WAGO TECHDOCS

Podręcznik

WAGO Edge Controller

752-8303/8000-0002

Wersja 1.4.0, ważna od wersji firmware'u 04.04.xx(26)

© 2024 WAGO GmbH & Co. KG
Wszystkie prawa zastrzeżone.

WAGO GmbH & Co. KG

Hansastraße 27
D-32423 Minden

Tel.: +49 (0) 571/8 87 – 0
Faks: +49 (0) 571/8 87 – 844 169

e-mail: info@wago.com

Strona www: www.wago.com

Wsparcie techniczne PL

Tel.: +49 (0) 571/8 87 – 4 45 55
Faks: +49 (0) 571/8 87 – 84 45 55

e-mail: support@wago.com

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

e-mail: documentation@wago.com

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

Znak WAGO jest zarejestrowanym znakiem towarowym spółki WAGO Verwaltungsgesellschaft mbH.

Spis treści

1 Informacje ogólne 8
1.1 Zakres obowiązywania 8
1.2 Komplet dokumentacji 8
1.3 Prawa autorskie 8
1.4 Prawa własności 9
1.5 Symbole 11
1.6 Zastosowane systemy liczbowe 12
1.7 Sposoby zapisu 12
1.8 Podstawy prawne 13
1.8.1 Zastrzeżenie prawa do zmian technicznych 13
1.8.2 Kwalifikacje personelu 13
1.8.3 Użytkowanie zgodne z przeznaczeniem 13
1.8.3.1 Użytkowanie niezgodne z przeznaczeniem 13
1.8.3.2 Gwarancja i odpowiedzialność 14
1.8.3.3 Obowiązki instalatora/operatora 14

2 Bezpieczeństwo 15
2.1 Wskazówki dotyczące bezpieczeństwa 15
2.2 Specjalne warunki zastosowania 17

3 Przegląd 18

4 Właściwości 19
4.1 Widok 19
4.2 Nadruk 20
4.3 Złącza 22
4.3.1 Złącza z przodu obudowy 22
4.3.2 Złącza u góry 22
4.3.3 „X1“ i „X2“ – złącza ETHERNET 23
4.3.4 „X3“ – złącze szeregowe RS-232/-485 23
4.3.4.1 Praca jako interfejs RS-232 24
4.3.4.2 Praca jako interfejs RS-485 24
4.3.5 „X4“ – złącze CAN 25
4.3.6 „X5“ – złącze zasilające POWER 26
4.3.7 „X6“ i „X7“ – złącza USB 2.0 26
4.3.8 „X8“ – wyjście Lineout na słuchawki 26
4.3.9 „X9“ – złącze HDMI typ A 26
4.3.10 „X10“ – złącze USB C 27
4.3.11 „X11“ – 4 dwustanowe wejścia i wyjścia DIO 27
4.3.12 „µSD“ – gniazdo karty pamięci 28
4.4 Zegar czasu rzeczywistego 29
4.5 Elementy sygnalizacyjne 30
4.5.1 LED statusu 30
4.6 Elementy obsługi 31
4.6.1 Przełącznik trybu pracy 31
4.6.2 Przycisk „CFG/RST“ 31
4.7 Schemat połączeń wewnętrznych 32
4.8 Dane techniczne 33

4.8.1 Urządzenie ... 33
4.8.2 Warunki klimatyczne ... 33
4.8.3 Zasilanie ... 33
4.8.4 Sprzęt ... 34
4.8.5 Komunikacja ... 34
4.8.6 Złącza ... 34
4.8.7 Złącza ... 35
4.9 Aprobaty ... 36
4.10 Normy i dyrektywy ... 36

5 Funkcje ... 37

5.1 Przeglądarka internetowa ... 37
5.2 Monitorowanie połączenia ... 38
5.3 WBM do konfiguracji i parametryzacji ... 38
5.4 Sieć ... 38
5.4.1 Konfiguracja złącz ... 38
5.4.1.1 Praca przy rozłączonych interfejsach sieciowych ... 38
5.4.2 Bezpieczeństwo sieci ... 38
5.4.2.1 Użytkownicy (User) i hasła ... 38
5.4.2.2 Usługi i użytkownicy ... 39
5.4.2.3 Grupa użytkowników WBM ... 39
5.4.2.4 Grupa użytkowników Linux® ... 40
5.4.2.5 Grupa użytkowników SNMP ... 41
5.4.2.6 Uwierzytelnianie serwera WWW ... 41
5.4.2.7 Szyfrowanie TLS ... 41
5.4.3 Konfiguracja sieci ... 42
5.4.3.1 Nazwa hosta/nazwa domeny ... 42
5.4.3.2 Bramy domyślne ... 42
5.5 Funkcje karty pamięci ... 43
5.5.1 Backup ... 43
5.5.2 Restore ... 43
5.5.3 Create Image ... 44
5.6 Doinstalowanie oprogramowania ... 44
5.7 Bootowanie ... 45
5.8 Elementy oprogramowania wymagające licencji ... 47

6 Montaż ... 48

6.1 Wytyczne i normy dotyczące instalacji ... 48
6.2 Pozycje montażowe ... 48
6.3 Montaż na szynie ... 49

7 Montaż przewodów ... 50

7.1 Uziemienie ... 50
7.2 Podłączanie urządzeń ... 50
7.3 Podłączanie napięcia zasilającego ... 51

8 Uruchamianie ... 52

8.1 Włączanie ... 52
8.2 Logowanie ... 52
8.3 Ustalanie adresu IP hosta ... 52
8.4 Ustawianie adresu IP ... 52

8.4.1 Połączenie IP przez USB 53
8.4.2 Zmiana adresu IP przy użyciu „WAGO Ethernet Settings“ 53
8.4.3 Czasowe ustawienie stałego adresu IP 55
8.4.4 Ustawianie adresu IP przez WMB 56
8.4.5 Przydzielanie adresu IP przy pomocy DHCP 56
8.5 Wyzwalanie funkcji RESET 57
8.5.1 Gorący reset 57
8.5.2 Zimny reset 57
8.5.3 Reset programowy (restart) 58
8.5.4 Factory Reset 58
8.6 Konfiguracja w systemie zarządzania przez WWW (WBM) 60
8.6.1 Zarządzanie użytkownikami WBM 62
8.6.2 Ogólne informacje o stronie 67
8.6.3 Funkcja Reboot 69

9 Środowisko systemowe CODESYS V3 70

9.1 Wskazówki ogólne 70
9.2 Priorytety CODESYS V3 71
9.3 Zakresy pamięci w CODESYS V3 72
9.3.1 Pamięć programu i danych 72
9.3.2 Ograniczenie modułu 72
9.3.3 Pamięć RAM nieulotna 72
9.3.4 Dostęp do pliku z aplikacji IEC 72
9.3.5 Zmiana ustawień sieci przez aplikację IEC 73
9.3.6 EtherCAT 73

10 Diagnostyka 74

11 Serwis 75

11.1 Zmiana konfiguracji przy użyciu WBM 75
11.2 Zmiany firmware'u 76
11.2.1 Przeprowadzanie aktualizacji/aktualizacji wstecznej przy użyciu WAGOupload 77
11.2.2 Przeprowadzanie aktualizacji/aktualizacji wstecznej przy użyciu karty pamięci i WBM 78

12 Demontaż 79

12.1 Demontaż z szyny 79

13 Utylizacja 80

13.1 Sprzęt elektryczny i elektroniczny 80
13.2 Opakowanie 80

14 Akcesoria 82

15 Załącznik 83

15.1 Dialogi konfiguracyjne 83
15.1.1 Web Based Management (WBM) 83
15.1.1.1 Zakładka „Information“ 83
15.1.1.1.1 Strona „Device Status“ 83
15.1.1.1.2 Strona „Vendor Information“ 85
15.1.1.1.3 Strona „PLC Runtime Information“ 86
15.1.1.1.4 Strona „WAGO Software License Agreement“ 87

15.1.1.1.5 Strona „Open Source Licenses“ 88
15.1.1.1.6 Strona „WBM Third Party License Information“ 89
15.1.1.1.7 Strona „Trademarks Information“ 90
15.1.1.1.8 Strona „WBM Version“ 91
15.1.1.2 Zakładka „Configuration“ 92
15.1.1.2.1 Strona „PLC Runtime Configuration“ 92
15.1.1.2.2 Strona „TCP/IP Configuration“ 94
15.1.1.2.3 Strona „Ethernet Configuration“ 96
15.1.1.2.4 Strona „Configuration of Host and Domain Name“ 100
15.1.1.2.5 Strona „Routing“ 102
15.1.1.2.6 Strona „Clock Settings“ 107
15.1.1.2.7 Strona „Configuration of Serial Interface RS232/RS485“ 109
15.1.1.2.8 Strona „Configuration of Service Interface“ 111
15.1.1.2.9 Strona „Create bootable Image“ 112
15.1.1.2.10 Strona „Firmware Backup“ 113
15.1.1.2.11 Strona „Firmware Restore“ 115
15.1.1.2.12 Strona „Active System“ 117
15.1.1.2.13 Strona „Mass Storage“ 118
15.1.1.2.14 Strona „Software Uploads“ 119
15.1.1.2.15 Strona „Configuration of Network Services“ 120
15.1.1.2.16 Strona „Configuration of NTP Client“ 122
15.1.1.2.17 Strona „PLC Runtime Services“ 123
15.1.1.2.18 Strona „SSH Server Settings“ 124
15.1.1.2.19 Strona „DHCP Server Configuration“ 125
15.1.1.2.20 Strona „Configuration of DNS Server“ 126
15.1.1.2.21 Strona „Status overview“ 127
15.1.1.2.22 Strona „Configuration of Connection <n>“ 128
15.1.1.2.23 Strona „Configuration of General SNMP Parameters“ 135
15.1.1.2.24 Strona „Configuration of SNMP v1/v2c Parameters“ 136
15.1.1.2.25 Strona „Configuration of SNMP v3 Parameters“ 138
15.1.1.2.26 Strona „Favorites“ 142
15.1.1.2.27 Strona „Autostart“ 144
15.1.1.2.28 Strona „Monitoring“ 145
15.1.1.2.29 Strona „Browser Security“ 146
15.1.1.2.30 Strona „Docker Settings“ 147
15.1.1.2.31 Strona „Fonts“ 148
15.1.1.2.32 Strona „Display Orientation“ 149
15.1.1.2.33 Strona „Screensaver“ 150
15.1.1.2.34 Strona „WBM User Configuration“ 152
15.1.1.3 Zakładka „Fieldbus“ 153
15.1.1.3.1 Strona „OPC UA Configuration“ 153
15.1.1.3.2 Strona „BACnet Status“ 155
15.1.1.3.3 Strona „BACnet Configuration“ 156
15.1.1.3.4 Strona „BACnet Storage Location“ 158
15.1.1.3.5 Strona „BACnet Files“ 160
15.1.1.4 Zakładka „Security“ 161
15.1.1.4.1 Strona „OpenVPN / IPsec Configuration“ 161
15.1.1.4.2 Strona „General Firewall Configuration“ 163
15.1.1.4.3 Strona „Interface Configuration“ 164
15.1.1.4.4 Strona „Configuration of MAC address filter“ 166

15.1.1.4.5 Strona „Configuration of User Filter“ 169
15.1.1.4.6 Strona „Certificates“ 172
15.1.1.4.7 Strona „Boot mode configuration“ 173
15.1.1.4.8 Grupa „Security Settings“ 174
15.1.1.4.9 Strona „Advanced Intrusion Detection Environment (AIDE)“ . 175
15.1.1.4.10 Strona „WAGO Device Access“ 177
15.1.1.5 Zakładka „Diagnostic“ 178
15.1.1.5.1 Strona „Log Message Viewer“ 178
15.1.1.5.2 Strona „Download“ 179
15.1.1.5.3 Strona „Network Capture“ 180

Spis ilustracji 183

Indeks tabel 184

1 Informacje ogólne

Produkt WAGO można instalować i stosować wyłącznie zgodnie z zaleceniami zawartymi w tej dokumentacji.

Wskazówka

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

1.1 Zakres obowiązywania

Niniejsza dokumentacja dotyczy produktu 752-8303/8000-0002.

1.2 Komplet dokumentacji

Oprócz niniejszego podręcznika WAGO należy skorzystać również z następującej dokumentacji:

- WAGO I/O System 750, podręcznik do zastosowanego sterownika PLC
- WAGO I/O System 750, podręcznik „Cyber-Security dla sterowników PFC100/PFC200“
- Instrukcja migracji; migracja z ***e!****COCKPIT* do CODESYS V3.5
- Podręcznik dotyczący technologii „Industrial ETHERNET“

Dokumentacja ta udostępniona jest do pobrania na stronie internetowej www.wago.com.

Więcej informacji na temat CODESYS V3.5 można znaleźć w pomocy online CODESYS na stronie help.codesys.com (do ServicePack 17), a w nowej pomocy online na stronie de.helpme-codesys.com (aktualny ServicePack).

1.3 Prawa autorskie

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

1.4 Prawa własności

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

- Adobe® i Acrobat® są zarejestrowanymi markami Adobe Systems Inc.
- Android™ jest marką firmy Google LLC.
- Apple, logo Apple, iPhone, iPad i iPod touch są zarejestrowanymi znakami towarowymi firmy Apple Inc., zarejestrowanymi w Stanach Zjednoczonych i innych krajach. „App Store“ jest marką usługi zarejestrowanej przez Apple Inc.
- AS-Interface® jest zarejestrowaną marką AS-International Association e.V.
- BACnet® jest zarejestrowaną marką American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc. (ASHRAE).
- *Bluetooth*® jest zarejestrowanym znakiem towarowym Bluetooth SIG, Inc.
- CiA® i CANopen® są zarejestrowanymi markami CAN in AUTOMATION – International Users and Manufacturers Group e. V.
- CODESYS jest zarejestrowanym znakiem towarowym CODESYS Development GmbH.
- DALI jest zarejestrowaną marką Digital Illumination Interface Alliance (DiiA).
- EtherCAT® jest zarejestrowaną marką i opatentowaną technologią, licencjonowaną przez Beckhoff Automation GmbH, Niemcy.
- EtherNet/IP™ jest zarejestrowaną marką Open DeviceNet Vendor Association, Inc (ODVA).
- EnOcean® jest zarejestrowaną marką EnOcean GmbH.
- Google Play™ jest zarejestrowanym znakiem towarowym Google Inc.
- IO-Link jest zarejestrowaną marką PROFIBUS Nutzerorganisation e.V.
- KNX® jest zarejestrowaną marką KNX Association cvba.
- Linux® jest zarejestrowaną marką Linus Torvalds.
- LON® jest zarejestrowaną marką Echelon Corporation.
- Modbus® jest zarejestrowaną marką Schneider Electric, z licencją dla Modbus Organization, Inc.

- OPC UA jest zarejestrowaną marką OPC Foundation.
- PROFIBUS® jest zarejestrowaną marką PROFIBUS Nutzerorganisation e.V. (PNO).
- PROFINET® jest zarejestrowaną marką PROFIBUS Nutzerorganisation e.V. (PNO).
- QR Code jest zarejestrowaną marką DENSO WAVE INCORPORATED.
- Subversion® jest zarejestrowaną marką Apache Software Foundation.
- Windows® jest zarejestrowaną marką Microsoft Corporation.

1.5 Symbole

NIEBEZPIE-CZEŃSTWO

Ostrzeżenie przed obrażeniami ciała!
Oznaczenie bezpośredniego zagrożenia o wysokim stopniu ryzyka, które, jeśli nie zostanie wyeliminowane, może skutkować śmiercią lub poważnymi obrażeniami ciała.

NIEBEZPIE-CZEŃSTWO

Ostrzeżenie przed obrażeniami ciała spowodowanymi przez prąd elektryczny!
Oznaczenie bezpośredniego zagrożenia o wysokim stopniu ryzyka, które, jeśli nie zostanie wyeliminowane, może skutkować śmiercią lub poważnymi obrażeniami ciała.

OSTRZEŻENIE

Ostrzeżenie przed obrażeniami ciała!
Oznaczenie możliwego zagrożenia o średnim stopniu ryzyka, które, jeśli nie zostanie wyeliminowane, może skutkować śmiercią lub poważnymi obrażeniami ciała.

PRZESTROGA

Ostrzeżenie przed obrażeniami ciała!
Wskazanie na prawdopodobieństwo wystąpienia zagrożenia o niskim poziomie ryzyka, które, jeśli nie zostanie wyeliminowane, może spowodować niewielkie lub umiarkowane obrażenia ciała.

UWAGA

Ostrzeżenie przed szkodami materialnymi!
Wskazanie na prawdopodobieństwo wystąpienia zagrożenia, które, jeśli nie zostanie wyeliminowane, może doprowadzić do powstania szkód materialnych.

ESD

Ostrzeżenie przed szkodami materialnymi w następstwie wyładowań elektrostatycznych!
Wskazanie na prawdopodobieństwo wystąpienia zagrożenia, które, jeśli nie zostanie wyeliminowane, może doprowadzić do powstania szkód materialnych.

Wskazówka

Ważna wskazówka!
Wskazuje na prawdopodobieństwo nieprawidłowego funkcjonowania, która jednak, jeśli nie zostanie wyeliminowane, nie prowadzi do szkód materialnych.

Informacja

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

1.6 Zastosowane systemy liczbowe

Tabela 1: Zastosowane systemy liczbowe

System liczbowy	Przykład	Komentarz
Dziesiętny	100	Zwykły zapis
Szesnastkowy	0x64	Notacja szesnastkowa
Binarny	'100' '0110.0100'	Zapis w apostrofach, półbajt oddzielony kropką

1.7 Sposoby zapisu

Tabela 2: Sposoby zapisu

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

1.8 Podstawy prawne

1.8.1 Zastrzeżenie prawa do zmian technicznych

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

1.8.2 Kwalifikacje personelu

Wszystkie prace przy urządzeniach z serii 752 mogą być wykonywane wyłącznie przez wykwalifikowanych elektryków z odpowiednią wiedzą fachową w zakresie techniki automatyzacji. Osoby te muszą znać aktualne normy i wytyczne dotyczące AKPiA.

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

1.8.3 Użytkowanie zgodne z przeznaczeniem

Edge Controller przeznaczony jest do zastosowania w układach AKPiA. Można je wykorzystywać w aplikacjach mieszkaniowych, handlowych i przemysłowych. W każdym przypadku należy przestrzegać parametrów technicznych.

W budynkach mieszkalnych, handlowych i komercyjnych oraz małych przedsiębiorstwach nie wolno wykorzystywać portu HDMI.
W przemyśle dozwolone jest stosowanie portu HDMI.

Produkt jest urządzeniem o konstrukcji otwartej, przystosowanej do montażu w dodatkowej obudowie.
Produkt ma stopień ochrony IP20 i jest przeznaczony do zastosowania w suchych pomieszczeniach.

1.8.3.1 Użytkowanie niezgodne z przeznaczeniem

Użytkowanie produktu niezgodnie z jego przeznaczeniem jest niedozwolone. Użytkowanie niezgodne z przeznaczeniem ma miejsce w szczególności w następujących przypadkach:

- nieprzestrzeganie zasad użytkowania zgodnego z przeznaczeniem.
- użytkowanie bez środków ochronnych w środowisku, w którym może wystąpić wilgoć, woda słona, mgła solna, kurz, żrące opary, gazy, bezpośrednie promieniowanie słoneczne lub promieniowanie jonizujące.
- użytkowanie produktu w obszarach o szczególnym zagrożeniu, które wymagają bezawaryjnej pracy ciągłej i w których awaria lub eksploatacja może prowadzić do bezpośredniego zagrożenia życia, zdrowia,

uszkodzenia ciała lub też do znacznych szkód materialnych albo środowiskowych (np. eksploatacja elektrowni jądrowych, systemów uzbrojenia, statków powietrznych i pojazdów lądowych).

1.8.3.2 Gwarancja i odpowiedzialność

Obowiązują postanowienia Ogólnych Warunków Handlowych i umów dla dostaw i usług firmy WAGO Kontakttechnik GmbH Co. & KG oraz warunki dla oprogramowania i produktów ze zintegrowanym oprogramowaniem zawarte w umowie licencyjnej dla oprogramowania WAGO, które są dostępne na stronie: www.wago.com. Zgodnie z tym gwarancja traci ważność w szczególności, gdy:

- produkt jest używany w sposób niewłaściwy.
- wada dotyczy cech specjalnych (konfiguracji sprzętu i oprogramowania).
- modyfikacje sprzętu lub oprogramowania zostały wykonane przez użytkownika lub osoby trzecie, niewymienione w tej dokumentacji lub osoby, które przyczyniły się do powstania wady lub ją spowodowały.

W każdym przypadku nadrzędne pozostają ustalenia dotyczące poszczególnych umów.

1.8.3.3 Obowiązki instalatora/operatora

Odpowiedzialność za bezpieczeństwo instalacji lub systemu zbudowanego przy użyciu tego produktu spoczywa na instalatorze/operatorze. Odpowiada on za prawidłową instalację produktu i bezpieczeństwo w systemach. Instalator/operator musi przestrzegać obowiązujących ustaw, norm, rozporządzeń, przepisów lokalnych, przyjętych standardów i zasad techniki aktualnych w momencie instalacji oraz stosować się do zaleceń opisanych w instrukcji obsługi. Ponadto muszą być przestrzegane postanowienia dotyczące instalacji, określone w aprobatach. W przypadku, gdy nie są one dotrzymane, produkt nie może być stosowany w zakresach objętych aprobatą.

2 Bezpieczeństwo

2.1 Wskazówki dotyczące bezpieczeństwa

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

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

NIEBEZPIECZEŃSTWO

Nie pracować przy urządzeniach znajdujących się pod napięciem!
Niebezpieczne napięcie elektryczne może spowodować porażenie prądem elektrycznym i oparzenia.
Część instalacji, na której urządzenie ma być zamontowane lub zdemontowane, należy zawsze odłączyć od zasilania!

NIEBEZPIECZEŃSTWO

Stosować tylko źródło napięcia SELV!
Urządzenie należy stosować wyłącznie ze źródłem napięcia SELV (Safety Extra Low Voltage), spełniającym wymagania LPS (Limited Power Source) zgodnie z DIN EN 60950-1.

NIEBEZPIECZEŃSTWO

Przestrzegać przepisów dotyczących zapobiegania wypadkom!
W trakcie montażu, uruchamiania, eksploatacji, konserwacji i usuwania usterek należy zawsze przestrzegać przepisów dotyczących zapobiegania wypadkom, właściwych dla danej maszyny/instalacji (np. przepis 3 DGUV „Instalacje i urządzenia elektryczne“).

NIEBEZPIECZEŃSTWO

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

UWAGA

Przestrzegać stopnia ochrony IP!
Urządzenie jest urządzeniem „typu otwartego”, odpowiadającym stopniowi ochrony IP20. Jeśli środowisko pracy nie spełnia tych wymogów, należy umieścić urządzenie w szafie sterowniczej lub w obudowie.

UWAGA

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

UWAGA

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

UWAGA

Czyścić wyłącznie przy użyciu dozwolonych materiałów!
Obudowę i zabrudzone styki wolno czyścić wyłącznie przy użyciu propanolu.

