 129
Tabela 184 Strona WBM „Configuration of General SNMP Parameter“ – grupa „General SNMP Configuration“ 130
Tabela 185 Strona WBM „Configuration of SNMP v1/v2c Parameters“ – grupa „Communities“ 130
Tabela 186 Strona WBM „Configuration of SNMP v1/v2cparameters" – grupa „Trap Receivers" 130
Tabela 187 Strona WBM „Configuration of SNMP v3 Parameters“ – grupa „User“ 131
Tabela 188 Strona WBM „Configuration of SNMP v3 Parameters“ – grupa „Trap Receivers“ 131
Tabela 189 Strona WBM „Commissioning Settings" – grupa „Commissioning" 132
Tabela 190 Strona WBM „Docker Settings“ – grupa „Docker Status“ 132
Tabela 191 Strona WMB „Users Configuration” – grupa „Change Passwords“ 133
Tabela 192 Strona WBM „OPC UA Configuration“ – grupa „OPC UA Server Configuration“ 133
Tabela 193 Strona WBM „OPC UA Configuration“ – grupa „OPC UA Server Security Settings“ 134
Tabela 194 Strona WBM „BACnet Status” – grupa „BACnet Information“ 135
Tabela 195 Strona WBM „BACnet Status” – grupa „BACnet License“ 135
Tabela 196 Strona WBM „BACnet Status" – grupa „BACnet Data Link" 135
Tabela 197 Strona WBM „BACnet Data Link" – grupa „BACnet Restart" 135
Tabela 198 Strona WBM „BACnet Configuration” – grupa „BACnet Service“ 135
Tabela 199 Strona WBM „BACnet Configuration“ – grupa „BACnet Data“ 136
Tabela 200 Strona WBM „BACnet Configuration" – grupa „BACnet Log Level" 136
Tabela 201 Strona WBM „BACnet Configuration“ – grupa „BACnet Network Capture“ 137
Tabela 202 Strona WBM „BACnet Data Link" – grupa „BACnet Restart" 137
Tabela 203 Strona WBM „BACnet Data Link" – grupa „BACnet/IP" 137
Tabela 204 Strona WBM „BACnet Data Link" – grupa „BACnet/SC" 137
Tabela 205 Strona WBM „BACnet Data Link" – grupa „BACnet/SC Certificate Authority (CA)" 138
Tabela 206 Strona WBM „BACnet Data Link" – grupa „BACnet/SC Certificate" 138
Tabela 207 Strona WBM „BACnet Configuration" – grupa „BACnet/SC Certificate Signing Request (CSR)" 138
Tabela 208 Strona WBM „BACnet Data Link" – grupa „BACnet/SC Default Certificates" 138
Tabela 209 Strona WBM „BACnet Storage Location” – grupa „BACnet Persistence“ 139
Tabela 210 Strona WBM „BACnet Storage Location” – grupa „BACnet Trendlog“ 139
Tabela 211 Strona WBM „BACnet Storage Location” – grupa „BACnet Eventlog“ 139
Tabela 212 Strona WBM „BACnet Info" – grupa „Refresh Options" 139
Tabela 213 Strona WBM „BACnet Info" – grupa „BACnet/IP Statistics" 140