UWAGA

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

UWAGA

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

ESD

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

2.2 Specjalne warunki zastosowania

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

- Komponentów systemu sterowania oraz sieci sterowniczych nie należy łączyć z otwartą siecią, na przykład Internetem lub siecią biurową. WAGO zaleca umieszczenie sieci sterowniczych za firewallem.
- Aby zredukować niebezpieczeństwo cyberataku i tym samym zwiększyć cyberbezpieczeństwo, wszystkie porty i usługi w komponentach systemu sterowania, które nie są wykorzystywane przez aplikację (np. CODESYS) należy zamykać.
  Porty i usługi dobrze jest otwierać tylko na czas uruchamiania lub konfiguracji.
- Fizyczny i elektroniczny dostęp do wszystkich komponentów automatyki należy ograniczyć do kręgu osób upoważnionych.
- Przed pierwszym uruchomieniem należy koniecznie zmienić ustawione standardowo hasła! W ten sposób redukuje się ryzyko ingerencji osób nieupoważnionych w system.
- Używane hasła należy regularnie zmieniać! W ten sposób redukuje się ryzyko ingerencji osób nieupoważnionych w system.
- Należy regularnie przeprowadzać analizę zagrożeń. Pozwala to na sprawdzenie, czy podjęte działania odpowiadają wymogom w zakresie ochrony.
- Przy projektowaniu instalacji należy zastosować mechanizmy „Defense-in-depth“ w celu ograniczenia dostępu do indywidualnych produktów i sieci oraz ich kontroli.

Wskazówka

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

Aby chronić dane, należy stosować metody ich szyfrowania oraz przestrzegać zaleceń Federalnego Urzędu ds. Bezpieczeństwa w zakresie techniki informatycznej, zawartych w publikacji „Cloud: Risiken und Sicherheitstipps“.
Należy uwzględnić zalecenia odpowiednich organów, zawarte w porównywalnych publikacjach na terenie kraju użytkownika.

3 Przegląd

Sterownik łączy w sobie funkcje HMI i sterownika, dzięki czemu może zastąpić sterownik PLC. W sterowniku działa zarówno oprogramowanie wizualizacyjne, jak i runtime. Przeznaczony jest on do montażu na szynie i wykorzystuje różne interfejsy.

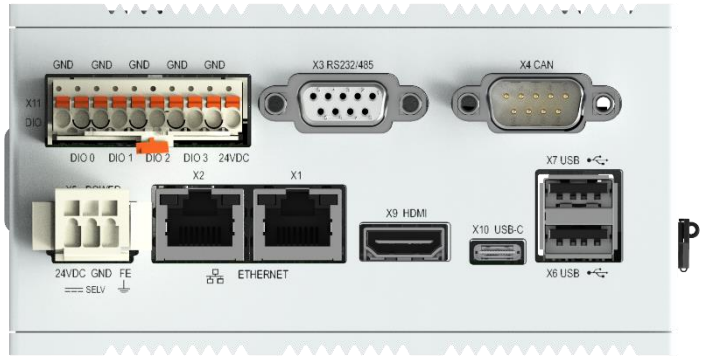
Wśród złącz dostępne są: złącze sieci ETHERNET, USB i microSD, Lineout (wyjście do słuchawek) i HDMI.

Złącza obejmują ponadto dwustanowe wejścia i wyjścia, interfejs RS-232/RS-485 i CAN, służące do podłączania dodatkowych wejść/wyjść.

Sterownik ma także NVRAM.

4 Właściwości

4.1 Widok



Ilustracja 1: Widok z przodu

Z **przodu** znajdują się złącza. Szczegóły w rozdziale „Właściwości“ > „Złącza“.

Ilustracja 2: Widok z góry

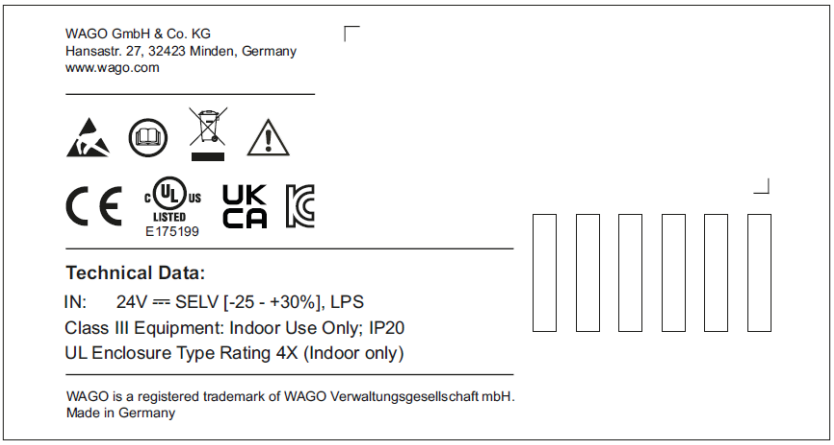
U góry znajduje się złącze „X8 Lineout“, przełącznik trybu pracy (BAS) z możliwością wyboru pozycji RESET-STOP-RUN, przycisk „CFG/RST“, wskaźniki LED „SYS, RUN, CAN, H11, H22 i gniazdo karty pamięci „µSD“. Szczegóły w rozdziale „Właściwości“ > „Złącza“, > „Elementy sygnalizacyjne“ i > „Elementy obsługi“.

4.2 Nadruk

Nadruk i tabliczka znamionowa znajdują się na spodzie urządzenia.
Zawiera ona następujące dane produktu:

Tabela 3: Nadruk

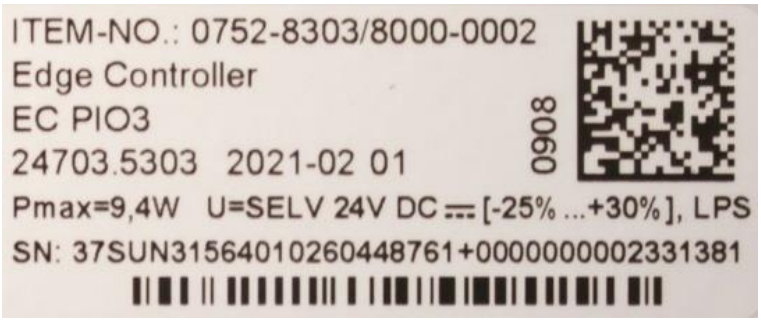
Pole	Przykład
Napięcie zasilania	24V SELV [−25% … +30%], LPS
Klasa ochronności	Class III
Stopień ochrony IP	IP20



Ilustracja 3: Nadruk (przykład)

Tabela 4: Tabliczka znamionowa

Pole	Przykład
Nr katalogowy	ITEM-NO.: 0752-8303/8000-0002
Nazwa produktu 1	Edge Controller
Nazwa produktu 2	EC PIO3
Numer kontrolny	24703.5303
Data produkcji (rok – miesiąc)	2021-02
Indeks dopuszczenia: Wersja sprzętu	 01
Pobór mocy	Pmax.=9,4 W
Napięcie zasilania	U=SELV 24V DC (−25% … +30%), LPS
Numer seryjny	SN:37SUN31564010260448761+0 000000002331381
Kod kreskowy	
Kod DataMatrix	



Ilustracja 4: Tabliczka znamionowa (przykład)

4.3 Złącza

4.3.1 Złącza z przodu obudowy

Tabela 5: Złącza z przodu obudowy

Złącze	Funkcja
X1 i X2	Złącza ETHERNET ze wskaźnikami LED
X3	Złącze szeregowe RS-232 lub RS-485
X4	Złącze CAN
X5	POWER. Zasilanie
X6 i X7	Złącza USB 2.0 Host
X9	Złącze HDMI
X10	Złącze USB C
X11	4 dwustanowe wejścia i wyjścia DIO

4.3.2 Złącza u góry

Tabela 6: Złącza u góry

Złącze	Funkcja
X8	Wyjście Lineout na słuchawki
µSD	Gniazdo karty microSD i microSDHC, z pokrywą, z możliwością plombowania

4.3.3 „X1“ i „X2“ – złącza ETHERNET

Złącza ETHERNET są gniazdami RJ-45. Przy LINK świeci pomarańczowa LED, a podczas transmisji danych miga zielona LED.

Złącza i przewody odpowiadają kategorii 5e oraz dyrektywom dotyczącym interfejsów ETHERNET.

Zintegrowany switch ETHERNET 10/100 Mbit wspiera Auto-MDI(X). Można stosować zarówno przewody crossover, jak i patch.

4.3.4 „X3“ – złącze szeregowe RS-232/-485

To złącze jest wbudowanym gniazdem D-Sub 9 i posiada separację galwaniczną od napięcia zasilającego produktu oraz innych złącz. Wspiera prędkości transmisji od 1200 do 115 200.

Gniazdo zawiera złącze zgodne z RS-232 i złącze zgodne z RS-485. NIE MOŻNA używać obu złącz równocześnie.

Urządzenia komunikujące się ze sobą muszą mieć ustawiony taki sam rodzaj złącza, ponieważ poziomy napięć dla obu typów NIE są ze sobą kompatybilne!

Tabela 7: Znaczenie pinów X3

Styk	RS-232 (DCE)		RS-485	
	Sygnał	**Opis**	**Sygnał**	**Opis**
1	NC	Niewykorzystane	NC	Niewykorzystane
2	RxD (out)	Receive Data	NC	Niewykorzystane
3	TxD (in)	Transmit Data	A (Tx/Rx+)	Transmit/receive data +
4	NC	Niewykorzystane	NC	Niewykorzystane
5	FB_GND	Masa	FB_GND	Masa
6	NC	Niewykorzystane	FB_5V	Zasilanie
7	NC	Niewykorzystane	NC	Niewykorzystane
8	NC	Niewykorzystane	B (Tx/Rx−)	Transmit/receive data −
9	NC	Niewykorzystane	NC	Niewykorzystane
Obudowa	Ekran	Ekranowanie	Ekran	Ekranowanie

UWAGA

Niewłaściwa parametryzacja może uszkodzić urządzenie będące partnerem w komunikacji!
Poziomy napięć dla RS-232 i RS-485 nie są kompatybilne!
Gdy w sterowniku i urządzeniu, będącym partnerem w komunikacji, zastosowane są różne złącza (RS-232 <> RS-485 lub RS-485 <> RS-232), może dojść do uszkodzenia złącza partnerskiego. Dlatego przy parametryzacji sterownika należy pamiętać o ustawieniu złącza zgodnego ze złączem partnera komunikacyjnego!

W celu zwiększenia odporności na zakłócenia konieczne jest zastosowanie stałego ekranowania. Dlatego metalowa obudowa gniazda połączona jest z uziemieniem funkcjonalnym.

Podłączony przewód danych musi być ekranowany. Zastosowana obejma przewodu powinna stanowić wystarczające zabezpieczenie przewodu przed wyrwaniem i równocześnie tworzy powierzchniowy styk ekranu z obudową.

Kierunek przepływu danych złącza RS-232 produktu odpowiada typowi urządzenia DCE.

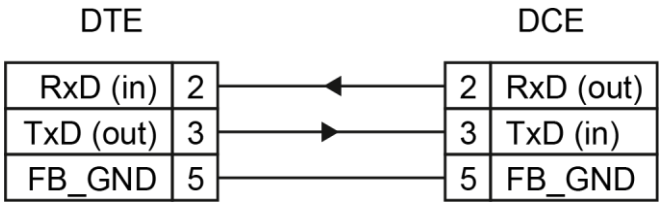
4.3.4.1 Praca jako interfejs RS-232

Zależnie od typu urządzenia DTE (Data Terminal Equipment, np. PC) lub DCE (Data Communication Equipment, np. PFC, modem) transmisja sygnałów RS-232 przebiega w różnych kierunkach.

Tabela 8: Funkcja sygnałów RS-232 przy DTE/DCE

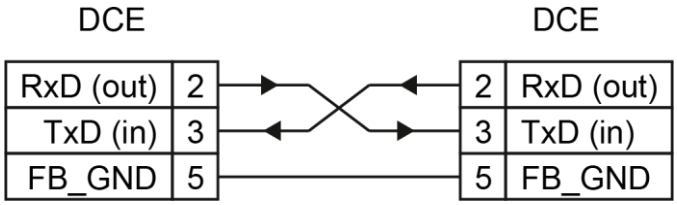
Styk	Sygnał	Kierunek transmisji danych	
		DTE	DCE
2	RxD	Wejście	Wyjście
3	TxD	Wyjście	Wejście
5	FB_GND	---	---

Przy połączeniu DTE do DCE sygnały łączone są bezpośrednio (1:1).



Ilustracja 5: Podłączenie przy połączeniu DTE-DCE (1:1)

Przy połączeniu DCE do DCE sygnały krzyżują się (cross-over).



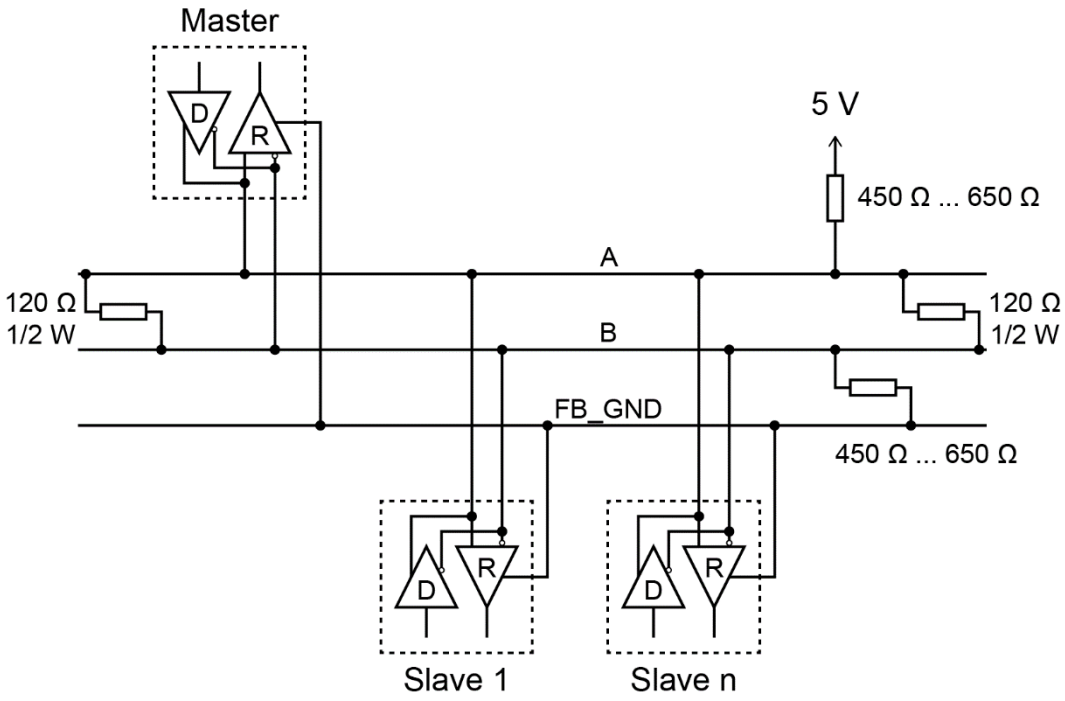
Ilustracja 6: Podłączenie przy połączeniu DCE-DCE (cross-over)

4.3.4.2 Praca jako interfejs RS-485

Aby ograniczyć zjawisko odbicia sygnałów, na obu końcach przewodu RS-485 musi znajdować się terminacja. W razie konieczności można zastosować po 1 rezystorze pull-up lub pull-down. Zapewniają one utrzymanie zdefiniowanego poziomu sygnału na magistrali w przypadku, gdy żadne urządzenie w sieci nie jest aktywne, tzn. wszystkie urządzenia znajdują się w stanie „Tri-State“.

Wskazówka

Pamiętać o zakończeniu magistrali!
Sieć RS-485 musi posiadać terminację na obu końcach!
Nie należy stosować więcej niż 2 terminacji na sieć!
Na odcinkach będących odejściami lub odgałęzieniami nie należy używać terminacji! Przewody odejściowe powinny być jak najkrótsze!
Praca bez właściwej terminacji sieci RS-485 może prowadzić do błędów w transmisji.



Ilustracja 7: Terminacja sieci RS-485

4.3.5 „X4“ – złącze CAN

To złącze jest wbudowanym wtykiem D-Sub 9 i posiada separację galwaniczną od napięcia zasilającego urządzenia oraz innych złącz.
Złącze odpowiada ISO 11898-2.

Tabela 9: Znaczenie pinów X4

Pin	Znaczenie
1	-
2	CAN-L (CAN data low)
3	GND (potencjał odniesienia 0 V lub masa)
4	-
5	-
6	-
7	CAN-H (CAN data high)
8	-
9	-

W celu zwiększenia odporności na zakłócenia konieczne jest zastosowanie stałego ekranowania. Dlatego metalowa obudowa wtyku połączona jest pojemnościowo z uziemieniem funkcjonalnym.
Podłączony przewód danych musi być ekranowany. Zastosowana obejma przewodu powinna stanowić wystarczające zabezpieczenie przewodu przed wyrwaniem i równocześnie tworzy powierzchniowy styk ekranu z obudową.

4.3.6 „X5“ – złącze zasilające POWER

Napięcie zasilające należy podłączyć do złącza X5. Należy do tego użyć dostarczonego wraz z urządzeniem gniazda 734-103 z 3 zaciskami CAGE CLAMP®.
Więcej informacji dotyczących zasilania znaleźć można w rozdziale „Dane techniczne“.

Tabela 10: Znaczenie pinów X5

Pin	Nazwa	Znaczenie
1	24VDC	Napięcie zasilania +24 V DC
2	GND	Potencjał odniesienia 0 V (masa)
3	FE	Uziemienie funkcjonalne

4.3.7 „X6“ i „X7“ – złącza USB 2.0

Te złącza USB 2.0 Host wyposażone są w 4-biegunowe gniazda typu A. Każde złącze może dostarczyć maks. 500 mA.

Złącza te odpowiadają specyfikacji USB 2.0.

Można do nich podłączać alternatywne urządzenia służące do wprowadzania danych, takie jak klawiatury i myszy lub maks. 2 pamięci USB. Te urządzenia USB należy podłączyć przed włączeniem Power ON.

4.3.8 „X8“ – wyjście Lineout na słuchawki

Wyjście audio jest 3-biegunowym gniazdem stereo typu jack, 3,5 mm. Można tu podłączyć słuchawki lub kompaktowy głośnik i dzięki temu uzyskać np. akustyczne sygnały ostrzegawcze lub komunikaty słowne, zawarte w aplikacji sterowania.

4.3.9 „X9“ – złącze HDMI typ A

HDMI to skrót od High Definition Multimedia Interface. Złącze HDMI to standardowy złącze, umożliwiające równoczesną transmisję dźwięku i obrazu tylko jednym przewodem. Poprzez złącze HDMI produkt można podłączyć do monitora. Obsługiwana jest rozdzielczość Full HD (1920×1080).

Wskazówka

Różnice w zastosowaniu złącza HDMI!
W budynkach mieszkalnych, handlowych i komercyjnych oraz małych przedsiębiorstwach nie wolno wykorzystywać portu HDMI.
W przemyśle dozwolone jest stosowanie portu HDMI.

4.3.10 „X10“ – złącze USB C

Przy uruchamianiu i w celu konserwacji połączenie IP można utworzyć przez złącze serwisowe USB, patrz też rozdział „Uruchamianie" > „Ustawianie adresu IP" > „Połączenie IP przez USB".

Złącze serwisowe USB zostało zrealizowane jako gniazdo USB-C. Złącze wspiera specyfikację USB 2.0.

Sterownik przedstawiany jest w urządzeniu host (PC) jako urządzenie peryferyjne w trybie device.

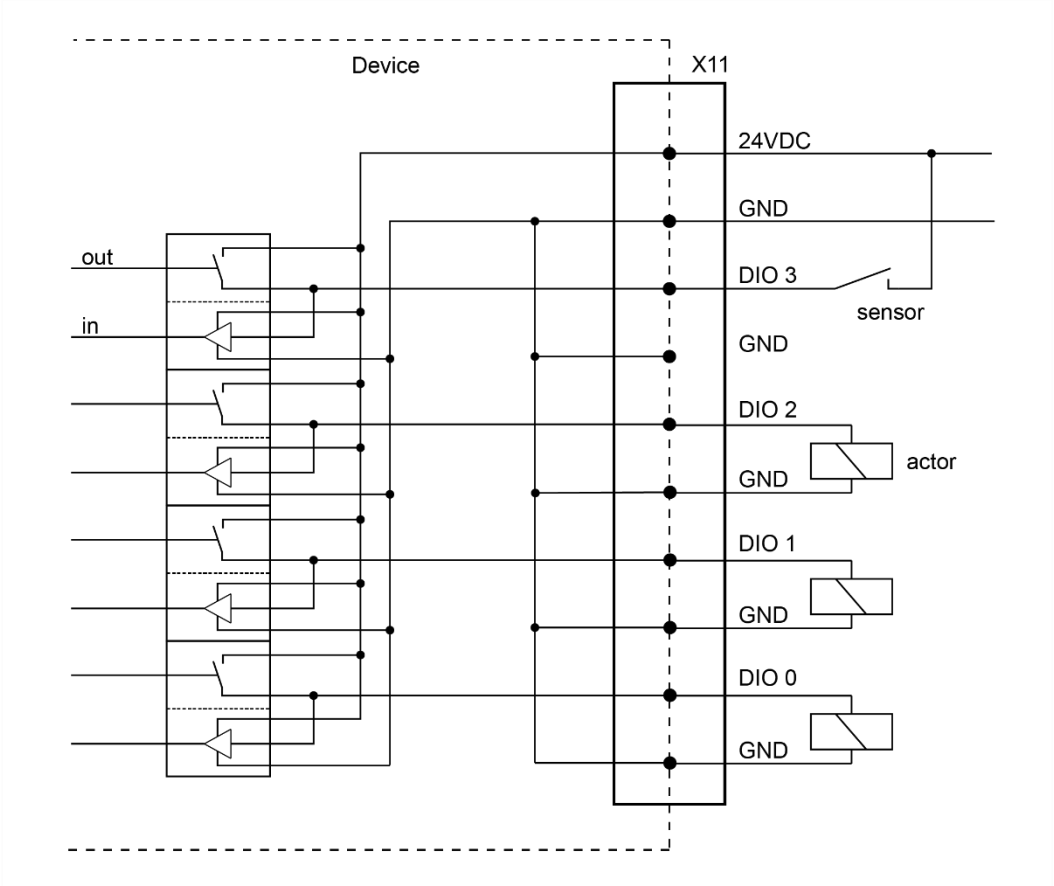
4.3.11 „X11“ – 4 dwustanowe wejścia i wyjścia DIO

Cztery dwustanowe złącza z możliwością konfiguracji jako wejścia lub wyjścia służą do podłączania czujników i elementów wykonawczych.
Wykorzystano tu 10-biegunowy wielowtyk *picoMAX*® z 10 zaciskami Push-in CAGE CLAMP®S (gniazdo 2091-1110).
Złącza są specyfikowane zgodnie z EN 61010-2-201:
Obwód prądu stałego, zastosowanie ogólne

Tabela 11: Znaczenie pinów X11

CAGE CLAMP®	Nazwa	Znaczenie
1	GND	Potencjał odniesienia 0 V (masa)
2	DIO 0	Dwustanowe wejście/wyjście 0
3	GND	Potencjał odniesienia 0 V (masa)
4	DIO 1	Dwustanowe wejście/wyjście 1
5	GND	Potencjał odniesienia 0 V (masa)
6	DIO 2	Dwustanowe wejście/wyjście 2
7	GND	Potencjał odniesienia 0 V (masa)
8	DIO 3	Dwustanowe wejście/wyjście 3
9	GND	Potencjał odniesienia 0 V (masa)
10	24 V DC	Napięcie zasilania dwustanowych wejść i wyjść

Wejścia/wyjścia posiadają separację galwaniczną od napięcia zasilającego produktu oraz innych złącz.



Ilustracja 8: Złącza DIO X11 (przykład)

4.3.12 „µSD“ – gniazdo karty pamięci

Produkt wyposażony jest z boku w gniazdo kart pamięci microSD i microSDHC.

Dopuszczalne jest zastosowanie przetestowanych przez WAGO kart pamięci microSD (maks. 2 GB) i microSDHC (maks. 32 GB).

PRZESTROGA

Stosować tylko karty pamięci zalecane przez WAGO!
W przypadku zastosowania kart pamięci niezalecanych przez WAGO nie ma gwarancji prawidłowego funkcjonowania oraz wydajności!

Wskazówka

Pamiętać o sformatowaniu karty pamięci!
Należy pamiętać, że karty pamięci ≤ 2 GB często sformatowane są przy pomocy systemu plików „FAT16“ i w katalogu głównym mogą pomieścić maksymalnie 512 bajtów. Przy większej liczbie bajtów niż 512 należy utworzyć podkatalog lub sformatować kartę pamięci przy pomocy „FAT32“.

4.4 Zegar czasu rzeczywistego

Zegar czasu rzeczywistego (RTC= **R**eal **T**ime **C**lock) jest wbudowany w urządzenie i nie jest dostępny. Służy wyłącznie do wewnętrznego zastosowania.

Odchyłki/dokładność

Odchylenie jest mniejsze niż ± 4 s/dzień przy temperaturze otoczenia 25°C.

Rezerwa działania

Po wyłączeniu napięcia zasilania przy temperaturze 25°C zegar działa nadal co najmniej przez 35 dni (ok. 840 godzin).
Po wyłączeniu zegara, po upływie więcej niż 35 dni bez zasilania, pokazuje się dialog umożliwiający jego ponowne ustawienie. Wyświetlanie dialogu można włączyć lub wyłączyć.
Do buforowania nie jest wykorzystywana bateria.

Rozdzielczość

Rozdzielczość zegara przy wyświetlaniu daty i godziny wynosi 1s.
Data i godzina generowane i odpytywane są przez aplikację.

4.5 Elementy sygnalizacyjne

4.5.1 LED statusu

Po lewej stronie znajdują się 1 trójkolorowa LED i 4 dwukolorowe LED.

LED SYS wskazuje status.

Tabela 12: LED SYS

Wskazanie	Znaczenie
Zielony migający	Produkt jest gotowy do pracy.
Czerwony migający	Wystąpił błąd. Wyświetlony zostaje odpowiedni komunikat błędu.
Niebieski migający	Wystąpił błąd połączenia ze sterownikiem. Brak komunikacji

LED RUN sygnalizuje status programu.

Tabela 13: LED RUN

Wskazanie	Znaczenie
Zielony migający	Aplikacja i projekt bootowalny nie są załadowane.
Zielony migający	Aplikacje CODESYS V3 działają.
Czerwony migający	Wszystkie aplikacje CODESYS V3 zostają zatrzymane.

LED CAN sygnalizuje status CANopen.

Tabela 14: LED CAN

Wskazanie	Znaczenie
Zielony migający	Komunikacja CAN działa.
Czerwony migający	Komunikacja CAN jest zakłócona.

Dwie pozostałe LED „H11“ i „H22“ przeznaczone są do wykorzystania w przyszłości.

4.6 Elementy obsługi

Po lewej stronie znajdują się przełącznik trybu pracy (BAS) i przycisk „CFG/RST“.

4.6.1 Przełącznik trybu pracy

Przełącznik trybu pracy ma następujące ustawienia:

Tabela 15: Ustawienia przełącznika trybu pracy

Pozycja	Działanie	Funkcja
RESET	Powracający do pozycji wyjściowej	**Gorący reset** lub **Zimny reset** (zależnie od długości przytrzymania przycisku, patrz rozdział „Uruchamianie“ > „Wyzwalanie funkcji RESET“)
STOP	Pozostający na danej pozycji	**Stop** Wszystkie aplikacje CODESYS V3 zostają zatrzymane.
RUN	Pozostający na danej pozycji	**Normalny tryb pracy** Aplikacja CODESYS V3 działa.

Przy pomocy przycisku „CFG/RST“ można wykonać „Factory Reset“. Patrz rozdział „Serwis“ > „Factory Reset“.

4.6.2 Przycisk „CFG/RST“

Przycisk „CFG/RST“ znajduje się w zagłębieniu, które uniemożliwia jego nieumyślne użycie. Jest to przycisk o krótkim skoku i niewielkiej sile docisku, wynoszącej od 1,1 N do 2,1 N (110 gf … 210 gf). Przycisk można uruchomić dowolnym nadającym się do tego celu przedmiotem (np. długopisem).

Przyciskiem „CFG/RST“ można:

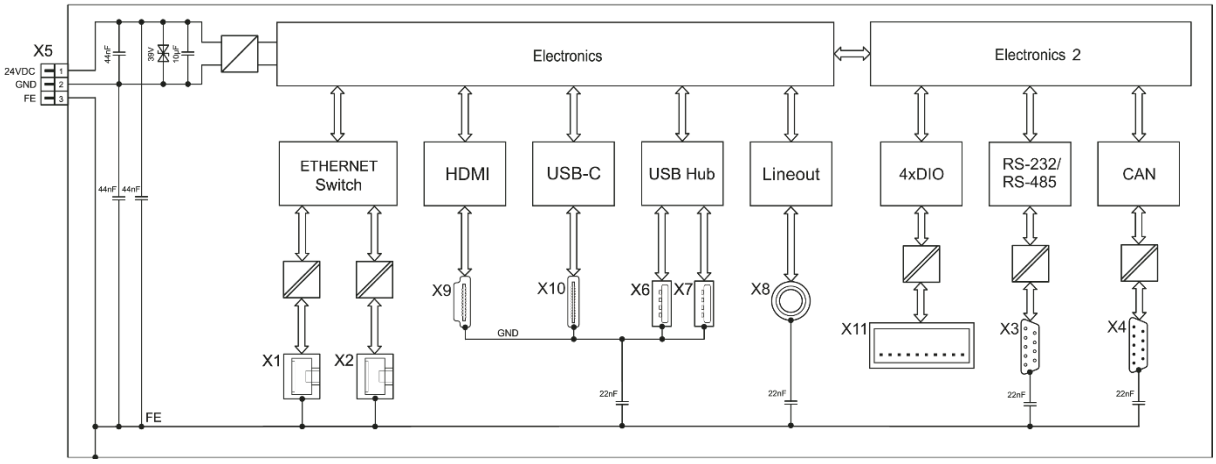
- zmienić konfigurację przy użyciu WBM
- odświeżyć ustawienia fabryczne („Factory Reset“).

Informacje na temat tych funkcji znajdują się w rozdziałach o w/w nazwach w dalszej części tego podręcznika.

4.7 Schemat połączeń wewnętrznych

UWAGA

Nie stosować urządzeń USB z uziemieniem!
Złącza USB nie są ekranowane bezpośrednio, lecz są uziemione przy pomocy kondensatorów przeciwzakłóceniowych. Do złącz USB można podłączyć tylko klawiatury, myszy lub zewnętrzne pamięci USB. Nie wolno podłączać urządzeń uziemionych, np. drukarek, gdyż spowoduje to zmostkowanie kondensatorów przeciwzakłóceniowych oraz zredukowanie ochrony przed zakłóceniami.



Ilustracja 9: Schemat połączeń wewnętrznych

4.8 Dane techniczne

4.8.1 Urządzenie

Tabela 16: Dane techniczne – urządzenie

Materiał obudowy	Aluminium, powlekane proszkowo
Wymiary (szerokość × wysokość × głębokość)	65 × 123 × 115 mm
Typ mocowania	Szyna montażowa
Masa	835 g
Stopień ochrony IP	IP20
Klasa ochronności	SK III
Kategoria przepięć	II
Stopień zanieczyszczenia	2

4.8.2 Warunki klimatyczne

Tabela 17: Dane techniczne – warunki klimatyczne

Dopuszczalna temperatura pracy	−20 ... +60°C
Dopuszczalna temp. składowania	−20 ... +80°C
Wilgotność względna (bez kondensacji)	90%
Praca w zależności od wysokości n.p.m.	0 … 2000 m

4.8.3 Zasilanie

Tabela 18: Dane techniczne – zasilanie

Napięcie	Źródło napięcia SELV (Safety Extra Low Voltage – bardzo niskie napięcie bezpieczne), spełniające wymagania LPS (Limited Power Source) zgodnie z EN 60950-1 24 V DC (18 ... 31,2 V) z ochroną przed zmianą polaryzacji
Maks. pobór prądu w całym zakresie napięcia, bez użycia/przy użyciu zewnętrznych urządzeń USB	120 mA / 390 mA
Maks. pobór mocy w całym zakresie napięcia, bez użycia/przy użyciu zewnętrznych urządzeń USB	2,9 W / 9,4 W

4.8.4 Sprzęt

Tabela 19: Dane techniczne – sprzęt

Procesor	ARM® Cortex® A9 Quadcore 1.0 GHz
Zewnętrzne rozszerzenie pamięci (gniazdo „µSD“)	Karta pamięci microSD (maks. 2 GB) lub microSDHC (maks. 32 GB)
Pamięć główna (RAM)	2 GB
Pamięć wewnętrzna (flash)	4 GB

4.8.5 Komunikacja

Tabela 20: Dane techniczne – komunikacja

Sieć obiektowa	MODBUS TCP/UDP/RTU i CAN
Protokoły	ETHERNET TCP/IP, DHCP, DNS, FTP, FTPS, HTTP, HTTPS i SSH

4.8.6 Złącza

Tabela 21: Dane techniczne − złącza

Złącza ETHERNET	2 × gniazdo RJ-45, ze switchem, 10/100 Mbit/s, przewody przyłączeniowe: skrętka SF-UTP, 100 Ohm, kategoria 5e, patch lub crossover, maks. dł. 100 m
Złącze szeregowe RS-232/-485	1 x wbudowane gniazdo D-Sub 9
Złącze CAN	1 x wbudowany wtyk D-Sub 9
Złącza USB	2 × gniazdo USB 2.0 Host (typ A), 480 Mbit/s, przewody przyłączeniowe: maks. dł. 3 m, pobór prądu maks. 2 × 500 mA 1 x gniazdo USB OTG (typ C)
Gniazdo „µSD“	Do kart pamięci microSD i microSDHC
HDMI	1 × HDMI (typ A)

4.8.7 Złącza

Tabela 22: Dane techniczne – złącza

Zasilanie	3 × CAGE CLAMP® przewód przyłączeniowy maks. 3 m do zasilacza, przekrój przewodu 0,14 ... 1,5 mm^2 / AWG 25 ... 14, długość odizolowania przewodu 7 mm / 0,28 in, materiał przewodu miedź (Cu), wytrzymałość termiczna przewodów min. 75°C
Wyjście audio na słuchawki	3-biegunowe gniazdo typu jack stereo, 3,5 mm, wyjście słuchawkowe 62,5 mW na 16 Ohm, zakres częstotliwości 20 … 20 000 Hz
4 dwustanowe wejścia i wyjścia DIO	10 × Push-in CAGE CLAMP®, 4 x wejścia zgodnie z IEC 61131-2 typ 1/wyjścia jako high-side switch 24 V 0,5A przekrój przewodu 0,2 … 1,5 mm^2 / AWG 24 … 14, dł. odizolowania 8 … 9 mm / 0,31 … 0,35 inch materiał przewodu miedź (Cu), wytrzymałość termiczna przewodów min. 75°C

4.9 Aprobaty

Produkt uzyskał następujące aprobaty:

Znak zgodności

UK Conformity Assessed

cULus: UL61010-1, UL61010-2-201

Korea Certification: R-R-W43-EDGE752

Eurasian Conformity: EAC RU Д-DE.PA01.B.09690/21

Informacja

Dodatkowe informacje na temat aprobat
Szczegółowe informacje dotyczące aprobat można znaleźć w Internecie:
https://www.wago.com/de <Numer katalogowy>

4.10 Normy i dyrektywy

Produkty spełniają następujące normy EMC:

EMC CE – odporność na zakłócenia	EN 61000-6-2
EMV CE - emisja zakłóceń	EN 61000-6-3

Wskazówka

Różnice w zastosowaniu złącza HDMI!
W budynkach mieszkalnych, handlowych i komercyjnych oraz małych przedsiębiorstwach nie wolno wykorzystywać portu HDMI.
W przemyśle dozwolone jest stosowanie portu HDMI.

5 Funkcje

Sterownik łączy w sobie funkcje urządzenia HMI i sterownika, gdyż jest urządzeniem PLC zgodnie z IEC 61131-3. Do 4 dwustanowych wejść/wyjść można podłączyć 4 elementy wykonawcze lub czujniki. Jeśli jest potrzebna większa liczba tych urządzeń, przez złącza sieci obiektowej można podłączyć dodatkowe węzły sieciowe.

Uruchamia się go w przeglądarce internetowej przy pomocy oprogramowania „Web-Based-Management WBM“. Podczas bieżącej pracy systemu z aplikacją stworzoną w CODESYS V3 przez port HDMI wyświetlana jest Target-Wizualizacja, która została zaprogramowana na komputerze inżynierskim za pomocą CODESYS V3. Za pomocą zintegrowanego z panelem serwera WWW wizualizację można udostępnić innym urządzeniom wyświetlającym.

Komunikacja z komputerem inżynierskim bazuje na sieci ETHERNET. Komunikacja z innymi sterownikami lub interfejsami odbywa się przez sieć ETHERNET lub inną sieć obiektową.

Wskazówka

Różnice w zastosowaniu złącza HDMI!
W budynkach mieszkalnych, handlowych i komercyjnych oraz małych przedsiębiorstwach nie wolno wykorzystywać portu HDMI.
W przemyśle dozwolone jest stosowanie portu HDMI.

5.1 Przeglądarka internetowa

Zintegrowana przeglądarka internetowa wyświetla strony internetowe sterownika/sterowników przez złącze HDMI.
W systemie WBM można skonfigurować do 10 sterowników. Korzystając z listy „PLC-List“/„Browser Favorites“ można wybrać sterowniki i bezpośrednio uruchomić stworzoną dla nich wizualizację internetową. Przeglądarka internetowa jest w stanie wyświetlać strony internetowe przez zaszyfrowane połączenie (HTTPS).

Wirtualna klawiatura otwiera się automatycznie przy uruchomieniu pola edycji. Poprzez naciśnięcie przycisku „Zmień klawiaturę“ można wybierać różne poziomy znaków (litery i cyfry). W ramach wizualizacji CODESYS można wybrać klawiatury: „virtual keyboard“, bądź „CODESYS numpad and keypad“.

Jako stronę startową można ustawić jedną z poniższych opcji:

- WBM
- lista „PLC List“/„Browser Favorites“
- bezpośrednie uruchomienie wizualizacji internetową sterownika

Informacja na temat skonfigurowania strony startowej, patrz strona „Favorites" w WBM.

5.2 Monitorowanie połączenia

Jeśli połączenie z wizualizacją CODESYS zostanie przerwane, w przeglądarce pojawi się komunikat o błędzie. Urządzenie próbuje automatycznie co 10 sekund ponownie nawiązać połączenie (reconnect).

5.3 WBM do konfiguracji i parametryzacji

System zarządzania przez WWW (WBM) jest interfejsem użytkownika służącym do konfiguracji lub parametryzacji sterownika. System WBM można otworzyć bezpośrednio na sterowniku, bądź na komputerze inżynierskim.

Szczegółowy opis dostępnych elementów obsługi oraz funkcji można znaleźć w rozdziale „Uruchamianie“.

5.4 Sieć

5.4.1 Konfiguracja złącz

Złącza ETHERNET X1 i X2 połączone są z wewnętrznym 3-portowym switchem, którego trzeci port połączony jest z CPU. „Configuration Type“ jest fabrycznie ustawiony na „DHCP“. Ustawienia TCP/IP takie jak adres IP lub maska podsieci dotyczą zarówno X1, jak i X2.

5.4.1.1 Praca przy rozłączonych interfejsach sieciowych

W przypadku pracy przy rozłączonych interfejsach sieciowych oba interfejsy ETHERNET można konfigurować i używać osobno.
Należy pamiętać, że oba interfejsy nadal mają ten sam adres MAC. Dlatego nie mogą być wykorzystywane w tym samym segmencie sieci.

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

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

5.4.2 Bezpieczeństwo sieci

5.4.2.1 Użytkownicy (User) i hasła

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

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

Wskazówka

Zmienić hasła
Ustawione fabrycznie, standardowe hasła podane w niniejszej instrukcji obsługi nie stanowią wystarczającego zabezpieczenia! Należy zmienić te hasła stosownie do potrzeb!

5.4.2.2 Usługi i użytkownicy

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

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

5.4.2.3 Grupa użytkowników WBM

WBM ma własną administrację użytkownika. Występujący tu użytkownicy są ze względów bezpieczeństwa odseparowani od pozostałych grup w systemie.
Przy pierwszym uruchomieniu i zalogowaniu w WBM jako admin system automatycznie żąda nadania nowego hasła.
To nie oznacza jednak zmiany haseł dla użytkowników Linux® „root“ i „admin“!

Tabela 23: Użytkownicy WBM

Użytkownik	Uprawnienia	Standardowe hasło
admin	Pełne (administrator)	wago
user	Ograniczone	user

5.4.2.4 Grupa użytkowników Linux®

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

Hasła dla tych użytkowników można konfigurować poprzez połączenie terminalowe SSH.

Tabela 24: Użytkownicy Linux®

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

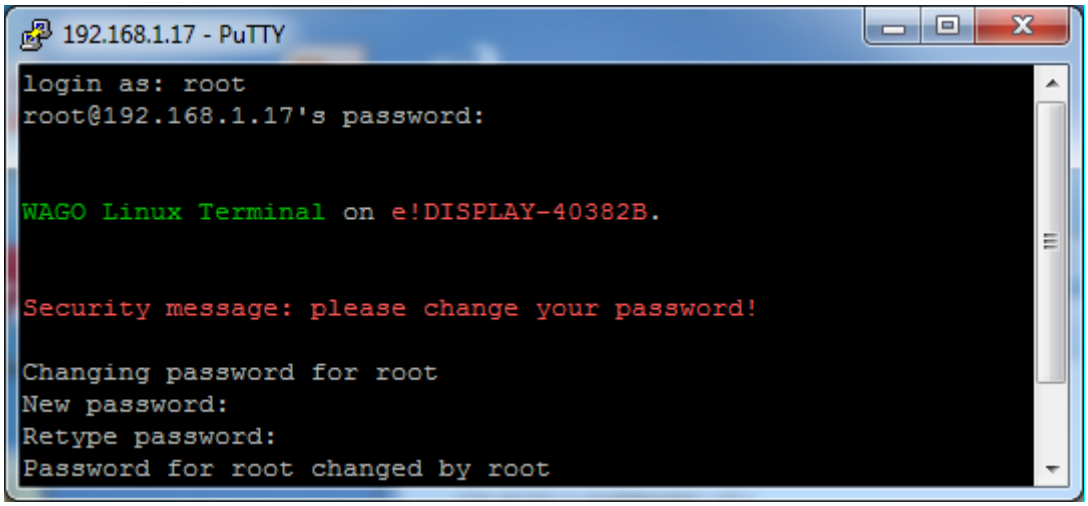
Wskazówka

Zmienić hasła

Ustawione fabrycznie, standardowe hasła podane w niniejszej instrukcji obsługi nie stanowią wystarczającego zabezpieczenia! Należy zmienić te hasła stosownie do potrzeb!

Przykład

Zmiany ustawionego wcześniej hasła dla użytkownika Linux® „root“ dokonuje się w programie terminalowym PuTTY przez ETHERNET za pomocą SSH.
Po uruchomieniu oprogramowania putty.exe pojawia się „login as“. Należy tu wpisać „root“ i nacisnąć [**Enter**]. Nastąpi pytanie o hasło. Należy wpisać ustawione wcześniej hasło „wago“. Następnie pojawi się żądanie nadania nowego hasła „New password:“. Należy wpisać indywidualne hasło o odpowiednim poziomie bezpieczeństwa i nacisnąć [**Enter**]. Następnie pojawi się polecenie powtórzenia hasła „Retype password:“. Należy ponownie wpisać swoje hasło i zakończyć procedurę zmiany naciskając [**Enter**].
Procedurę tę należy powtórzyć przy logowaniu się jako użytkownik Linux® „admin“.



Ilustracja 10: Przykład hasła Linux®

5.4.2.5 Grupa użytkowników SNMP

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

5.4.2.6 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.

5.4.2.7 Szyfrowanie TLS

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

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

Możliwe są ustawienia „Strong“ i „Standard“. Przy ustawieniu „Strong" serwer internetowy zezwala tylko na wersję TLS 1.2 i na silne algorytmy. Starsze oprogramowanie i starsze systemy operacyjne mogą nie obsługiwać protokołu TLS 1.2 i algorytmów szyfrowania. Ustawienie „Standard" zezwala na wersje TLS 1.0, TLS 1.1, TLS 1.2, a także metody kryptograficzne, które obecnie nie są już uważane za bezpieczne. Użycie jest zalecane tylko w przypadku zgodności wstecznej ze starszymi systemami.

Informacja

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

Informacja

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

Przewodnik można znaleźć w Internecie pod adresem: https://www.bsi.bund.de > „Topics“ > „Standards and Criteria“ > „Minimum Standards“.

5.4.3 Konfiguracja sieci

5.4.3.1 Nazwa hosta/nazwa domeny

Bez konfiguracji nazwy hosta produkt otrzymuje standardową nazwę, w skład której wchodzą ostatnie trzy wartości adresu MAC produktu. Nazwa ta obowiązuje do momentu skonfigurowania nazwy hosta lub dostarczenia jej przez DHCP do produktu (informacje na temat konfiguracji patrz rozdział „Uruchamianie“ > „Konfiguracja w systemie zarządzania przez WWW (WMB)“). Przy ustawianiu nazwy hosta należy pamiętać, że nazwa dostarczona przez odpowiedź DHCP jest natychmiast aktywowana i zastępuje nazwę standardową. Jeśli ma obowiązywać tylko nazwa skonfigurowana, administrator sieci musi tak dostosować konfigurację aktywnego serwera DHCP, aby w odpowiedzi DHCP nie były wysyłane nazwy hosta.