Tabela 214 Strona WBM „BACnet Info" – grupa „BACnet/SC Statistics" ... 140
Tabela 215 Strona WBM „BACnet Info" – grupa „BACnet/SC Connections" ... 140
Tabela 216 Strona WBM „OpenVPN / IPsec" – grupa „OpenVPN" ... 141
Tabela 217 Strona WBM „OpenVPN / IPsec" – grupa „IPsec" ... 141
Tabela 218 Strona WBM „General Firewall Configuration" – grupa „Global Firewall Parameter" ... 142
Tabela 219 Strona WBM „Interface Configuration" – grupa „Firewall Configuration Bridge <n> / VPN / WAN" ... 142
Tabela 220 Porty dla funkcjonalności telecontrol ... 143
Tabela 221 Strona WBM „Configuration of MAC address filter" – grupa „Global MAC address filter state" ... 144
Tabela 222 Strona WBM „Configuration of MAC address filter" – grupa „MAC address filter state Bridge <n>" ... 144
Tabela 223 Strona WBM „Configuration of MAC address filter" – grupa „MAC address filter whitelist" ... 144
Tabela 224 Strona WBM „Configuration of User Filter" – grupa „User filter" ... 145
Tabela 225 Strona WBM „Certificates" – grupa „Installed Certificates" ... 145
Tabela 226 Strona WBM „Certificates" – grupa „Installed Private Keys" ... 146
Tabela 227 Strona WBM „Boot mode configuration" – grupa „Force internal boot" ... 146
Tabela 228 Strona WBM „Security Settings" – grupa „TLS Configuration" ... 147
Tabela 229 Strona WBM „Advanced Intrusion Detection Environment (AIDE)" – grupa „Run AIDE check at startup" ... 147
Tabela 230 Strona WBM „Advanced Intrusion Detection Environment (AIDE)" – grupa „Control AIDE and show log" ... 147
Tabela 231 Strona WBM „WAGO Device Access" – grupa „Unauthenticated Requests" ... 148
Tabela 232 Strona WBM „WAGO Device Access" – grupa „CORS Configuration" ... 148
Tabela 233 Strona WBM „Log Message Viewer" – grupa „Refresh Options" ... 149
Tabela 234 Strona WBM „Download" – grupa „Diagnostic Information" ... 150
Tabela 235 Strona WBM „Network Capture" – grupa „State" ... 150
Tabela 236 Strona WBM „Network Capture" – grupa „Configuration" ... 150
Tabela 237 Strona WBM „Network Capture" – grupa „Filter Configuration" ... 151
Tabela 238 Strona WBM „Network Capture" – grupa „Log Download" ... 151

Spis ilustracji

Ilustracja 1 Złącze komunikacyjne, terminator sieci i terminacja bias 22
Ilustracja 2 Okno przeglądarki WBM (przykład) 23
Ilustracja 3 Wiesz nagłówkowy WBM z niewyświetlanymi zakładkami (przykład) 23
Ilustracja 4 Wiersz statusu WBM (przykład) 24
Ilustracja 5 Podłączenie sterownika do usługi chmury (przykład) 47
Ilustracja 6 WAGO Ethernet Settings – ekran startowy (przykład) 82
Ilustracja 7 WAGO Ethernet Settings – zakładka „Network“ (przykład) 82
Ilustracja 8 Przykład testu działania 85
Ilustracja 9 Okno logowania 87
Ilustracja 10 Okno przeglądarki WBM (przykład) 88
Ilustracja 11 Wiesz nagłówkowy WBM z niewyświetlanymi zakładkami (przykład) 88
Ilustracja 12 Wiersz statusu WBM (przykład) 88
Ilustracja 13 „WAGO Ethernet Settings“ – ekran startowy (przykład) 91
Ilustracja 14 „WAGO Ethernet Settings“ – konfiguracja połączeń komunikacyjnych (przykład) 91
Ilustracja 15 „WAGO Ethernet Settings“ – zakładka Identification (przykład) 92
Ilustracja 16 „WAGO Ethernet Settings“ – zakładka Network (przykład) 92
Ilustracja 17 „WAGO Ethernet Settings“ – zakładka Protokół (przykład) 93
Ilustracja 18 „WAGO Ethernet Settings“ – zakładka Status (przykład) 93

WAGO GmbH & Co. KG
Postfach 2880 · D - 32385 Minden
Hansastraße 27 · D - 32423 Minden
info@wago.com
www.wago.com

Centrala	+49 (0) 571/887 – 0
Dział sprzedaży	+49 (0) 571/887 – 44 222
Zamówienia	+49 (0) 571/887 – 44 333

Znak WAGO jest zastrzeżonym znakiem towarowym spółki WAGO Verwaltungsgesellschaft mbH.
Copyright – WAGO GmbH & Co. KG – Wszelkie prawa zastrzeżone. Treść i struktura strony internetowej, katalogów, filmów oraz innych utworów WAGO są objęte prawami autorskimi. Rozpowszechnianie i zmiana treści stron oraz filmów są niedozwolone. Ponadto treści te nie mogą być ani kopiowane w celach komercyjnych, ani udostępniane osobom trzecim. Ochroną prawa autorskiego są objęte również zdjęcia i filmy, które zostały udostępnione WAGO GmbH & Co. KG przez osoby trzecie.“