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

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

5.4.3.2 Bramy domyślne

W ramach konfiguracji TCP/IP produkt dopuszcza ustawienie dwóch bram domyślnych. Urządzenie w sieci wysyła wszystkie pakiety danych dla systemów, znajdujących się poza swoją siecią lokalną, do bramy domyślnej. Ta może przesyłać te pakiety dalej tak, aby dotarły do systemu docelowego.

Bramom domyślnym nie przypisuje się tak zwanej metryki, określającej zwłokę czasową, z którą pakiet danych może być wysłany. Jeśli skonfigurowanych jest kilka bram domyślnych, system operacyjny wysyła pakiety danych do tej bramy, która ma najniższą wartość metryki. Jeśli ta brama nie jest dostępna, podejmowana jest próba wysyłki do bramy o następnej wyższej wartości metryki. Jeśli kilka bram ma taką samą metrykę, brama ustalana jest losowo. Jeśli ta brama nie może wysłać pakietu danych, pakiet wysyłany jest równolegle do wszystkich bram o tej samej wartości metryki.

Metryka skonfigurowanych bram domyślnych może zostać dla produktu zadana. Standardowa wartość metryki wynosi 20. Oprócz bram konfigurowanych bezpośrednio można ustawiać kolejne bramy przez odpowiedzi DHCP. Wszystkie bramy nadesłane przez DHCP otrzymują niezmiennie metrykę o wartości 10. Tym samym w standardowym przypadku bramy DHCP mają priorytet ze względu na niższą wartość metryki.

5.5 Funkcje karty pamięci

Karta pamięci jest opcjonalna i spełnia rolę dodatkowego obszaru zapisu – oprócz pamięci wewnętrznej lub dysku. Na karcie pamięci można zapisywać ustawienia urządzeń i firmware produktu.

5.5.1 Backup

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

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

Pliki wewnętrznego dysku zapisywane są na wybranym medium 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.

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

5.5.2 Restore

Przy pomocy tej funkcji 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).

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

Wskazówka

W razie zmiany parametrów urządzenie zostaje uruchomione ponownie!
Należy pamiętać, że w przypadku zastąpienia parametrów innymi ustawieniami z karty pamięci, urządzenie uruchamia się ponownie w celu zastosowania danych.

Wskazówka

Rozmiar danych nie może przekraczać rozmiaru napędu wewnętrznego!
Należy pamiętać, że rozmiar danych w katalogu media/sd/copy nie może przekraczać rozmiaru wewnętrznego dysku.

5.5.3 Create Image

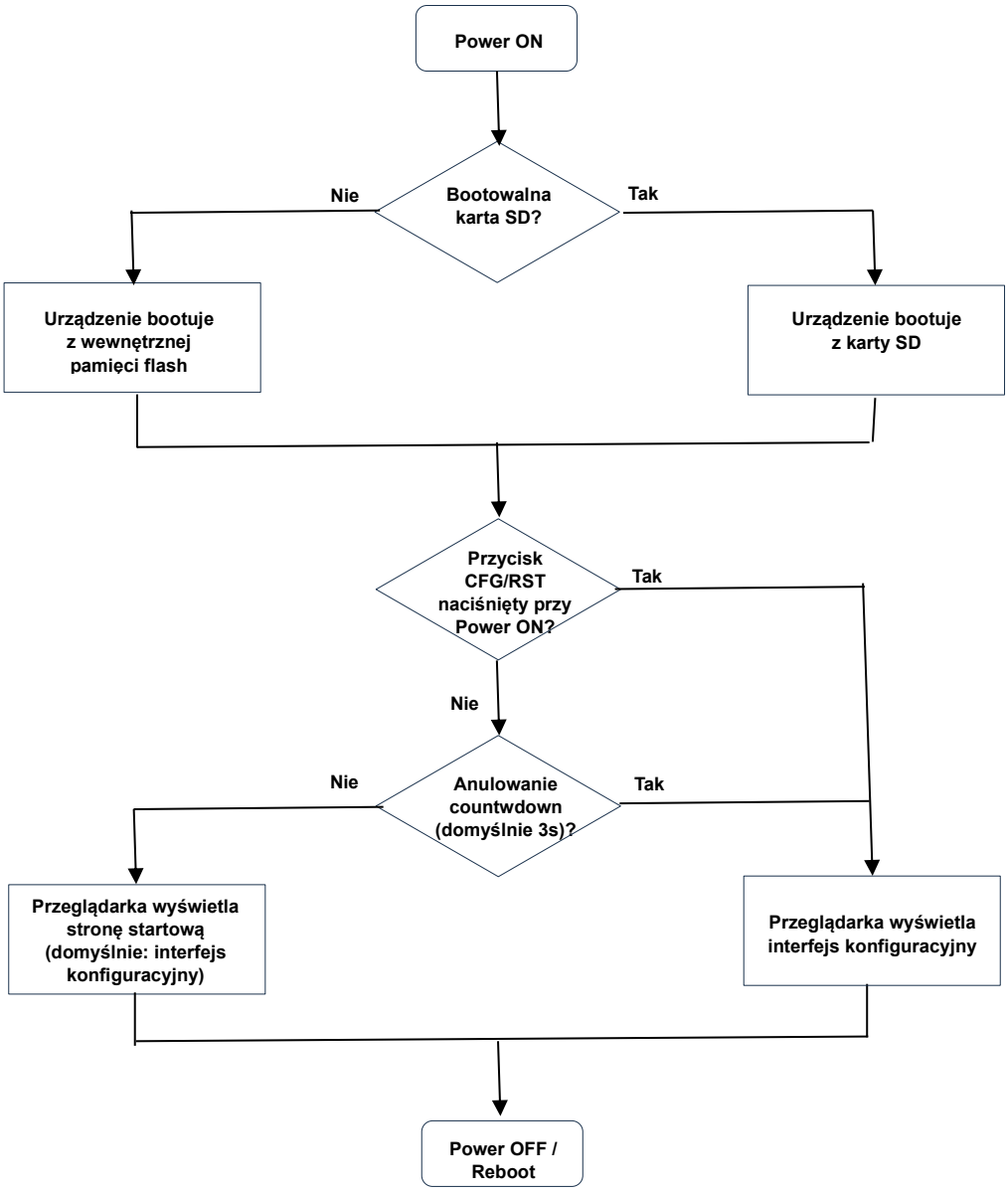
Ta funkcja WBM umożliwia tworzenie bootowalnych kopii aktualnie bootowanego systemu. Tzn. że jeśli produkt został uruchomiony z wewnętrznej pamięci (flash), to przy pomocy funkcji „Create Image“ w wersji WBM Legacy zostaje zapisana kopia na karcie pamięci. Jeśli produkt został uruchomiony z karty pamięci, kopia zostaje zapisana w wewnętrznej pamięci flash. Dotychczasowy obraz (image) zostaje usunięty.

5.6 Doinstalowanie oprogramowania

Produkt oferuje możliwość doinstalowania lub aktualizacji poszczególnych pakietów oprogramowania. Pakiety oprogramowania sporządzane są przez WAGO.
Można je zainstalować na komputerze przez system WBM. Patrz też strona WBM „Software Uploads".

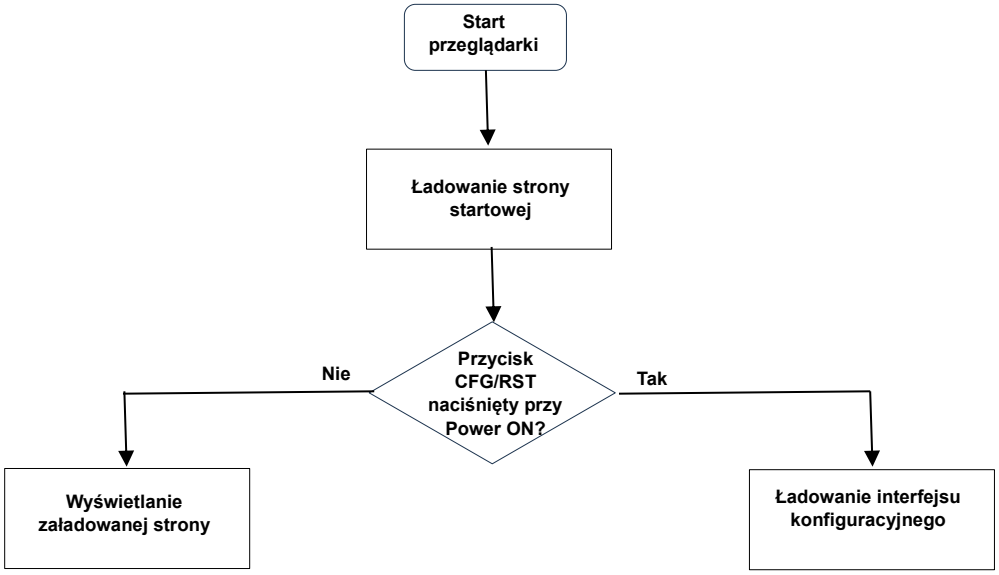
5.7 Bootowanie

Reakcja przy starcie



Ilustracja 11: Reakcja przy starcie

Przeglądarka



Ilustracja 12: Przebieg procesu przeglądarki

Przycisk „CFG/RST“

Naciśnięcie przycisku „CFG/RST“ w trakcie pracy otwiera system WBM. Naciśnięcie przy starcie (Power ON) produktu zatrzymuje normalny automatyczny start i powoduje uruchomienie jedynie WBM. Przycisk nie wprowadza zmian w ustawieniach.

5.8 Elementy oprogramowania wymagające licencji

Dla produktu dostępne są komponenty programowe systemu runtime CODESYS V3, podlegające kontroli licencji (licencje runtime).

Licencjonowanie można przeprowadzić przy użyciu Add-on Licensing.

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

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

6 Montaż

ESD

Unikać wyładowań elektrostatycznych!
W urządzeniu zintegrowane są komponenty elektroniczne, które mogą zostać zniszczone przez wyładowania elektrostatyczne w następstwie dotknięcia. Należy przestrzegać środków ochrony przed wyładowaniami elektrostatycznymi zgodnie z IEC 61340-5-1/-3. Przy obsłudze urządzenia należy pamiętać o odpowiednim uziemieniu otoczenia (osoby, stanowisko pracy oraz opakowanie).

UWAGA

Nie zakrywać otworów wentylacyjnych!
W celu zapewnienia odpowiedniej cyrkulacji powietrza otwory wentylacyjne należy odkryć.
Odstęp otworów wentylacyjnych od granicznych powierzchni powinien wynosić co najmniej 100 mm.

Wskazówka

Unikać bezpośredniej ekspozycji na światło!
Produkt należy umieścić tak, aby nie był wystawiony na bezpośrednie działanie silnego źródła światła, np. promieni słonecznych.

6.1 Wytyczne i normy dotyczące instalacji

DIN 60204	Wyposażenie elektryczne maszyn
DIN EN 50178	Urządzenia elektroniczne do stosowania w instalacjach dużej mocy (VDE 0160)
EN 60439	Rozdzielnice i sterownice niskonapięciowe

6.2 Pozycje montażowe

Obowiązuje znamionowa pozycja montażowa: przód urządzenia po właściwej stronie, czytelny opis, otwory wentylacyjne u góry i na dole.

Alternatywnie produkt można zamontować poziomo, a więc złączami skierowanymi do dołu. W tym celu należy zdjąć znajdujący się z tyłu adapter szyny montażowej i zamontować go z boku.

Produkt nie może być eksploatowany bezpośrednio w układzie szeregowym! Aktywne urządzenia sąsiadujące (równoważny produkt przy pełnym obciążeniu) muszą znajdować się w odległości co najmniej 12 mm, a pasywne urządzenia (bez aktywnego wytwarzania ciepła) w odległości co najmniej 6 mm.

6.3 Montaż na szynie

Montaż zatrzaskowy produktu na szynie montażowej T 35 zgodnie z normą EN 60715:

1. Zahaczyć produkt na górnej krawędzi szyny montażowej.
2. Docisnąć produkt w kierunku szyny montażowej, aby spowodować zadziałanie zaczepu.
3. W celu ustabilizowania produktu na szynie montażowej założyć blokadę końcową przed i za produktem (np. nr katalogowy 249-197).

7 Montaż przewodów

7.1 Uziemienie

Uziemienie realizowane jest przez złącze X5.
Należy do tego użyć dostarczonego wraz z urządzeniem wielowtyku (gniazdo 734-103) z 3 zaciskami CAGE CLAMP®. Otworzyć zacisk CAGE CLAMP® nr 3 przy pomocy przyrządu montażowego. Wprowadzić przewód maks. 1,5 mm² odizolowany na długości 7 mm i wyciągnąć przyrząd montażowy.
Włożyć wtyk do złącza X5 i następnie sprawdzić stabilność połączenia.

7.2 Podłączanie urządzeń

Elektryczne urządzenia peryferyjne podłącza się przez złącza umieszczone na górze i z przodu.

Złącza ETHERNET służą do podłączania sieci LAN lub do Internetu w celu zapewnienia komunikacji ze sterownikiem. Można stosować zarówno przewody crossover, jak i patch kategorii 5e.

Złącza USB 2.0 służą do podłączania klawiatury lub myszy jako alternatywnych urządzeń do wprowadzania danych. Można podłączyć także maksymalnie 2 pamięci USB. Ponieważ na rynku dostępnych jest wiele urządzeń USB, nie możemy zagwarantować prawidłowego funkcjonowania poszczególnych urządzeń.
Urządzenia USB/HDMI należy podłączyć przed włączeniem Power ON, gdyż nie są one przystosowane do hot pluggingu.

UWAGA

Nie stosować urządzeń USB z uziemieniem!
Złącza USB nie są ekranowane bezpośrednio, lecz są uziemione przy pomocy kondensatorów przeciwzakłóceniowych. Do złącz USB można podłączyć tylko klawiatury, myszy lub zewnętrzne pamięci. Nie wolno podłączać urządzeń uziemionych, np. drukarek, gdyż spowoduje to zmostkowanie kondensatorów przeciwzakłóceniowych oraz zredukowanie ochrony przed zakłóceniami.

UWAGA

HDMI tylko w warunkach przemysłowych!
Złącze HDMI może być stosowane tylko w warunkach przemysłowych. Nie należy podłączać portu HDMI w budynkach mieszkalnych, handlowych i komercyjnych oraz małych przedsiębiorstwach.

Karty pamięci **microSD** wtyka się do gniazda tak głęboko, aż będzie słyszalne zadziałanie zaczepów. W celu ochrony gniazdo można zaplombować.
Przy demontażu należy ponownie docisnąć kartę, aż zaczep zostanie zluzowany. Teraz można wyciągnąć kartę.

Jeśli aplikacja zawiera akustyczne sygnały/ostrzeżenia, można wykorzystać **wyjście audio** do połączenia wtyku typu jack 3,5 mm słuchawek lub innego systemu audio.

Więcej informacji na temat złącz znaleźć można w rozdziale „Właściwości“ > „Złącza“ i „Dane techniczne“.

7.3 Podłączanie napięcia zasilającego

Napięcie zasilające należy podłączyć do złącza X5, pinu 1 (+) i 2 (−).
Należy do tego użyć dostarczonego wraz z urządzeniem wielowtyku (gniazdo 734-103).

8 Uruchamianie

8.1 Włączanie

Produkt nie ma włącznika/wyłącznika i dlatego uruchamiany jest razem z całą instalacją.

Po uruchomieniu systemu użytkownik dociera, w zależności od ustawienia, automatycznie lub ręcznie przez złącze HDMI do systemu WBM, „PLC-List“/„Browser Favorites“ lub do wybranego sterownika. Automatyczną nawigację można przerwać i przejść do menu wyboru, klikając wyświetlony licznik.

8.2 Logowanie

Przed otwarciem interfejsu użytkownika WBM system prosi o podanie nazwy użytkownika i hasła. Przy pierwszym uruchomieniu WBM należy podać hasło inicjalne. Można zalogować się jako „administrator“ lub „user“. Grupy użytkowników dysponują różnymi funkcjonalnościami. Patrz „Konfiguracja w systemie zarządzania przez WWW (WBM) > Zarządzanie użytkownikami WBM“ i „Konfiguracja w systemie zarządzania przez WWW (WBM) > Prawa dostępu“.

8.3 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.

8.4 Ustawianie adresu IP

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

Tabela 25: 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 sterownik 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 rozdział „Konfiguracja“).

Przykład integracji sterownika (192.168.1.17) w istniejącej sieci:

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

Tabela 26: Maska sieci 255.255.255.0

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

8.4.1 Połączenie IP przez USB

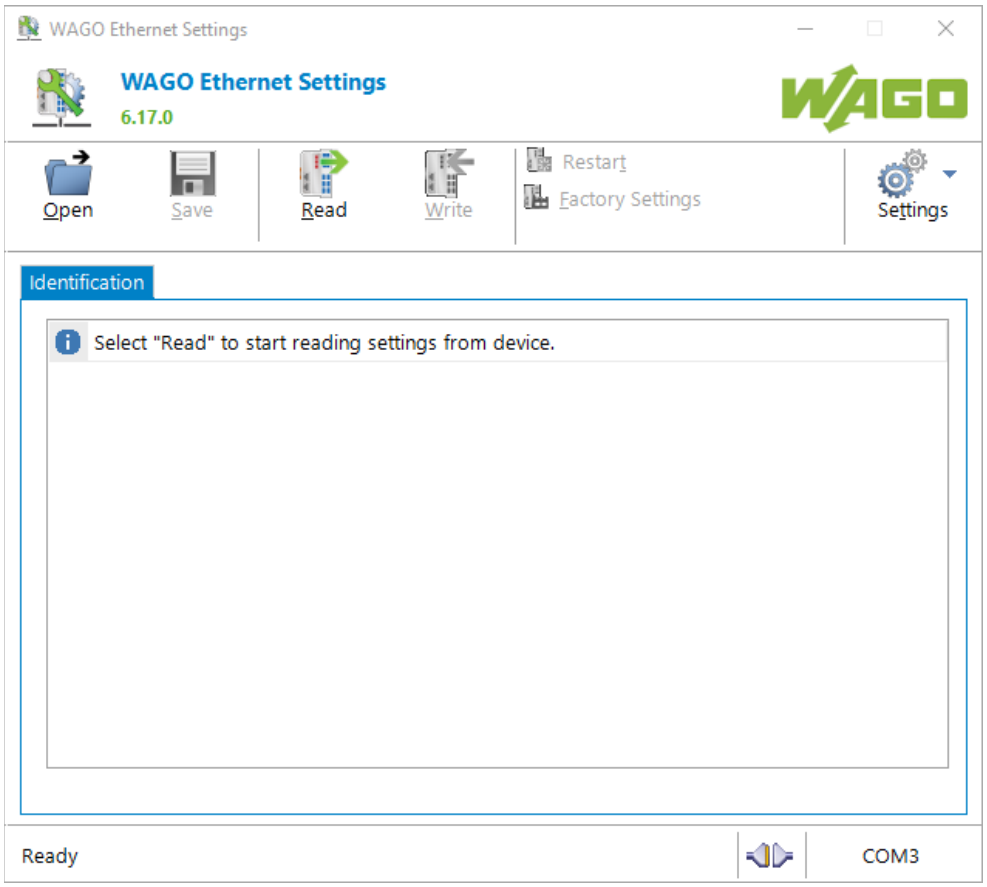
1. Podłącz sterownik do PC korzystając ze złącza serwisowego USB i odpowiedniego przewodu serwisowego USB C.
2. Przy zastosowaniu Windows 10 przejdź do kroku 4.
   Przy wersjach poniżej Windows 7 sterownik zachowuje się po włączeniu jak zewnętrzny napęd. Na napędzie zapisany jest sterownik dla połączenia IP przez USB.
3. Zainstaluj ten sterownik.
   Po tym możliwa będzie komunikacja za pośrednictwem połączenia IP przez USB.
4. Wpisz do przeglądarki stały adres IP 192.168.42.42.
   Zostanie otwarty system Web-Based-Management sterownika. W nim można wprowadzić wymagane ustawienia sterownika.

8.4.2 Zmiana adresu IP przy użyciu „WAGO Ethernet Settings“

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

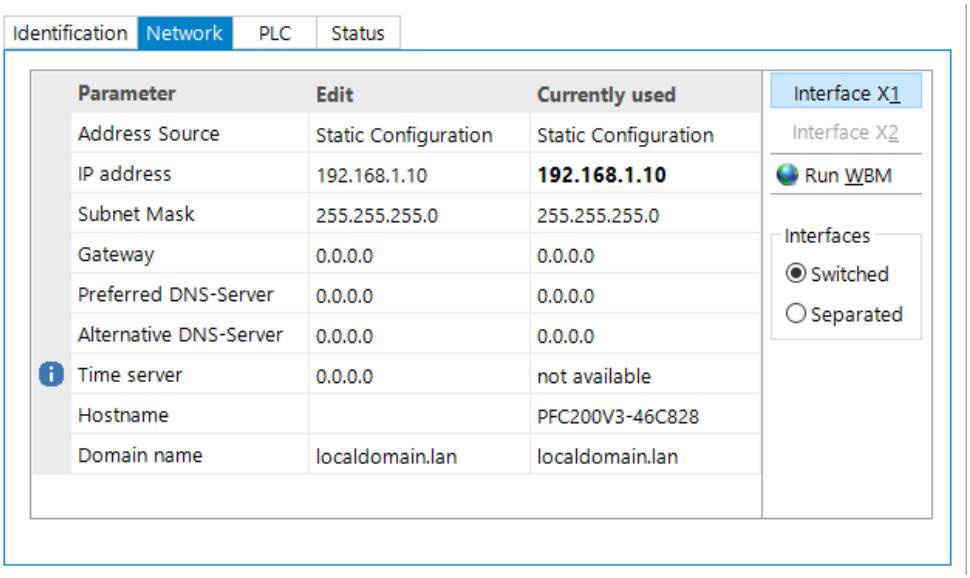
Do transmisji danych należy użyć przewodu serwisowego USB C lub sieci IP.

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



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

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



Ilustracja 14: „WAGO Ethernet Settings“ – zakładka „Network“ (przykład)

7. Aby móc nadać stały adres, wybierz w punkcie „Address Source“ w kolumnie „Parametr“ wartość „Static Configuration“. Standardowo aktywowany jest BootP.

8. W kolumnie „Parametr“ 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 też, w razie potrzeby, wprowadzić dalsze ustawienia bezpośrednio w systemie zarządzania przez WWW (WBM). W tym celu kliknij przycisk **[Run WBM]** po prawej stronie okna.

8.4.3 Czasowe ustawienie stałego adresu IP

Ta procedura pozwala ustawić tymczasowy adres IP dla interfejsu X1 jako stały adres „192.168.1.17“.
Przy włączonym switchu stały adres stosowany jest także dla interfejsu X2.
Przy wyłączonym switchu pierwotne ustawienia adresu dla interfejsu X2 nie ulegają zmianie.
Nie jest przeprowadzany reset.

Aby ustawić czasowo stały adres IP, postępuj w następujący sposób:

1. Ustaw przełącznik trybu pracy w pozycji STOP.

2. Naciśnij przycisk „CFG/RST“ przez czas dłuższy niż 8 sekund.

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

Aby anulować to ustawienie, postępuj w następujący sposób:

- Przeprowadź reset oprogramowania lub
- Wyłącz i ponownie włącz sterownik.

8.4.4 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.

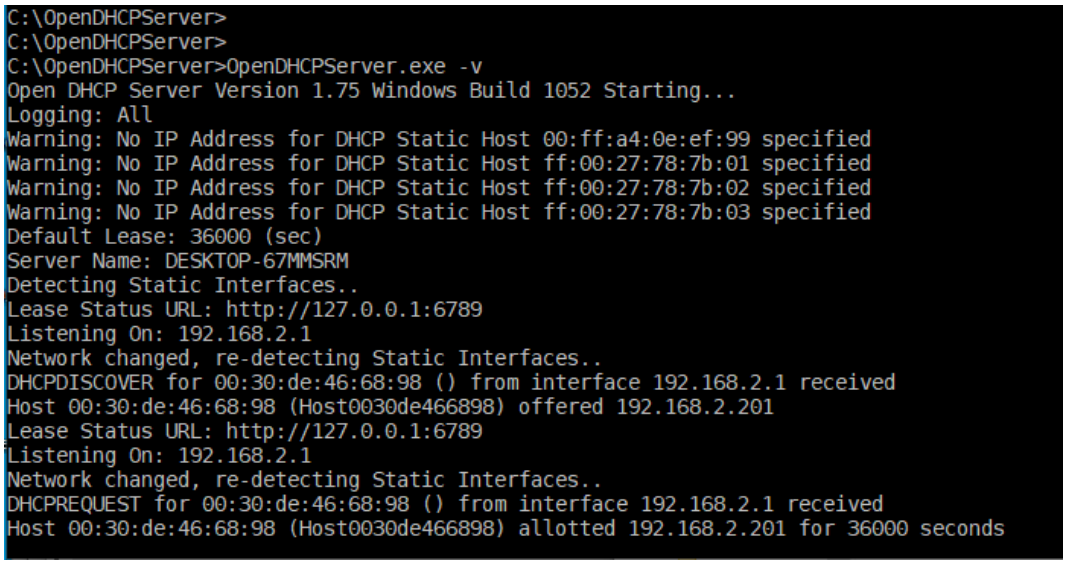
8.4.5 Przydzielanie adresu IP przy pomocy DHCP

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 urządzenia nadrukowany jest na etykiecie umieszczonej z boku.

Na poniższej ilustracji widoczny jest odpowiedni widok „Open DHCP“.



Ilustracja 15: „Open DHCP, przykład widoku“

W prezentowanym przykładzie przedrostek „Host“ i MAC-ID brzmi „00:30:de:46:68:98“.

Tym samym nazwa hosta brzmi „Host0030de466898“.

8.5 Wyzwalanie funkcji RESET

Przy pomocy przełącznika trybu pracy i przycisku „CFG/RST“ można realizować różne funkcje resetu.

8.5.1 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.

8.5.2 Zimny reset

Przy zimnym resecie resetowane są wszystkie aplikacje CODESYS V3. Wszystkie dane globalne i zmienne nieulotne ustawiane na poziomie ich wartości

inicjacyjnych.
Odpowiada on poleceniu „Reset cold“ w środowisku CODESYS V3 IDE.

W celu przeprowadzenia zimnego resetu należy ustawić przełącznik trybu pracy w pozycji RESET i przytrzymać go dłużej niż 7 sekund.
Wykonanie sygnalizowane jest dłuższym zgaśnięciem czerwonej LED „RUN“ po upływie 7 sekund. Następnie można puścić przełącznik trybu pracy.

8.5.3 Reset programowy (restart)

Przy resecie programowym sterownik uruchamiany jest ponownie.

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

Wykonanie sygnalizowane jest krótkim czerwonym, a następnie białym rozbłyskiem LED SYS. Po kilku sekundach wskaźniki LED SYS sygnalizują pomyślne zakończenie procesu bootowania sterownika.

8.5.4 Factory Reset

UWAGA

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

Wskazówka

Wszystkie parametry i hasła zostaną nadpisane!
Przy Factory Reset wszystkie parametry i hasła sterownika zostaną nadpisane.
Zapisane aplikacje, włącznie z danymi dotyczącymi wizualizacji, zostaną usunięte.
Niezainstalowane funkcje firmware'u nie zostaną nadpisane.
W razie pytań należy skontaktować się z pomocą WAGO.

Po Factory Reset sterownik uruchamiany jest ponownie.

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

1. Uruchom przycisk Reset (CFG/RST).
2. Ustaw przełącznik trybu pracy w pozycji RESET.
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.

Wskazówka

Nie przerywać procedury resetu!
Przy zbyt wczesnym puszczeniu przycisku resetu (CFG/RST) sterownik uruchomi się ponownie, bez zrealizowania Factory Reset.

8.6 Konfiguracja w systemie zarządzania przez WWW (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 sieci ETHERNET przez interfejs ETHERNET X1 i sieć ETHERNET.

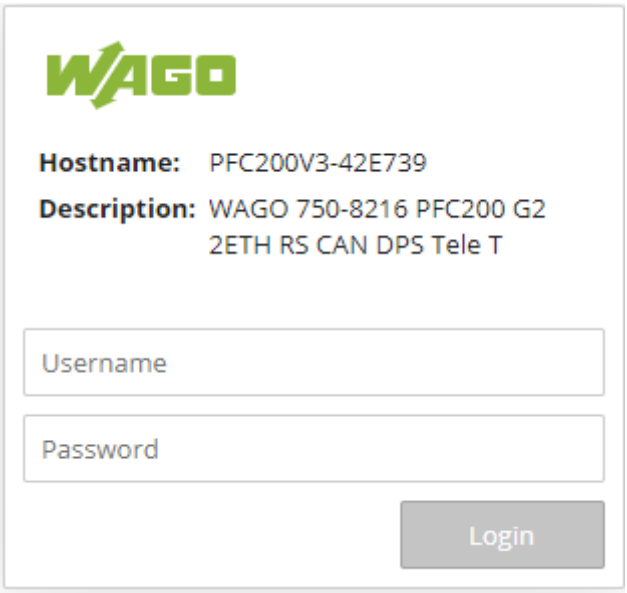
2. Na PC otwórz przeglądarkę internetową.

3. W pasku adresu przeglądarki internetowej wpisz „https://“, a następnie adres IP sterownika, a po nim „/wbm“, np. „https://192.168.1.17/wbm“. Pamiętaj, że PC i sterownik muszą znajdować się w tej samej podsieci (patrz rozdział „Ustawianie adresu IP“).
Jeśli nie znasz adresu IP i nie masz możliwości ustalenia go, przełącz sterownik czasowo na stały domyślny adres IP „192.168.1.17“ (tryb „Fix IP Address“ patrz rozdział „Uruchamianie“ > … > „Czasowe ustawienie stałego adresu IP“).

Wskazówka

Uwzględnić obciążenie przez program CODESYS
Jeśli sterownik 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 uzasadnione jest zatem zatrzymanie aplikacji CODESYS.

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



Ilustracja 16: Wpisywanie uwierzytelnienia (przykład)

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.

8.6.1 Zarządzanie użytkownikami WBM

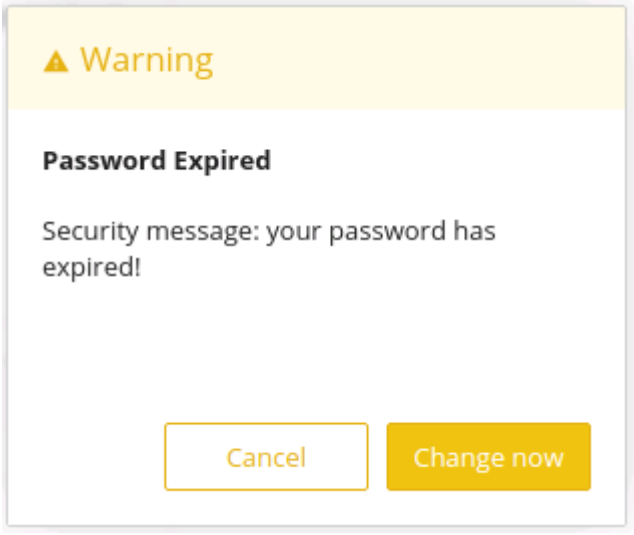
Poprzez zarządzanie użytkownikami można ograniczyć dostęp do funkcji WBM tylko dla wybranych osób.

Wskazówka

Zmienić hasła

Ustawione fabrycznie, standardowe hasła podane w niniejszej instrukcji obsługi nie stanowią wystarczającego zabezpieczenia! Należy zmienić te hasła stosownie do potrzeb!

Po zalogowaniu się odpowiedni komunikat ostrzegawczy będzie wyświetlany na każdej wywołanej stronie WBM aż do zmiany hasła.



Ilustracja 17: Przypomnienie o konieczności zmiany hasła

Po kliknięciu przycisku **[Change now]** następuje przekierowanie bezpośrednio na stronę WBM, na której można zmienić hasło.

Tabela 27: Fabryczne ustawienia użytkownika

Użytkownik	Uprawnienia	Standardowe hasło
root	Pełne (administrator)	wago
admin	Pełne (administrator)	wago
user	Ograniczone	user

Wskazówka

Rozszerzone uprawnienia użytkowników WBM

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

Zarządzanie użytkownikami dla aplikacji sterowania ustalane i realizowane jest osobno.

Prawa dostępu dla stron WBM zostały przedstawione w tabeli poniżej. Użytkownik „root“ ma takie same uprawnienia jak użytkownik „admin“ i dlatego nie jest wymieniony osobno.

Tabela 28: Prawa dostępu dla stron WBM

Zakładka/nawigacja			Tytuł strony WBM	Użytkownik
Information				
	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	Tademarks Information	user
	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 Domain Name	user
		Routing	Routing	user
	Clock		Clock Settings	user
	Administration			
		Serial Interface	Configuration of Serial Interface RS232/RS485	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
	Cloud Connectivity			
		Status	Przegląd	admin
		Connection 1	Configuration	admin
		Connection 2	Configuration	admin

Tabela 28: Prawa dostępu dla stron WBM

Zakładka/nawigacja			Tytuł strony WBM	Użytkownik
	SNMP			
		General Configuration	Configuration of general SNMP parameters	admin
		SNMP v1/v2c	Configuration of SNMP v1/v2c parameters	admin
		SNMP v3	Configuration of SNMP v3 Users	admin
	Browser Settings			
		Favorites	Favorites	user
		Autostart	Autostart	user
		Monitoring	Monitoring	user
		Browser Security	Browser Security	user
	Docker		Docker Settings	admin
	Display			
		Font Upload	Fonts	user
		Display Orientation	Display Orientation	user
		Screensaver	Screensaver	user
	Users		WBM User Configuration	user
Fieldbus				
	OPC UA		OPC UA Configuration	admin
	BACnet			
		Status	BACnet Status	admin
		Configuration	BACnet Configuration	admin
		Storage Location	BACnet Storage Location	admin
		Files	BACnet Files	admin
Security				
	OpenVPN / IPsec		OpenVPN / IPsec Configuration	admin
	Firewall			
		General Configuration	General Firewall Configuration	admin
		Interface Configuration	Interface Configuration	admin
		MAC Address Filter	Configuration of MAC Address Filter	admin
		User Filter	Configuration of User Filter	admin
	Certificates		Certificates	admin
	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				

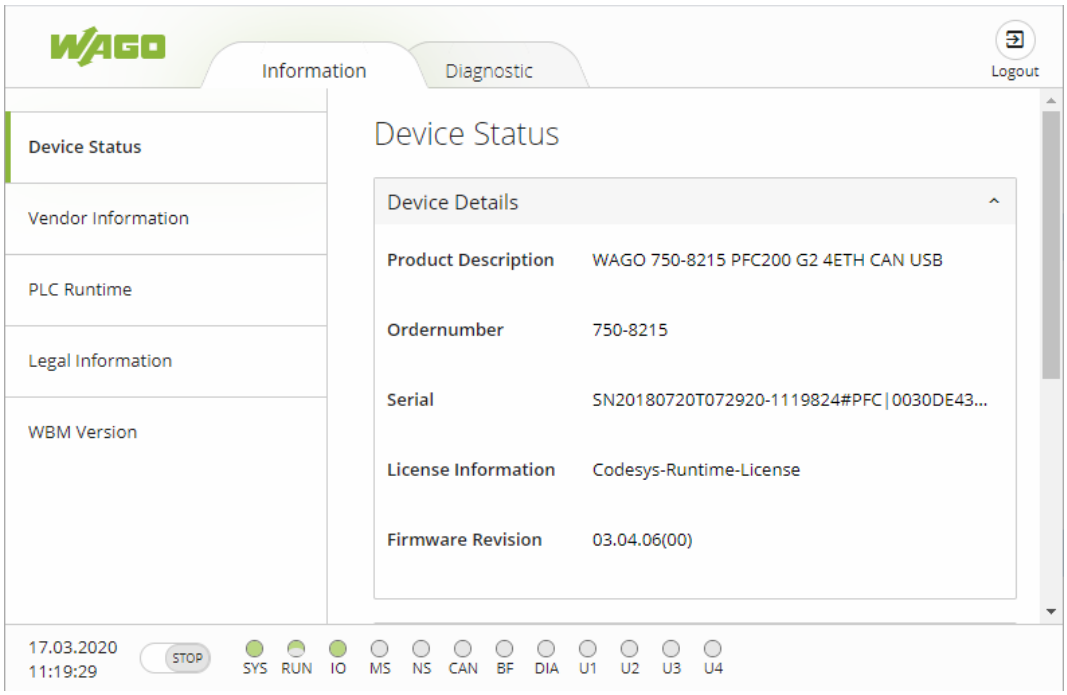
Tabela 28: Prawa dostępu dla stron WBM

Zakładka/nawigacja		Tytuł strony WBM	Użytkownik
	Log Message	Log Message Viewer	user
	Download	Download	admin
	Network Capture	Network Capture	admin

8.6.2 Ogólne informacje o stronie

W pasku przeglądarki internetowej wyświetlony zostaje adres IP danego urządzenia.

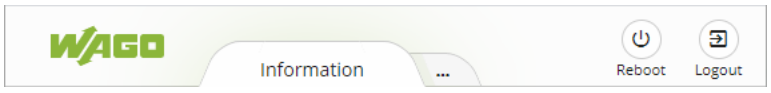
Strony WMB wyświetlane są dopiero po zalogowaniu. Aby się zalogować, należy wpisać w oknie logowania nazwę użytkownika i hasło, a następnie kliknąć przycisk **[Login]**.



Ilustracja 18: 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.

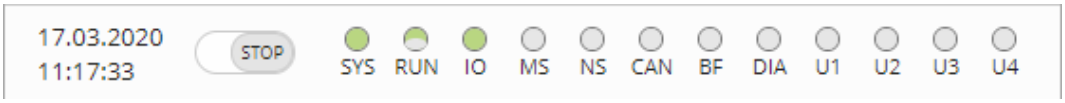
Gdy na wybranej szerokości okna nie mieszczą się wszystkie zakładki, w miejscu niewyświetlonej zakładki widoczna jest zakładka z symbolem (…). Dzięki temu poprzez listę rozwijalną można wybrać zakładki, które nie są wyświetlane.



Ilustracja 19: 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 20: Wiersz statusu WBM (przykład)

- Data i godzina – lokalny czas i lokalna data na urządzeniu
- Stan przełącznika trybu pracy
- Stany LED urządzenia:
  LED posiadają odpowiednie opis (np. SYS, RUN, ...), a ich stany są przedstawione w sposób graficzny.
  Możliwe są następujące stany LED:

  - kolor szary: LED jest wyłączona.
  - kolor na całej powierzchni: LED jest włączona i ma odpowiedni kolor.
  - kolor na połowie powierzchni: LED miga w odpowiednim kolorze. Druga połówka powierzchni jest wtedy szara lub może również mieć jakiś kolor. Ten ostatni przypadek oznacza, że LED miga w różnych kolorach.

  Po najechaniu kursorem na LED otwiera się tooltip, zawierający dalsze informacje. Wyświetlony tekst zawiera komunikat, który wprowadził LED w aktualny stan. Podana jest też godzina komunikatu.
  Stany wyświetlone w WBM nie odpowiadają w każdym momencie aktualnym stanom urządzenia. Transmisja danych wymaga określonego czasu, a odpytywanie następuje w określonych interwałach. Czas między odpytywaniami wynosi 30 sekund.

Wskazówka

Po zmianach parametrów nie należy przeprowadzać restartu poprzez wyłączanie i ponowne załączanie!
Aby zmiany parametrów zostały zrealizowane, wymagany jest restart sterownika. Zapisanie zmian wymaga czasu.
W celu przeprowadzenia restartu nie należy włączać i wyłączać sterownika, ponieważ w efekcie zbyt wczesnego wyłączenia zmiany mogą zostać utracone.
Restart należy przeprowadzić tylko programowo poprzez funkcję Reboot. Dzięki temu wszystkie procesy zapisu zostaną przeprowadzone poprawnie i w pełni zakończone.

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

8.6.3 Funkcja Reboot

Kliknąć przycisk **[Reboot]**. Aby przeprowadzić restart, należy kliknąć przycisk **[Reboot]**. Aby anulować restart, należy kliknąć przycisk **[Cancel]**.

9 Środowisko systemowe CODESYS V3

9.1 Wskazówki ogólne

Informacja

Dodatkowa informacja

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

9.2 Priorytety CODESYS V3

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

Tabela 29: Priorytety CODESYS V3

Scheduler	Zadanie	Priorytet Linux®	Priorytet IEC	Komentarz
Preemptives Scheduling - Zakres czasu rzeczywistego	Magistrala systemowa lub obiektowa – HIGH	-95 … -86		Magistrala systemowa (-88)
	Monitorowanie przełącznika trybu pracy	-85		Zadanie rejestruje zmiany przełącznika trybu pracy i zmienia stan aplikacji PLC. (start, stop, zimny/gorący reset)
	Watchdog CODESYS	-83		Wykonywanie funkcjonalności watchdoga
	Zadania IEC cykliczne i sterownia 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) Master/slave Modbus (43)
	Zadania IEC cykliczne i sterownia zdarzeniami	-42 … -32	4 … 14	Dla zadań czasu rzeczywistego, których wykonanie nie może mieć wpływu na komunikację sieciową.
	Magistrala systemowa lub obiektowa – LOW	-13 … -4		
Fair Scheduling - Bez zakresu czasu rzeczywistego	Komunikacja CODESYS	Back-ground (20)		Komunikacja ze środowiskiem programistycznym CODESYS
	Zadania IEC cykliczne, dowolne i sterowania zdarzeniami		15	M.in. standardowe priorytety i zadania wizualizacji

9.3 Zakresy pamięci w CODESYS V3

Zakresy pamięci sterownika mają w CODESYS V3 następujące wielkości:

- Pamięć programowa: 32 MB
- Pamięć danych/znaczniki: 128 MB
- Dane wejściowe: 64 kB
- Dane wyjściowe: 64 kB
- Retain/tPersistent: 128 kByte
- Ograniczenie modułu: 12 * 4096 B = 48 kB

9.3.1 Pamięć programu i danych

Pamięć programu (także kodu) ma wielkość maksymalnie 32 MB.
Pamięć danych ma wielkość 128 MB.
Oba zakresy są od siebie odseparowane i w zależności od wielkości programu zostają udostępnione w systemie wraz z jego pobraniem. Ewentualne przekroczenie ograniczenia wartości sygnalizowane jest jako błąd.

9.3.2 Ograniczenie modułu

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

Wielkość zakresu pamięci obliczana jest z ograniczenia modułu * 12 (a więc 4096 bajtów * 12).

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

9.3.3 Pamięć RAM nieulotna

Dla aplikacji IEC 61131 dostępna pamięć nieulotna wynosi 128 kB.
Obszar nieulotny jest podzielony na obszar Retain i obszar Persistent. Obszary te są rozdzielane automatycznie przez CODESYS V3.

9.3.4 Dostęp do pliku z aplikacji IEC

Dostęp do plików przez aplikację IEC jest ograniczony do następujących katalogów:

- /home/codesys
- /media/sd
- /tmp

9.3.5 Zmiana ustawień sieci przez aplikację IEC

Aby ustawienia sieciowe mogły być zmieniane z poziomu aplikacji IEC lub poprzez sieć obiektową (np. PROFINET DCP), parametr „IP Source“ musi być ustawiony na „Iexternal“ (strona WBM „TCP/IP Configuration“ – grupa „Bridge Interfaces“).

Zmiana ustawień sieci przez aplikację IEC odbywa się np. poprzez zaznaczenie opcji „Adjust operating system settings” w CODESYS (podwójne kliknięcie na element „Ethernet (Ethernet)“ w drzewie urządzeń > Zakładka „General“ > opcja „Adjust operating system settings").

9.3.6 EtherCAT

Połączenie EtherCAT realizowane jest poprzez funkcjonalność CODESYS V3 i biblioteki CODESYS V3.

Aby móc korzystać z funkcji mastera EtherCAT, należy przełączyć interfejsy sieciowe z „switched” na „separated” (strona WBM „Ethernet Configuration“ – grupa „Bridge Configuration“) i zrestartować sterownik lub przynajmniej runtime, aby adresy MAC zostały przydzielone prawidłowo.
W celu skonfigurowania mastera EtherCAT dodanego do projektu wybrana zostaje odpowiednia karta sieciowa w CODESYS (dwukrotne kliknięcie na element „EtherCAT_Master“ w drzewie urządzeń > zakładka „General“ > „Source address MAC“ > przycisk [Select]).

10 Diagnostyka

Do celów diagnostycznych należy wykorzystywać wskazania LED statusu, umieszczonej z przodu urządzenia, oraz komunikaty o błędach wyświetlane w WBM w obszarze „Diagnostic“.
Wskaźniki oraz ich znaczenie są następujące:

Tabela 30: Sygnalizacja LED

Wskaźnik LED	Znaczenie
Zielony migający	Sterownik jest gotowy do pracy.
Czerwony migający	Wystąpił błąd. Wyświetlony zostaje odpowiedni komunikat błędu.
Niebieski migający	Wystąpił błąd połączenia ze sterownikiem; brak komunikacji.

W przypadku wystąpienia błędu połączenia należy sprawdzić:

- czy sterownik pracuje,
- czy ustawienia sieciowe są prawidłowe,
- czy adres URL sterownika jest prawidłowy.

Jeśli błędów nie uda się usunąć, należy skontaktować się z działem wsparcia technicznego WAGO. support@wago.com
Należy podać kolor wskaźnika LED.

Dziennik zdarzeń

W dzienniku zdarzeń protokołowane są komunikaty systemowe, np. „Start sterownika“ lub „Przerwanie komunikacji“.
Dziennik zdarzeń można odczytać w WBM w zakładce „Diagnostic“.

11 Serwis

11.1 Zmiana konfiguracji przy użyciu WBM

U góry znajduje się **przycisk „CFG/RST“.** Można nim otworzyć system zarządzania przez WWW (WBM) w celu konfiguracji urządzenia. Przycisk można nacisnąć szpiczastym, niemetalowym przedmiotem.
Podczas działania wizualizacji zostaje w ten sposób otwarty system WBM. Podczas startu (Power ON) urządzenia zatrzymana zostaje lista autostartu i urządzenie uruchamia tylko system WBM. Przycisk nie wprowadza zmian w ustawieniach.

11.2 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

Uwzględnić dokumentację dla docelowej wersji firmware'u!
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.

Dlatego po zmianie firmware'u należy korzystać z dokumentacji odpowiadającej docelowemu firmware'owi.

W razie pytań należy skontaktować się z pomocą WAGO.

Firmware można aktualizować na dwa różne sposoby:

- przy użyciu WAGOupload
- przy użyciu karty pamięci i WBM

11.2.1 Przeprowadzanie aktualizacji/aktualizacji wstecznej przy użyciu WAGOupload

1. Uruchom WAGOupload.
2. Kliknij funkcję **[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 przycisk **[Next]**.
8. Potwierdź listę przyciskiem **[Next]**.
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.

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

Aby wgrać do sterownika wyższą lub niższą wersję firmware'u, należy postępować w następujący sposób:

1. Najpierw skopiuj obraz 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 nowym firmware'em do gniazda. Należy ewentualnie zastosować specjalny obraz aktualizacji wstecznej (patrz wyżej).
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.

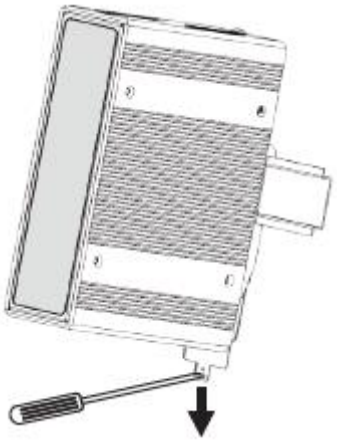
Sterownik uruchamiany jest teraz z nową wersją firmware'u.

12 Demontaż

12.1 Demontaż z szyny

1. W celu demontażu należy pociągnąć zaczep do dołu. Należy użyć do tego śrubokręta lub przyrządu montażowego.

2. Następnie ruchem wahadłowym zdjąć produkt z szyny montażowej,



Ilustracja 21: Demontaż z szyny

13 Utylizacja

13.1 Sprzęt elektryczny i elektroniczny

Sprzętu elektrycznego i elektronicznego nie należy utylizować razem z odpadami komunalnymi. Dotyczy to także produktów bez tego znaku.

Urządzenia elektryczne i elektroniczne zawierają surowce, materiały i substancje, które mogą być szkodliwe dla środowiska oraz zdrowia. Wycofane z eksploatacji urządzenia elektryczne i elektroniczne należy utylizować zgodnie z przepisami. Na terenie Europy obowiązuje dyrektywa WEEE 2012/19/EU. W poszczególnych krajach mogą obowiązywać osobne dyrektywy i ustawy.

Prawidłowa utylizacja służy zachowaniu zdrowia, chroni środowisko przed szkodliwymi substancjami pochodzącymi z urządzeń elektrycznych i elektronicznych.

- Należy przestrzegać krajowych i lokalnych przepisów dotyczących utylizacji sprzętu elektrycznego i elektronicznego.
- Przed utylizacją należy usunąć dane zapisane w urządzeniach elektrycznych i elektronicznych.
- Ze sprzętu należy wyjąć zamontowane ewentualnie baterie, akumulatory i karty pamięci.
- Urządzenia elektryczne i elektroniczne należy oddać do lokalnych punktów zbiórki odpadów.

Nieprawidłowa utylizacja sprzętu elektrycznego i elektronicznego może mieć negatywny wpływ na zdrowie ludzi i środowisko.

13.2 Opakowanie

Opakowanie zawiera materiały, które mogą być użyte ponownie.
Na terenie Europy obowiązują dyrektywy dotyczące opakowań PPWD 94/62/EU i 2004/12/EU. W poszczególnych krajach mogą obowiązywać osobne dyrektywy i ustawy.

Prawidłowa utylizacja opakowań chroni środowisko oraz umożliwia zrównoważone i efektywne wykorzystanie zasobów.

- Należy przestrzegać krajowych i lokalnych przepisów dotyczących utylizacji opakowań.
- Wszystkie opakowania należy zutylizować w sposób, zapewniający odpowiednio wysoki poziom recyklingu, odzysku oraz ponownego użycia surowców.

Nieprawidłowa utylizacja opakowań może mieć szkodliwy wpływ na środowisko i przyczyniać się do marnotrawstwa surowców.

14 Akcesoria

Dla produktu dostępnych jest szereg certyfikowanych akcesoriów.

Tabela 31: Akcesoria – karty pamięci

Karta pamięci microSD, 1 Gbyte	758-879/000-002
Karta pamięci microSD, 2 Gbyte	758-879/000-3102

Tabela 32: Akcesoria – przewody przyłączeniowe i wtyki

Przewód przyłączeniowy USB A-B, 3 m	758-879/000-101
Gniazdo (wielowtyk) do podłączania napięcia zasilającego	734-103
Wtyczka sieci obiektowej CANopen	750-963

15 Załącznik

15.1 Dialogi konfiguracyjne

15.1.1 Web Based Management (WBM)

15.1.1.1 Zakładka „Information“

15.1.1.1.1 Strona „Device Status“

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

Grupa „Device Details“

W tej grupie wyświetlane są dane identyfikacyjne produktu.

Tabela 33: Strona WBM „Device Status“ – grupa „Device Details“

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

Grupa „Network TCP/IP Details“

W tej grupie wyświetlane są właściwości sieci i złącz produktu.

Tabela 34: Strona WBM „Device Status“ – grupa „Network TCP/IP Details“

Parametr	**Znaczenie**	
Bridge <n>	Aktualnie skonfigurowany bridge; dla każdego skonfigurowanego bridge'a właściwości są wyświetlane w osobnym obszarze.	
Mac Address	Adres MAC, służący do identyfikacji i adresowania produktu	
IP Source	Aktualne odniesienie adresu IP	
	none	Nie została wybrana metoda przydzielania adresów IP; ma to miejsce np. wtedy, gdy bridge został dodany przez zmiany w konfiguracji bridge'ów. W zakładce **Configuration** na stronie **Networking** > **TCP/IP Configuration** należy wybrać źródło.
	static IP	Statyczne przydzielanie adresów
	dhcp	Dynamiczne przydzielanie adresów IP poprzez DHCP
	bootp	Dynamiczne przydzielanie adresów IP poprzez BootP (gdy BootP jest obsługiwany)
	external	Adres IP przypisywany jest ewentualnie przez aplikację sieciową; ma to miejsce na przykład wtedy, gdy adres IP zarządzany jest przez aplikację.
IP Address	Aktualny adres IP produktu	
Subnet Mask	Aktualna maska podsieci produktu	

15.1.1.1.2 Strona „Vendor Information“

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

15.1.1.1.3 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 35: Strona WBM „PLC Runtime Information” – grupa „Runtime“

Parametr	Znaczenie
Wersja	Tu wyświetlana jest wersja aktywowanego systemu runtime. Przy wyłączonym systemie runtime wyświetlana jest informacja „None“.

Grupa „WebVisu“

Tu znajduje się link, którym można otworzyć WebVisu.

15.1.1.1.4 Strona „WAGO Software License Agreement“

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

15.1.1.1.5 Strona „Open Source Licenses“

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

15.1.1.1.6 Strona „WBM Third Party License Information“

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

15.1.1.1.7 Strona „Trademarks Information“

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

15.1.1.1.8 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.

15.1.1.2 Zakładka „Configuration“

15.1.1.2.1 Strona „PLC Runtime Configuration“

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

Grupa „General PLC Runtime Configuration“

Tabela 36: Strona WBM „PLC Runtime Configuration” – grupa „General PLC Runtime Configuration“

Parametr	Znaczenie	
PLC runtime version	Tu można wybrać, który system runtime PLC jest aktywowany.	
	none	Żaden system runtime nie jest aktywowany.
	CODESYS V3	System runtime CODESYS V3 jest aktywowany.
Home directory on memory card enabled	Tu ustawia się, czy katalog Home dla systemu runtime ma być zapisywany na karcie pamięci.	
	Disabled	Katalog Home dla systemu operacyjnego zapisywany jest w wewnętrznej pamięci sterownika.
	Enabled	Katalog Home dla systemu operacyjnego zapisywany jest na karcie pamięci.

Wskazówka

Przy przełączeniu systemu runtime usuwane są wszystkie dane!
Przy przełączeniu systemu runtime katalog Home dla systemu operacyjnego zostaje całkowicie usunięty.

Wskazówka

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

Aby przejąć zmiany, należy kliknąć odpowiedni przycisk **[Submit]**. Zmiana systemu runtime zostaje 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!

Grupa „Webserver Configuration“

Tabela 37: Strona WBM „PLC Runtime Configuration” – grupa „Webserver Configuration“

Parametr	Znaczenie	
CODESYS 3 Webserver State	Tu wyświetlany jest status (enabled/disabled) serwera WWW CODESYS V3.	
Default Webserver	Tu można wybrać, czy przy wpisaniu adresu IP sterownika ma być wyświetlany Web-Based-Management, czy wizualizacja sieciowa systemu runtime.	
	Zarządzanie przez stronę WWW	Wyświetlany jest Web-Based-Management.
	WebVisu	Wyświetlana jest wizualizacja sieciowa systemu runtime.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

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

15.1.1.2.2 Strona „TCP/IP Configuration“

Na stronie „TCP/IP Configuration“ znajdują się ustawienia TCP/IP dla złącz sieci ETHERNET.

Grupa „TCP/IP Configuration“

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

Tabela 38: Strona WBM „TCP/IP Configuration“ – grupa „TCP/IP Configuration“

Parametr	**Znaczenie**	
Network Details Bridge <n>	Ustawienia dla aktualnie skonfigurowanego bridge'a	
Current IP Address	Tu wyświetlany jest aktualny adres IP.	
Current Subnet Mask	Tu wyświetlana jest aktualna maska podsieci.	
Current Default Gateway	Tu wyświetlany jest adres IP aktualnej domyślnej bramy.	
IP Source	Tu można zdecydować, czy ma być zastosowane statyczne czy dynamiczne adresowanie IP.	
	Static IP	Statyczne adresowanie IP
	DHCP	Dynamiczne adresowanie IP przez DHCP
	BootP	Dynamiczne adresowanie IP przez BootP
	external	Adres IP przypisywany jest ewentualnie przez aplikację sieciową; ma to miejsce na przykład wtedy, gdy adres IP zarządzany jest przez aplikację.
IP Address	Tu wpisuje się statyczny adres IP. Jest ona aktywna, gdy w polu **IP Source** zaznaczony jest „Static IP“.	
Subnet Mask	Tu należy wpisać maskę podsieci. Jest ona aktywna, gdy w polu **IP Source** zaznaczony jest „Static IP“.	
Default Gateway	Tu wpisuje się adres IP domyślnej bramy.	

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

Grupa „DNS Server“

Tabela 39: Strona WBM „TCP/IP Configuration“ – grupa „DNS Server“

Parametr	Znaczenie
aktywny	Tu wyświetlane są aktywne serwery DNS. Można użyć maksymalnie 3 aktywnych serwerów DNS. Indeks odzwierciedla kolejność zapytań. Pierwszy serwer DNS przydzielony przez DHCP otrzymuje najwyższy priorytet.
Assigned by DHCP	Tu wyświetlane są serwery DNS przydzielone przez DHCP (lub BootP). Jeśli nie został przydzielony serwer DNS przez DHCP (lub BootP), wyświetlana jest informacja „no DNS Servers assigned by DHCP“.
Assigned by user	Tu wyświetlane są adresy wpisanych serwerów DNS. Jeśli nie został wpisany serwer DNS, wyświetlana jest informacja „no DNS Servers configured“.
New Server IP	Tu dodaje się kolejne adresy serwera DNS. Można wpisać maksymalnie 3 adresy. Wpisy zastosowane w rzeczywistości wynikają z alternatywnej kombinacji list „Assigned by DHCP“ i „Assigned by user“.

Aby usunąć wybrany serwer DNS, należy kliknąć przycisk **[Delete]**. Zmiana zostaje zrealizowana natychmiast.

Aby dodać wpisany serwer DNS, należy kliknąć przycisk **[Add]**. Zmiana zostaje zrealizowana natychmiast.

15.1.1.2.3 Strona „Ethernet Configuration“

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

Grupa „Bridge Configuration“

Tabela 40: Strona WBM „Ethernet Configuration“ – grupa „Bridge Configuration“

Parametr	Znaczenie
Bridge 1 … <n>	Tu przyporządkowuje się fizyczne porty X1 … X<n> do bramy logicznej. W tym celu należy nacisnąć odpowiedni przycisk opcji. Przyporządkowanie zostaje zaznaczone kolorem. Jeden port może być przyporządkowany do tylko jednej bramy.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

Grupa „Switch Configuration“

Grupa ta widoczna jest tylko wtedy, gdy obsługiwana jest konfiguracja parametrów.

Tabela 41: Strona WBM „Ethernet Configuration“ – grupa „Switch Configuration“

Parametr	Znaczenie	
Port Mirror	Tu włącza się i wyłącza mirroring między portami.	
	None	Oba porty ETHERNET pracują normalnie.
	X1	Wymiana danych między X1 i systemem PFC jest odzwierciedlana na porcie X2.
	X2	Wymiana danych między X2 i systemem PFC jest odzwierciedlana na porcie X1.
Broadcast Protection	Tu ustawia się ograniczenie broadcast jako zabezpieczenie przed przeciążeniem.	
	Disabled	Brak ograniczenia pakietów broadcast
	1 % … 5 %	Limitowanie przychodzących pakietów broadcast do wybranej wartości procentowej ogólnej możliwej przepustowości (10/100Mbit).
Rate Limit	Tu ustawia się podstawowe ograniczenie przychodzącej transmisji danych.	
	Disabled	Brak limitu dla przychodzącej transmisji danych.
	64 kbps … 99 mbps	Limit do podanej wielkości dla przychodzącej transmisji danych.

Aby przejąć zmiany, należy kliknąć odpowiedni przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

Grupa „Dummy Interfaces“

Tabela 42: Strona WBM „Ethernet Configuration“ – grupa „Dummy Interfaces“

Parametr	Znaczenie
Name	Nazwa wybranego interfejsu Dummy
Add Dummy Interface	Tworzenie nowego interfejsu Dummy
Name	Wprowadzanie nazwy nowego interfejsu Dummy

Aby usunąć wybraną pozycję, należy kliknąć przycisk **[Delete]**. Zmiany zostają zrealizowane natychmiast.

Aby dodać nową pozycję, należy kliknąć przycisk **[Add]**. Zmiany zostają zrealizowane natychmiast.

Grupa „VLAN Interfaces“

Tabela 43: 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
Add	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

Aby usunąć wybraną pozycję, należy kliknąć przycisk **[Delete]**. Zmiany zostają zrealizowane natychmiast.

Aby dodać nową pozycję, należy kliknąć przycisk **[Add]**. Zmiany zostają zrealizowane natychmiast.

Grupa „Ethernet Interface Configuration“

Tabela 44: Strona WBM „Ethernet Configuration“ – grupa „Ethernet Interface Configuration“

Parametr	Znaczenie
Interface X<n>	Dla każdego interfejsu zintegrowanego w sterowniku wyświetlany jest osobny obszar.
Enabled	Tu można aktywować lub dezaktywować interfejs.
MAC Learning	Tu można dezaktywować lub aktywować „MAC Learning“.
Speed/Dupleks	Tu można wybrać prędkość i typ transmisji Generowana lista wyboru jest uzależniona od urządzenia i interfejsu. Przy aktywowanej opcji „Autonegotiation“ tryby łączeniowe negocjowane są automatycznie z urządzeniem przeciwstawnym.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiany zostają zrealizowane natychmiast.

15.1.1.2.4 Strona „Configuration of Host and Domain Name“

Na stronie „Configuration of Host and Domain Name“ znajdują się ustawienia nazwy hosta i domeny.

Grupa „Hostname“

Tabela 45: Strona WBM „Configuration of Host and Domain Name“ – grupa „Hostname“

Parametr	Znaczenie
Currently used	Jeśli została wybrana opcja dynamicznego przydzielania adresu IP przez DHCP, w tym miejscu zostaje wyświetlona nazwa aktualnie zastosowanego hosta.
Configured	Tu wpisuje się nazwę hosta produktu, która ma być potem stosowana, gdy interfejs sieciowy zostanie zmieniony na statyczny adres IP lub gdy przez odpowiedź DHCP nie jest podawana nazwa hosta.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**.

Aby zresetować pole edycji, należy kliknąć przycisk **[Clear]**.

Zmiana zostaje zrealizowana natychmiast.

Jeśli sterownik otrzymał nazwę hosta przez DHCP, jest ona preferowana i ręcznie skonfigurowana nazwa nie jest używana.
Aby przejąć ręcznie skonfigurowaną nazwę hosta, należy w razie potrzeby zredukować konfigurację serwera DHCP o przypisanie nazwy hosta.

Grupa „Domain Name“

Tabela 46: Strona WBM „Configuration of Host and Domain Name“ – grupa „Domain Name“

Parametr	Znaczenie
Currently used	Jeśli została wybrana opcja dynamicznego przydzielania adresu IP przez DHCP, w tym miejscu zostaje wyświetlona nazwa aktualnie zastosowanej domeny.
Configured	Tu wpisuje się nazwę domeny produktu, która ma być potem stosowana, gdy interfejs sieciowy zostanie zmieniony na statyczny adres IP lub gdy przez odpowiedź DHCP nie jest podawana nazwa hosta.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**.

Aby zresetować pole edycji, należy kliknąć przycisk **[Clear]**.

Zmiana zostaje zrealizowana natychmiast.

Jeśli sterownik otrzymał przez DHCP nazwę domeny, jest ona preferowana i ręcznie skonfigurowana nazwa nie jest używana.

Aby przejąć ręcznie skonfigurowaną nazwę domeny, należy w razie potrzeby zredukować konfigurację serwera DHCP o przypisanie nazwy domeny.

15.1.1.2.5 Strona „Routing“

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

Grupa „IP Forwarding through multiple interfaces“

Tabela 47: Strona WBM „Routing“ – grupa „IP Forwarding through multiple interfaces“

Parametr	Znaczenie
Enabled	Tu definiuje się, czy dozwolone jest przesyłanie dalej pakietów danych między różnymi interfejsami sieciowymi. Jeśli pole wyboru nie jest zaznaczone, zastosowane zostają ustawienia „Static Routes“, a wtedy pakiety danych IP, docierające do sterownika na jednym interfejsie sieciowym, nie mogą opuścić sterownika na innym interfejsie sieciowym. Jeśli pole wyboru jest zaznaczone, pakiety IP mogą być przesyłane dalej między interfejsami. Wymagane jest wtedy wprowadzenie dalszych ustawień na stronie WBM.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiany zostają zrealizowane 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 48: Strona WBM „Routing“ – grupa „Custom Routes“

Parametr	Znaczenie	
Enabled	Tu można zdecydować, czy wybrana trasa ma być zastosowana.	
	Disabled	Trasa nie jest zastosowana.
	Enabled	Trasa jest zastosowana.
Destination Address	Tu definiuje się, czy dostępni mają być dowolni uczestnicy komunikacji sieciowej, czy też tylko określone urządzenie lub urządzenie z danej puli adresów.	
	Default	Dostępni są dowolni uczestnicy komunikacji sieciowej.
	Network address	Dostępne jest tylko określone urządzenie lub urządzenie z danej puli adresów.
Destination Mask	Tu wpisuje się maskę podsieci urządzenia. Jeśli Destination Address jest zdefiniowany jako „default“, należy tu wpisać wartość „0.0.0.0“.	
Gateway Address	Tu ustawia się adres bramy. Jeśli pole „Interface“ jest puste, należy tu wpisać wartości. Jeśli w polu „Interface“ wpisana jest wartość, wypełnienie tego pola jest opcjonalne.	
Gateway Metric	Tu ustawia się liczbę, będącą metryką. Przy kilku trasach o tym samym adresie docelowym (Destination Address) i masce (Destination Mask) to metryka decyduje, do której bramy w pierwszej kolejności wysyłane są pakiety danych. Preferowane są trasy z niższą metryką. Najmniejsza wartość wynosi 0. Największa wartość to 2^{32}-1 = 4.294.967.295.	
Interface	Tu wpisuje się interfejs, przez który kierowane są pakiety wysyłane na adres docelowy (Destination Adress). Można zastosować bridge (br0-br3) jak również modemy (wwan0) lub nazwy interfejsów VPN. Jeśli pole „Gateway Address“ jest puste, należy tu wpisać wartość. Jeśli w polu „Gateway Address“ wpisana jest wartość, wypełnienie tego pola jest opcjonalne.	

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiany zostają zrealizowane natychmiast.

Aby dodać nową trasę, należy kliknąć przycisk **[Add]**. Zmiana zostaje zrealizowana natychmiast.

Aby usunąć istniejącą trasę, należy kliknąć przycisk **[Delete]**. Zmiana zostaje zrealizowana natychmiast.

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 routes)“.

Grupa „IP-Masquerading“

Dla każdego parametru wyświetlany jest osobny obszar. Jeśli nie ma tu wprowadzonych ustawień, wyświetlana jest informacja „(no masquerading configured)“.

Tabela 49: Strona WBM „Routing“ – grupa „IP-Masquerading“

Parametr	Znaczenie	
Enabled	Tu można zdecydować, czy ma być zastosowany IP-Masquerading	
	Disabled	IP-Masquerading nie jest zastosowany.
	Enabled	IP-Masquerading jest zastosowany.
Interface	Tu można wybrać jedną z proponowanych nazw dla interfejsu sieciowego. Wybierając „other“ można alternatywnie wpisać dowolną nazwę interfejsu sieciowego.	

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiany zostają zrealizowane natychmiast.

Aby dodać nową pozycję, należy kliknąć przycisk **[Add]**. Zmiana zostaje zrealizowana natychmiast.

Aby usunąć daną pozycję, należy kliknąć przycisk **[Delete]**. Zmiana zostaje zrealizowana natychmiast.

Pozycja zostaje wprowadzona do systemu tylko wtedy, gdy zaznaczona jest opcja „Enable“ w grupie „General Routing Configuration“. W ten sposób można wprowadzić wstępnie dane ustawienie, które zostanie przejęte dopiero w momencie generalnego załączenia.

Grupa „Port Forwarding“

Dla każdego parametru wyświetlany jest osobny obszar. Jeśli nie ma tu wprowadzonych ustawień, wyświetlana jest informacja „(no Port Forwarding configured)“.

Tabela 50: Strona WBM „Routing“ – grupa „Port Forwarding“

Parametr	Znaczenie	
Enabled	Tu można zdecydować, czy ma być zastosowany Port Forwarding.	
	Disabled	Port Forwarding nie jest zastosowany.
	Enabled	Port Forwarding jest zastosowany.
Interface	Tu można wybrać jedną z proponowanych nazw dla interfejsu sieciowego. Wybierając „other“ można alternatywnie wpisać dowolną nazwę interfejsu sieciowego.	
Port	Tu wpisuje się port, po którym przesyłane pakiety danych mają dotrzeć do produktu.	
Protocol	Tu można wybrać protokół, który ma być uwzględniony dla Port Forwarding. Do wyboru są protokoły TCP, UDP lub oba.	
Destination Address	Tu ustawia się adres sieciowy urządzenia docelowego. Adres ten zastępuje pierwotny adres docelowy pakietu danych.	
Destination Port	Tu ustawia się numer portu urządzenia docelowego. Wartość ta zastępuje pierwotny port docelowy pakietu danych.	

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiany zostają zrealizowane natychmiast.

Aby dodać nową pozycję, należy kliknąć przycisk **[Add]**. Zmiana zostaje zrealizowana natychmiast.

Aby usunąć daną pozycję, należy kliknąć przycisk **[Delete]**. Zmiana zostaje zrealizowana natychmiast.

Pozycja zostaje wprowadzona do systemu tylko wtedy, gdy zaznaczona jest opcja „Enable“ w grupie „General Routing Configuration“. W ten sposób można wprowadzić wstępnie dane ustawienie, które zostanie przejęte dopiero w momencie generalnego załączenia.

15.1.1.2.6 Strona „Clock Settings“

Na stronie „Clock Setting“ znajdują się ustawienia daty i godziny.

Grupa „Timezone and Format“

Tabela 51: Strona „Clock Setting“ – grupa „Timezone and Format“

Parametr	Znaczenie	
Timezone	Tu wybiera się strefę czasową odpowiednią dla danego kraju. Ustawienie podstawowe:	
	AST/ADT	„Atlantic Standard Time“, Halifax
	EST/EDT	„Eastern Standard Time“, New York, Toronto
	CST/CDT	„Central Standard Time“, Chicago, Winnipeg
	MST/MDT	„Mountain Standard Time“, Denver, Edmonton
	PST/PDT	„Pacific Standard Time“, Los Angeles, Whitehouse
	GMT/BST	„Greenwich Mean Time“, GB, P, IRL, IS, …
	CET/CEST	„Central European Time“, B, DK, D, F, I, CRO, NL, …
	EET/EEST	„East European Time“, BUL, FI, GR, TR, …
	CST	„China Standard Time“
	JST	„Japan/Korea Standard Time“
TZ String	W przypadku strefy czasowej, która nie została uwzględniona w parametrach „Time Zone“ wpisuje się nazwę danej strefy czasowej lub kraj i miasto, które się w niej znajdują. Oficjalną nazwę strefy czasowej można znaleźć na stronie: http://www.timeanddate.com/time/map/	
Time Format	Przełączanie między zegarem 12- i 24-godzinnym	

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

Grupa „UTC Time and Date“

Tabela 52: Strona WBM „Clock Settings“ – grupa „UTC Time and Date“

Parametr	Znaczenie
UTC Date	Tu ustawia się datę.
UTC Time	Tu ustawia się czas uniwersalny (GMT).

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

Grupa „Local Time and Date“

Tabela 53: Strona WBM „Clock Settings“ – grupa „Local Time and Date“

Parametr	Znaczenie
Local Date	Tu ustawia się datę.
Loacl Time	Tu ustawia się lokalny czas.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

15.1.1.2.7 Strona „Configuration of Serial Interface RS232/RS485“

Na stronie „Configuration of Serial Interface RS232/RS485“ znajdują się ustawienia dla interfejsu szeregowego.

Grupa „Serial Interface assigned to“

Tu wyświetlana jest aplikacja, do której przypisany jest aktualny interfejs szeregowy, oraz tryb interfejsu.

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“

Tu można wybrać aplikację, której przypisany został interfejs szeregowy po kolejnym restarcie sterownika.

Tabela 54: Strona WBM „Configuration of Serial Interface RS232” – grupa „Assign Owner of Serial Interface“

Parametr	Znaczenie
Linux® Console	Tu przypisuje się interfejs szeregowy do konsoli Linux®.
Unassigned (usage by Applications, Libraries, CODESYS)	Tu deklaruje się, że interfejs szeregowy nie jest przypisany do żadnej aplikacji i jest wolny, a więc można na przykład wykorzystać go w celu umożliwienia dostępu dla programu CODESYS przez bloki funkcyjne.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostanie zrealizowana dopiero po następnym restarcie sterownika. W tym celu należy skorzystać z funkcji Reboot WBM. Nie należy wyłączać sterownika zbyt wcześnie!

Grupa „Assign Mode of Serial Interface“

Tu można wybrać tryb, w którym interfejs szeregowy będzie pracować po następnym restarcie sterownika. Zmiana trybu jest możliwa tylko wtedy, gdy interfejs szeregowy ma wartość „Unassigned“.

Tabela 55: Strona WBM „Configuration of Serial Interface RS232” – grupa „Assign Owner of Serial Interface“

Parametr	Znaczenie
RS-232	Tu deklaruje się, że interfejs szeregowy pracuje w trybie „RS-232“.
RS-485	Tu deklaruje się, że interfejs szeregowy pracuje w trybie „RS-485“.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostanie zrealizowana dopiero po następnym restarcie sterownika. W tym celu należy skorzystać z funkcji Reboot WBM. Nie należy wyłączać sterownika zbyt wcześnie!

15.1.1.2.8 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 56: Strona WBM „Configuration of Service Interface” – grupa „ Assign Owner of Service Interface“

Parametr	Znaczenie
WAGO Service Communication	Tu deklaruje się, że złącze serwisowe wykorzystywane jest do komunikacji serwisowej WAGO lub komunikacji z systemem runtime.
Linux Console	Tu przypisuje się złącze serwisowe do konsoli Linux®.
Unassigned (usage by Applications, Libraries, CODESYS)	Tu deklaruje się, że złącze serwisowe nie jest przypisane do żadnej aplikacji i jest wolne, a więc można na przykład wykorzystać je w celu umożliwienia dostępu dla programu CODESYS przez bloki funkcyjne.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostanie zrealizowana dopiero po następnym restarcie sterownika. W tym celu należy skorzystać z funkcji Reboot WBM. Nie należy wyłączać sterownika zbyt wcześnie!

15.1.1.2.9 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 57: Strona WBM „Create bootable Image” – grupa „Create bootable image from boot device“

Parametr	**Znaczenie**		
Boot Device	Tu wyświetlane jest medium, z którego przeprowadzony był rozruch.		
Destination	W zależności od tego, z którego medium przeprowadzony był rozruch, po procesie bootowania można wybrać następujący cel dla utworzonego obrazu:		
	System bootowany z		Docelowa partycja dla „bootable Image“
	Karta pamięci	→	Internal Flash
	Pamięć wewnętrzna	→	Memory Card

- Wolna pamięć na urządzeniu docelowym:
  Jeśli wolne miejsce w pamięci wynosi mniej niż 5%, wysyłane jest odpowiednie ostrzeżenie. Mimo to można rozpocząć kopiowanie. Jeśli wolnego miejsca jest zdecydowanie za mało, wysyłany jest odpowiedni komunikat, a proces kopiowania nie może się rozpocząć.

- Device w użyciu przez CODESYS:
  Jeśli urządzenie jest używane przez CODESYS, wysyłany jest odpowiedni komunikat. Mimo to można rozpocząć kopiowanie, jednak nie jest to zalecane!

Aby rozpocząć kopiowanie, należy kliknąć przycisk **[Start Copy]**. Po pozytywnym wyniku testu proces rozpoczyna się od razu. Jeśli zostały wykryte błędy, wyświetlany jest odpowiedni komunikat i proces nie jest realizowany. Jeśli istnieją ostrzeżenia, są one jeszcze raz wyświetlane i należy potwierdzić, że mimo to można kontynuować proces.

15.1.1.2.10 Strona „Firmware Backup“

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

Grupa „Firmware Backup“

Tabela 58: Strona WBM „Firmware Backup“ – grupa „Firmware Backup“

Parametr	Znaczenie	
Boot Device	Tu wyświetlany jest nośnik pamięci, z którego przeprowadzony był rozruch.	
Destination	Tu wybiera się miejsce zapisu dla backupu.	
	Memory Card	Dane zostają zapisane na karcie pamięci. Ta możliwość wyboru widoczna jest tylko wtedy, gdy wetknięta jest karta pamięci i nie był z niej przeprowadzony rozruch.
	Network	Dane zapisywane są w systemie plików i udostępniane na PC do pobrania.
PLC Runtime Project	To pole wyboru należy zaznaczyć, gdy chce się zapisać projekt runtime'u PLC.	
Settings	To pole wyboru należy zaznaczyć, gdy chce się zapisać ustawienia urządzenia.	
System	To pole wyboru należy zaznaczyć, gdy chce się utworzyć kopię zapasową systemu operacyjnego urządzenia i głównego systemu plików.	
Encryption	To pole wyboru należy zaznaczyć, gdy chce się zapisać zaszyfrowane dane.	
Encryption passphrase	Tu wpisuje się hasło szyfrowania. Pole edycji widoczne jest tylko wtedy, gdy zaznaczone jest pole wyboru Encryption.	
Confirm passphrase	Tu ponownie wpisuje się hasło szyfrowania w celu potwierdzenia. Pole edycji widoczne jest tylko wtedy, gdy zaznaczone jest pole wyboru Encryption.	

Wskazówka

Uwzględnić wersję firmware'u!
Odświeżenie systemu operacyjnego sterownika (opcja „System“) dozwolone i możliwe jest tylko wtedy, gdy wersje firmware'u w momencie zabezpieczenia i przywracania są takie same.
Należy wtedy zrezygnować z odświeżenia systemu operacyjnego sterownika lub zrównać uprzednio wersje firmware'u sterownika z wersją firmware'u w momencie zabezpieczania.

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

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

Aby rozpocząć proces backupu, należy kliknąć przycisk **[Create Backup]**.

15.1.1.2.11 Strona „Firmware Restore“

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

Grupa „Firmware Restore“

Tabela 59: 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.
	Network	Dane do odświeżenia pobrane zostają z PC.
Boot Device	Tu wyświetlany jest nośnik pamięci, z którego przeprowadzony był rozruch.	
PLC Runtime Project	Tu wpisuje się nazwę pliku archiwalnego projektu CODESYS. Pole edycji aktywne jest tylko wtedy, gdy jako źródło danych wybrana jest sieć.	
Settings	Tu wpisuje się nazwę pliku archiwalnego dla ustawień. Pole edycji aktywne jest tylko wtedy, gdy jako źródło danych wybrana jest sieć.	
System	Tu wpisuje się nazwę pliku kopii zapasowej danych systemowych i głównego systemu plików. Pole edycji aktywne jest tylko wtedy, gdy jako źródło danych wybrana jest sieć.	
Decryption	To pole wyboru należy zaznaczyć, gdy chce się zapisać zaszyfrowane dane.	
Decryption passphrase	Tu wpisuje się hasło szyfrowania. Pole edycji widoczne jest tylko wtedy, gdy zaznaczone jest pole wyboru Decryption.	

Wskazówka

Uwzględnić wersję firmware'u!
Odświeżenie systemu operacyjnego sterownika (opcja „System“) dozwolone i możliwe jest tylko wtedy, gdy wersje firmware'u w momencie zabezpieczenia i przywracania są takie same.
Należy wtedy zrezygnować z odświeżenia systemu operacyjnego sterownika lub zrównać uprzednio wersje firmware'u sterownika z wersją firmware'u w momencie zabezpieczania.

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 urządzenie było bootowane 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 przy odświeżaniu zmieniają się parametry połączenia ETHERNET, WBM nie będzie mógł potem nawiązać połączenia z urządzeniem. Trzeba wtedy ponownie otworzyć WBM, wpisując w pasku adresu poprawny adres IP urządzenia.

Wskazówka

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

Aby rozpocząć proces odświeżania, należy kliknąć przycisk **[Restore]**.

15.1.1.2.12 Strona „Active System“

Na stronie „Active System“ znajdują się ustawienia do wyboru partycji, z której ma być uruchamiany system.

Grupa „Boot Device“

Tabela 60: Strona WBM „Active System“ – grupa "Boot Device"

Parametr	Znaczenie
Boot Device	Tu wyświetlany jest nośnik pamięci, z którego przeprowadzony był rozruch.

Grupy „System <n> (Internal Flash)“

Tabela 61: Strona WBM „Active System“ – grupa „System <n> (Internal Flash)“

Parametr	Znaczenie	
Active	Tu wyświetlana jest informacja, czy system jest aktywny.	
Configured	Tu wyświetlana jest informacja, czy po następnym procesie Reboot system ma być aktywny.	
State	Tu wyświetlany jest status systemu.	
	good	System jest aktualny i może być wykorzystany.
	bad	System nie jest aktualny i nie może być wykorzystany.

Aby przy następnym procesie Reboot ponownie uruchomić żądany system, należy kliknąć odpowiedni przycisk **[Activate]**.

Wskazówka

Przygotować system bootowalny!
W systemie bootowalnym musi istnieć backup firmware'u!

15.1.1.2.13 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 62: Strona WBM „Mass Storage“ – grupa „Devices"

Parametr	Znaczenie
<Device>	Tu wyświetlany jest nośnik pamięci.
Boot device	Tu wyświetlana jest informacja, czy z tego nośnika pamięci przeprowadzony był rozruch.
Volume name	Tu wyświetlana jest nazwa pamięci.

Grupa „Create new Filesystem on Memory Card“

Tabela 63: Strona WBM „Mass Storage“ – grupa "Create new Filesystem on Memory Card“

Parametr	Znaczenie	
Filesystem type	Tu wybiera się format, w którym tworzy się nowy system danych na karcie pamięci.	
	Ext4	System danych tworzony jest w formacie Ext4. Danych nie można odczytać w systemie Windows!
	FAT	System danych tworzony jest w formacie FAT.
Label	Tu wpisuje się nazwę, jaką ma otrzymać nośnik pamięci przy formatowaniu.	

Wskazówka

Dane zostają usunięte!
Przy formatowaniu dane zapisane na nośniku pamięci zostają usunięte!

Aby sformatować dany nośnik pamięci, należy kliknąć **[Start Formatting]**.

15.1.1.2.14 Strona „Software Uploads“

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

Wskazówka

Instalować pliki IPK tylko z zaufanych źródeł!
Pliki IPK są instalowane z rozszerzonymi uprawnieniami (uprawnienia root), o ile w metadanych nie określono inaczej.
Należy zachować ostrożność przy instalacji plików IPK i instalować je tylko z zaufanych źródeł.

Tabela 64: Strona WBM „Software Uploads“ – grupa „Upload new Software“

Parametr	Znaczenie
Software file	Tu pojawia się nazwa pliku wybranego pakietu oprogramowania, dopóki nie zostanie on przesłany do produktu. Jeśli pakiet nie został jeszcze wybrany, pojawia się tekst „Choose ipk file...“. W tym celu należy kliknąć pole edycji i wybrać na komputerze plik z pakietem.

Aby zainstalować pakiet, należy kliknąć przycisk **[Install]**.

Po zainstalowaniu plik z pakietem oprogramowania zostaje usunięty z urządzenia. Jeśli nie jest to możliwe na skutek błędu w trakcie przetwarzania, usunięcie nastąpi najpóźniej przy kolejnym restarcie produktu.

15.1.1.2.15 Strona „Configuration of Network Services“

Na stronie „Configuration of Network Services“ znajdują się ustawienia dla różnego typu usług.

Wskazówka

Zamknąć nieużywane porty i usługi!
Przez otwarte porty i usługi osoby nieuprawnione mogą uzyskać dostęp do systemu automatyki.
Aby zredukować niebezpieczeństwo cyberataku, należy zamykać wszystkie porty i usługi w komponentach systemu sterowania, które nie są wykorzystywane przez aplikację (np. port 6626 dla WAGO-I/O-CHECK i port 11740 dla CODESYS V3).
Porty i usługi dobrze jest otwierać tylko na czas uruchamiania lub konfiguracji.

Grupa „FTP“

Tabela 65: Strona WBM „Configuration of Network Services“ – grupa „FTP“

Parametr	Znaczenie
Service active	Tu można aktywować/dezaktywować serwis FTP. W ustawieniach fabrycznych ta usługa nie jest aktywna.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

Grupa „FTPES (explicit FTPS)“

Tabela 66: Strona WBM „Configuration of Network Services“ – grupa „FTPES (explicit FTPS)“

Parametr	Znaczenie
Service active	Tu można aktywować/dezaktywować serwis FTPS. W ustawieniach fabrycznych ta usługa nie jest aktywna.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

Grupa „HTTP“

Tabela 67: Strona WBM „Configuration of Network Services“ – grupa „HTTP“

Parametr	Znaczenie
Service active	Tu można aktywować/dezaktywować serwis HTTP. W ustawieniach fabrycznych ta usługa nie jest aktywna.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

Wskazówka

Utrata połączeń przy dezaktywacji
Przy dezaktywacji serwisu HTTP połączenie z produktem może zostać przerwane. Należy wtedy ponownie otworzyć stronę.

Grupa „HTTPS“

Tabela 68: Strona WBM „Configuration of Network Services“ – grupa „HTTPS“

Parametr	Znaczenie
Service active	Tu wyświetlany jest status usługi HTTPS.

Grupa „I/O-*CHECK*“

Grupa ta widoczna jest tylko wtedy, gdy sterownik obsługuje WAGO-I/O-*CHECK*.

Tabela 69: Strona WBM „Configuration of Network Services“ – grupa „I/O-*CHECK*“

Parametr	Znaczenie
Service active	Tu można aktywować/dezaktywować serwis WAGO-I/O-*CHECK*.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

15.1.1.2.16 Strona „Configuration of NTP Client“

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

Grupa „NTP Client Configuration“

Tabela 70: Strona WBM „Configuration of NTP Client“ – grupa „NTP Client Configuration“

Parametr	Znaczenie
Service enabled	Tu można aktywować/dezaktywować aktualizację godziny.
Update Interval (sec)	Tu definiuje się interwał czasowy aktualizacji serwera czasu.
Time Server <n>	Tu wpisuje się adresy IP maksymalnie 4 serwerów czasu. Serwer czasu nr 1 odpytywany jest jako pierwszy. Jeśli nie można pobrać z niego danych, odpytywany jest serwer nr 2.
Additionally assigned (DHCP)	Tu wyświetlane są serwery NTP przydzielone przez DHCP (lub BootP). Jeśli nie został przydzielony serwer NTP przez DHCP (lub BootP), wyświetlana jest informacja („no additional servers assigned“).

Aby aktualizować czas niezależnie od interwału, należy kliknąć przycisk **[Update Time]**.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiany zostają zrealizowane natychmiast.

15.1.1.2.17 Strona „PLC Runtime Services“

Na stronie „PLC Runtime Services“ znajdują się ustawienia dla różnego typu usług systemu runtime.

Grupa „CODESYS V3“

Tabela 71: Strona WBM „PLC Runtime Services“ – grupa „CODESYS V3“

Parametr	Znaczenie
CODESYS V3 State	Tu wyświetlany jest status systemu runtime CODESYS V3 (enabled/disabled).
Webserver enabled	Tu aktywuje się i dezaktywuje serwer WWW dla wizualizacji WWW CODESYS V3.
Seperated WebVisu ports (8080/8081)	Tu definiuje się, czy wizualizacja sieciowa CODESYS V3 jest udostępniana na portach 8080/8081. W ustawieniu domyślnym wizualizacja sieciowa jest udostępniana na portach WBM 80/443.
Port authentication enabled	Tu definiuje się, czy dla połączenia z urządzeniem wymagany jest Log-in. Nazwa użytkownika to admin, a hasłem jest hasło podane w „General Configuration“.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**.
Zmiana uwierzytelnienia zostanie zrealizowana po następnym restarcie.
Wszystkie inne zmiany zostają zrealizowane natychmiast.

15.1.1.2.18 Strona „SSH Server Settings“

Na stronie „SSH Server Settings“ znajdują się ustawienia dla usługi SSH.

Grupa „SSH Server“

Tabela 72: Strona WBM „SSH Server Settings“ – grupa „SSH Server“

Parametr	Znaczenie
Service active	Tu włączą się i wyłącza serwer SSH.
Port Number	Tu wpisuje się numer portu.
Allow root login	Tu blokuje się lub zezwala na dostęp do katalogu głównego.
Allow password login	Tu aktywuje się i dezaktywuje pytanie o hasło.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiany zostają zrealizowane natychmiast.

15.1.1.2.19 Strona „DHCP Server Configuration“

Na stronie „DHCP Server Configuration“ znajdują się ustawienia dla usługi DHCP.

Grupa „DHCP Server Configuration Bridge <n>“

Tabela 73: Strona WBM „DHCP Server Configuration“ – grupa „DHCP Configuration Bridge <n>“

Parametr	Znaczenie
Service active	Tu włączą się i wyłącza usługę DHCP dla interfejsu X<n>.
Start IP for Range	Tu należy wpisać wartość początkową dostępnego zakresu adresów IP.
End IP for Range	Tu należy wpisać wartość końcową dostępnego zakresu adresów IP.
Lease time (min)	Tu wpisuje się czas dzierżawy w minutach. Jako wartość standardowa wpisane jest 120 minut.
Static Hosts	Tu wyświetlane są statyczne przyporządkowania adresów MAC do adresów IP. Jeśli przyporządkowanie nie zostało zdefiniowane, wyświetlana jest informacja „No static hosts configured“.
Add Static Host	Następnie można dodać statyczne adresy MAC lub nazwy hosta i adresy IP.
MAC Address or Hostname	Tu wpisuje się nowe przyporządkowanie statyczne, np. „01:02:03:04:05:06=192.168.1.20“ lub „hostname=192.168.1.20“. Można wpisać 15 przyporządkowań lub nazw hosta.
addIp Address	Tu wpisuje się adresy IP, Można wpisać 15 adresów IP.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiany zostają zrealizowane natychmiast.

Aby przejąć nowy przyporządkowanie, należy kliknąć przycisk **[Add]**. Zmiana zostaje zrealizowana natychmiast.

Aby usunąć istniejące przyporządkowanie, należy kliknąć przycisk **[Delete]**. Zmiana zostaje zrealizowana natychmiast.

15.1.1.2.20 Strona „Configuration of DNS Server“

Na stronie „Configuration of DNS Server“ znajdują się ustawienia dla usługi DNS.

Grupa „DNS Server“

Tabela 74: Strona WBM „Configuration of DNS Server“ – grupa „DNS Server“

Parametr	Znaczenie	
Service active	Tu włączą się i wyłącza usługę serwera DNS.	
Mode	Tu wybiera się typ pracy serwera DNS.	
	Proxy	Zapytania buforowane są w celu optymalizacji przepustowości komunikacji.
	Relay	Wszystkie zapytania są przesyłane bezpośrednio dalej.
Static Hosts	Tu wyświetlane są statyczne przyporządkowania nazw do adresów IP. Jeśli przyporządkowanie nie zostało zdefiniowane, wyświetlana jest informacja „No static hosts configured“.	
Add Static Host	Następnie można dodać statyczne adresy IP i nazwy hosta.	
IP Address	Tu wpisuje się nowe stałe przyporządkowanie, np. „192.168.1.20:hostname“. Można wpisać 10 przyporządkowań.	
Nazwa hosta	Tu wpisuje się nazwę hosta.	

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiany zostają zrealizowane natychmiast.

Aby przejąć nowy przyporządkowanie, należy kliknąć przycisk **[Add]**. Zmiana zostaje zrealizowana natychmiast.

Aby usunąć istniejące przyporządkowanie, należy kliknąć przycisk **[Delete]**. Zmiana zostaje zrealizowana natychmiast.

15.1.1.2.21 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 75: Strona WBM „Overview“ – grupa „Connection <n>“

Parametr	Znaczenie
Is Active	Tu wyświetlany jest status komunikacji z chmurą.
Data from PLC Runtime	Tu wyświetlana jest informacja, ile kolekcji danych (Data-Collections) ze strony aplikacji IEC zostało zarejestrowanych do transmisji do chmury.
Cloud Connection	Tu wyświetlany jest status połączenia z chmurą.
Heartbeat	Tu wyświetlany jest aktualnie skonfigurowany interwał heartbeat mierzony w sekundach.
Telemetry data transmission	Tu wyświetlana jest informacja, czy transmisja danych jest aktywna, czy nieaktywna.
Cache fill level (QoS 1 and 2)	Tu wyświetlany jest stan zapełnienia pamięci dla wiadomości wychodzących, wyrażony w procentach.

Grupa „Diagnosis“

Grupa ta widoczna jest tylko wtedy, gdy dostępne są informacje diagnostyczne.

Tu wyświetlane są ostrzeżenia i błędy oraz informacje (o ile są dostępne) dotyczące możliwego usunięcia błędu.

15.1.1.2.22 Strona „Configuration of Connection <n>“

Na stronie „Configuration of Connection <n>“ znajdują się ustawienia i informacje dotyczące dostępu do chmury.

Dla każdego dostępu do chmury wyświetlana jest osobna strona.

Grupa „Configuration“

Wyświetlone parametry są zależne od ustawionej platformy chmury i ewentualnie od innych ustawień w tej grupie.
Zależności przedstawione są w osobnych tabelach.

Tabela 76: Strona WBM „Configuration of Connection <n>“ – grupa „Configuration“

Parametr	Znaczenie
Enabled	Tu aktywuje się i dezaktywuje funkcję Cloud Connectivity.
Cloud platform	Tu wybiera się platformę chmury.
Nazwa hosta	Tu wpisuje się nazwę hosta lub adres IP dla wybranej platformy chmury.
ID Scope	Tu wpisuje się punkt końcowy dla usługi Azure Device Provisioning Service (DPS).
Registration ID	Tu wpisuje się ID rejestru dla usługi Azure Device Provisioning Service (DPS).
Port number	Tu wpisuje się port, do którego ma być utworzone połączenie. Typowe wartości to 8883 dla połączeń szyfrowanych i 1883 dla połączeń nieszyfrowanych.
Device ID	Tu wpisuje się Device ID dla wybranej platformy chmury.
Client ID	Tu wpisuje się Client ID dla wybranej platformy chmury.
Authentication	Tu wybiera się metodę uwierzytelnienia. Możliwe ustawienia to „Shared Key Acces“ lub „X.509 Certificate“.
Activation Key	Tu wpisuje się kod aktywacji dla wybranej platformy chmury.
Clean Session	Tu deklaruje się, czy Clean Session ma być aktywna przy połączeniu z usługą chmury. Jeśli Clean Session jest aktywna, informacje i wiadomości dotyczące tego połączenia z usługą chmury nie są zapisywane.
TLS	Tu można zdecydować, czy dla połączenia z platformą chmury ma być zastosowane kodowanie TLS. Amazon Web Services (AWS) stosuje zawsze TLS.

Tabela 76: Strona WBM „Configuration of Connection <n>“ – grupa „Configuration“

Parametr	Znaczenie
CA file	Tu podaje się ścieżkę do pliku zakodowanego w formacie PEM, który zawiera stosowny i wiarygodny certyfikat CA potwierdzający tworzenie zakodowanych połączeń. Standardowo jest nim zainstalowany już w sterowniku certyfikat CA /etc/ssl/certs/ca-certificates.crt.
User	Tu wpisuje się nazwę użytkownika dla uwierzytelnienia usługi chmury.
Password	Tu wpisuje się hasło dla uwierzytelnienia usługi chmury.
Certification file	Tu wpisuje się ścieżkę do pliku zakodowanego w formacie PEM, wykorzystywanego do uwierzytelnienia usługi chmury.
Key file	Tu wpisuje się ścieżkę do pliku zakodowanego w formacie PEM, który zawiera prywatny kod do uwierzytelnienia usługi chmury.
Use websockets	Tu można zdecydować, czy połączenie z platformą chmury ma być nawiązane poprzez protokół Websocket przez port 443. Gdy pole wyboru nie jest zaznaczone, połączenie z platformą chmury zostaje nawiązane poprzez protokół MQTT przez port 8883.
Proxy Type	Tu wybiera się, jaki typ serwera proxy ma być wykorzystany.
HTTP Proxy Host	Tu wpisuje się nazwę hosta lub adres IP serwera proxy.
HTTP Proxy Port	Tu wpisuje się numer portu serwera proxy.
HTTP Proxy User	Tu wpisuje się nazwę użytkownika proxy.
HTTP Proxy Password	Tu wpisuje się hasło użytkownika proxy.
Use compression	Tu można zdecydować, czy dane mają być skompresowane za pomocą programu GZIP.
Data Protocol	Tu wybiera się protokół danych.
Cache mode	Tu definiuje się, w której pamięci ma być założona pamięć podręczna (cache) dla telegramów danych. To pole wyboru jest aktywne tylko wtedy, gdy wetknięta jest prawidłowo sformatowana karta SD. (Więcej informacji znaleźć można w instrukcji A500920.)
Last Will	Tu definiuje się, czy wiadomość Last Will ma być aktywowana/dezaktywowana.
(Last Will) Topic	Tu wpisuje się temat dla wysyłanej wiadomości Last Will.
(Last Will) Message	Tu wpisuje się treść, która ma być wysłana jako wiadomość Last Will.

Tabela 76: Strona WBM „Configuration of Connection <n>“ – grupa „Configuration“

Parametr	Znaczenie
(Last Will) QoS	Tu podaje się „Quality of Service“ (QoS) wiadomości Last Will.
(Last Will) Retain	Tu definiuje się, czy ostatnia wysłana z danym tematem wiadomość Last Wil ma być potraktowana przez brokera jako wiadomość zapisana (Retained Message).
Device info	Tu definiuje się, czy generowana jest wiadomość Device Info, informująca usługę chmury o podstawowej konfiguracji sterownika. (Więcej informacji znaleźć można w instrukcji A500920.)
Device status	Tu definiuje się, czy ma być generowana wiadomość Device State, informująca usługę chmury o zmianach przełącznika trybu pracy i wskaźników LED. (Więcej informacji znaleźć można w instrukcji A500920.)
Standard commands	Tu definiuje się, czy mają być wspierane zintegrowane standardowe komendy. (Listę standardowych komend można znaleźć w instrukcji A500920.) Jeśli pole wyboru nie jest zaznaczone, wspierane są tylko komendy zdefiniowane w programie IEC.
Application property template	Tu można utworzyć własność dla poszczególnych wiadomości MQTT do chmury Azure. Ten parametr jest opcjonalny, tzn. gdy pole pozostawione jest puste, ta własność nie jest wysyłana. Przy tworzeniu tej własności są do dyspozycji następujące komponenty: • <m>: Message type • <p>: Protocol version • <d>: DeviceI ID Przykłady: • MyKey=HelloWorld_<m> • TestKey=<m>/<p>/<d> • DeviceId=<d>

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**.

Zmiany zostaną zrealizowane dopiero po następnym restarcie sterownika. W tym celu należy skorzystać z funkcji Reboot WBM. Nie należy wyłączać sterownika zbyt wcześnie!

Poniższe tabele przedstawiają zależności między polami wyboru i edycji a poszczególnymi platformami chmury oraz możliwe ustawienia.

Tabela 77: Zależności między polami wyboru i edycji a poszczególnymi platformami chmury

Pole wyboru lub edycji	Platforma chmury						
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
Enabled	X	X	X	X	X	X	X
Cloud platform	X	X	X	X	X	X	X
Hostname	X	X	X	X	X	X	
Port number			X	X	(X)	X	
Device ID	X	X					
Client ID			X	X	X	X	
Authentication		X					X
Activation Key	X	X2					X2
Clean Session			X	(X)	(X)	X	
TLS			X	X	(X)	X	
CA file		X	X	X	X	X	X
User			X	X			
Password			X	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)	X
Use compression	X	X1	X1				X1
Cache mode	X	X	X	X	X	X	X
Last Will			X	X	X	X	
Last Will Topic			X3	X3	X3	X3	
Last Will Message			X3	X3	X3	X3	
Last Will QoS			X3	X3	X3	X3	
Last Will Retain			X3	X3	(X3)	X3	
Device info		X1	X1	X1	X1		X1
Device status		X1	X1	X1	X1		X1
Standard commands		X1	X1		X1		X1
Application property template		X1					X1

Tabela 77: Zależności między polami wyboru i edycji a poszczególnymi platformami chmury

Pole wyboru lub edycji	Platforma chmury						
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)

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 78: Możliwość wyboru protokołu danych dla poszczególnych platform chmury

Protokół danych	Platforma chmury						
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
WAGO Protocol		X	X	X	X		X
WAGO Protocol 1.5		X	X	X	X		X
Native MQTT			X	X	X	(X)	
Sparkplug payload B		X	X		X		

X: Możliwość wyboru
(X): Stała konfiguracja

Tabela 79: 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 80: Możliwość wyboru trybu pamięci podręcznej dla poszczególnych platform chmury

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 81: 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

15.1.1.2.23 Strona „Configuration of General SNMP Parameters“

Na stronie „Configuration of General SNMP Parameters“ znajdują się ogólne ustawienia dla SNMP.

Grupa „General SNMP Configuration“

Tabela 82: Strona WBM „Configuration of General SNMP Parameter“ – grupa „General SNMP Configuration“

Parametr	Znaczenie
Service active	Tu można aktywować/dezaktywować serwis SNMP.
Name of Device	Tu wpisuje się nazwę urządzenia (sysName).
Description	Tu wpisuje się opis urządzenia (sysDescription).
Physical Location	Tu wpisuje się lokalizację urządzenia (sysLocation).
Contact	Tu wpisuje się adres kontaktowy e-mail (sysContact).
ObjectID	Tu wpisuje się Object-ID.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**.

15.1.1.2.24 Strona „Configuration of SNMP v1/v2c Parameters“

Na stronie „Configuration of SNMP v1/v2c Parameters“ znajdują się ustawienia dla SNMP v1/v2c.

Grupa „Communities“

Tabela 83: Strona WBM „Configuration of SNMP v1/v2c Parameters“ – grupa „Communities“

Parametr	Znaczenie
Community <n>	Dla każdej skonfigurowanej Community wyświetlany jest osobny obszar. Jeśli nie skonfigurowano Community, wyświetlana jest informacja „(no Communities configured)“.
Name	Wyświetla nazwę Community do konfiguracji managera SNMP. Przez nazwę Community można tworzyć powiązania między managerami i agentami SNMP, którzy określani są jako Community i sterują identyfikacją oraz dostępem między urządzeniami SNMP.
Access	Tu wyświetlane są prawa dostępu dla Community. Możliwe wartości to: „ReadOnly“ lub „ReadWrite“.
Add new Community	W tym obszarze możesz dodać nową Community.
Name	Tu wpisuje się nazwę Community dla nowej konfiguracji managera SNMP. (s.o.). Nazwa Community może liczyć maksymalnie 32 znaki i nie może zawierać spacji. Aby móc zastosować protokół SNMP, musi być podana aktualna nazwa Community. Standardem jest „public“.
Access	Tu wybiera się prawa dostępu dla nowej Community. Możliwe wartości to: „ReadOnly“ lub „ReadWrite“.

Aby usunąć istniejącą Community, należy kliknąć odpowiedni przycisk **[Delete]**.

Aby dodać nową Community, należy kliknąć przycisk **[Add]**.

Grupa „Trap Receivers“

Tabela 84: Strona WBM „Configuration of SNMP v1/v2c Parameters“ – grupa „Trap Receivers“

Parametr	Znaczenie
Trap Receiver <n>	Dla każdego skonfigurowanego odbiorcy komunikatów trap wyświetlany jest osobny obszar. Jeśli odbiorca komunikatów trap nie został skonfigurowany, wyświetlana jest informacja „(no Trap Receivers configured)“.
Host	Tu wyświetlana jest nazwa hosta lub adres IP odbiorcy komunikatów trap (Managementstation).
Community Name	Tu wyświetlana jest nazwa Community do konfiguracji odbiorcy komunikatów trap. Nazwa Community może być weryfikowana przez odbiorcę komunikatów trap.
Version	Tu wyświetlana jest wersja SNMP, przez którą powinny być wysyłane komunikaty trap.
Add new Trap Receiver	W tym obszarze można dodać nowego odbiorcę komunikatów trap.
Host	Tu wpisuje się nazwę hosta lub adres IP nowego odbiorcy komunikatów trap (Managementstation).
Community Name	Tu wpisuje się nazwę Community do nowej konfiguracji odbiorcy komunikatów trap (s.o.). Nazwa Community może liczyć maksymalnie 32 znaki i nie może zawierać spacji.
Version	Tu wybiera się wersję SNMP, przez którą powinny być wysyłane komunikaty trap. Możliwe wartości: „v1“ lub „v2c“.

Aby usunąć istniejącego odbiorcę komunikatów trap, należy kliknąć odpowiedni przycisk **[Delete]**.

Aby dodać nowego odbiorcę komunikatów trap, należy kliknąć przycisk [**Add**].

15.1.1.2.25 Strona „Configuration of SNMP v3 Parameters“

Na stronie „Configuration of SNMP v3 Parameters“ znajdują się ustawienia dla SNMP v3.

Grupa „Users“

Tabela 85: Strona WBM „Configuration of SNMP v3 Parameters“ – grupa „User“

Parametr	Znaczenie
User <n>	Dla każdego skonfigurowanego użytkownika v3 wyświetlany jest osobny obszar. Jeśli użytkownik v3 nie został skonfigurowany, wyświetlana jest informacja „(no Users configured)“.
Security Authentication Name	Tu wyświetlana jest nazwa użytkownika.
Authentication Type	Tu wyświetlany jest typ uwierzytelnienia dla pakietów SNMP v3. Możliwe wartości to: - Brak uwierzytelnienia („None“) - Message Digest 5 („MD5“) - Secure Hash Algorithm („SHA“, „SHA224”, „SHA256”, „SHA384”, „SHA512”)
Authentication Key	Tu wyświetlany jest klucz dla uwierzytelniania.
Privacy	Tu wyświetlany jest algorytm kodowania dla wiadomości SNMP. Możliwe wartości to: - Brak kodowania („None“) - Data Encryption Standard („DES“) - Advanced Encryption Standard („AES“, „AES128”, „AES192”, „AES192C”, „AES256”, „AES256C”)
Privacy Key	Tu wyświetlany jest klucz do kodowania wiadomości SNMP. Jeśli brak jakiegokolwiek wyświetlenia, automatycznie zastosowany zostaje „Authentication Key“.
Access	Tu wyświetlane są prawa dostępu dla użytkownika. Możliwe wartości to: „ReadOnly“ lub „ReadWrite“.
Add new v3 User	W tym obszarze można wpisać nowego użytkownika v3. Można wpisać 10 użytkowników.
Security Authentication Name	Tu wpisuje się nazwę użytkownika. Musi ona być unikatowa; już istniejąca nazwa użytkownika nie zostanie zaakceptowana. Nazwa może zawierać min. 8 i maks. 32 znaków, w tym małe litery (a … z), duże litery (A … Z), cyfry (0 … 9), znaki specjalne !()*~'.-_, ale nie może zawierać spacji.

Tabela 85: Strona WBM „Configuration of SNMP v3 Parameters“ – grupa „User“

Parametr	Znaczenie
Authentication Type	Tu wpisuje się typ uwierzytelnienia dla pakietów SNMP v3. Możliwe wartości to: - Brak uwierzytelnienia („None“) - Message Digest 5 („MD5“) - Secure Hash Algorithm („SHA“, „SHA224”, „SHA256”, „SHA384”, „SHA512”)
Authentication Key	Tu należy podać klucz dla uwierzytelnienia. Klucz może zawierać min. 8 i maks. 32 znaków, w tym małe litery (a … z), duże litery (A … Z), cyfry (0 … 9), znaki specjalne !()*~'.-_, ale nie może zawierać spacji.
Privacy	Tu wpisuje się algorytm kodowania dla wiadomości SNMP. Możliwe wartości to: - Brak kodowania („None“) - Data Encryption Standard („DES“) - Advanced Encryption Standard („AES“, „AES128”, „AES192”, „AES192C”, „AES256”, „AES256C”)
Privacy Key	Tu wpisuje się klucz do kodowania wiadomości SNMP. Jeśli nic nie zostanie wpisane, automatycznie zastosowany zostaje „Authentication Key“. Klucz może zawierać min. 8 i maks. 32 znaków, w tym małe litery (a … z), duże litery (A … Z), cyfry (0 … 9), znaki specjalne !()*~'.-_, ale nie może zawierać spacji.
Access	Tu wybiera się prawa dostępu dla nowego użytkownika. Możliwe wartości to: „ReadOnly“ lub „ReadWrite“.

Aby usunąć użytkownika, należy kliknąć odpowiedni przycisk **[Delete]**.

Aby dodać nowego użytkownika, należy kliknąć przycisk **[Add]**.

Grupa „Trap Receivers“

Tabela 86: Strona WBM „Configuration of SNMP v3 Parameters“ – grupa „Trap Receivers“

Parametr	Znaczenie
Trap Receiver <n>	Dla każdego skonfigurowanego odbiorcy komunikatów trap v3 wyświetlany jest osobny obszar. Jeśli odbiorca komunikatów trap v3 nie został skonfigurowany, wyświetlana jest informacja „(no Trap Receivers configured)“.
Security Authentication Name	Tu wyświetlana jest nazwa użytkownika.
Authentication Type	Tu wyświetlany jest typ uwierzytelnienia dla pakietów SNMP v3. Możliwe wartości to: - Brak uwierzytelnienia („None“) - Message Digest 5 („MD5“) - Secure Hash Algorithm („SHA“, „SHA224”, „SHA256”, „SHA384”, „SHA512”)
Authentication Key	Tu wyświetlany jest klucz dla uwierzytelniania.
Privacy	Tu wyświetlany jest algorytm kodowania dla wiadomości SNMP. Możliwe wartości to: - Brak kodowania („None“) - Data Encryption Standard („DES“) - Advanced Encryption Standard („AES“, „AES128”, „AES192”, „AES192C”, „AES256”, „AES256C”)
Privacy Key	Tu wyświetlany jest klucz do kodowania wiadomości SNMP. Jeśli brak jakiegokolwiek wyświetlenia, automatycznie zastosowany zostaje „Authentication Key“.
Host	Tu wyświetlana jest nazwa hosta lub adres IP odbiorcy komunikatów trap dla v3.
Add new Trap Receiver	W tym obszarze można wpisać nowego odbiorcę komunikatów trap v3. Można utworzyć maksymalnie 10 odbiorców komunikatów trap.
Security Authentication Name	Tu wpisuje się nazwę użytkownika. Musi ona być unikatowa; już istniejąca nazwa użytkownika nie zostanie zaakceptowana. Nazwa może zawierać min. 8 i maks. 32 znaków, w tym małe litery (a … z), duże litery (A … Z), cyfry (0 … 9), znaki specjalne !()*~'.-_, ale nie może zawierać spacji.
Authentication Type	Tu wpisuje się typ uwierzytelnienia dla pakietów SNMP v3. Możliwe wartości to: - Brak uwierzytelnienia („None“) - Message Digest 5 („MD5“) - Secure Hash Algorithm („SHA“, „SHA224”, „SHA256”, „SHA384”, „SHA512”)

Tabela 86: Strona WBM „Configuration of SNMP v3 Parameters“ – grupa „Trap Receivers“

Parametr	Znaczenie
Authentication Key	Tu należy podać klucz dla uwierzytelnienia. Klucz może zawierać min. 8 i maks. 32 znaków, w tym małe litery (a … z), duże litery (A … Z), cyfry (0 … 9), znaki specjalne !()*~'.-_, ale nie może zawierać spacji.
Privacy	Tu wpisuje się algorytm kodowania dla wiadomości SNMP. Możliwe wartości to: - Brak kodowania („None“) - Data Encryption Standard („DES“) - Advanced Encryption Standard („AES“, „AES128”, „AES192”, „AES192C”, „AES256”, „AES256C”)
Privacy Key	Tu wpisuje się klucz do kodowania wiadomości SNMP. Jeśli nic nie zostanie wpisane, automatycznie zastosowany zostaje „Authentication Key“. Klucz może zawierać min. 8 i maks. 32 znaków, w tym małe litery (a … z), duże litery (A … Z), cyfry (0 … 9), znaki specjalne !()*~'.-_, ale nie może zawierać spacji.
Host	Tu wpisuje się nazwę hosta lub adres IP odbiorcy komunikatów trap dla v3.

Aby usunąć użytkownika, należy kliknąć odpowiedni przycisk **[Delete]**.

Aby dodać nowego użytkownika, należy kliknąć przycisk **[Add]**.

15.1.1.2.26 Strona „Favorites“

Na stronie „Favorites“ można ustawić stronę startową produktu. Poza tym strona ta udostępnia listę sterowników.

Na stronę startową można wybrać z listy konkretny sterownik, który będzie wyświetlany przy uruchomieniu produktu.

Gdy jako stronę startową wybrana jest strona WWW lub sterownik, strona WWW lub sterownik wyświetlany jest jako strona startowa niezależnie od tego, czy projekt bootowalny istnieje, czy nie.

Jeśli WBM lub „Browser Favorites“ zostały zaznaczone jako strona startowa i istnieje projekt bootowalny, jako strona startowa wyświetlana jest Target-Wizualizacja.

Jeśli WBM lub „Browser Favorites“ zostały zaznaczone jako strona startowa i nie ma projektu bootowalnego, jako strona startowa wyświetlany jest WBM lub „Browser Favorites“.

Wskazówka

Przy istniejącej Target-Wizualizacji nie ma możliwości ustawienia strony startowej!
Jeśli w produkcie zaprojektowana i uruchomiona jest Target-Wizualizacja, wybór strony startowej jest nieskuteczny, ponieważ Target-Wizualizacja została uruchomiona bezpośrednio.

Grupa „WBM“

Tu można aktywować/dezaktywować WBM jako stronę startową, pokazującą się przy uruchomieniu produktu.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**.

Grupa „Browser Favorites“

Tu można aktywować/dezaktywować listę „Browser Favorites“ jako stronę startową, pokazującą się przy uruchomieniu produktu.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**.

Grupy „Favorite n“

Każda grupa opisuje połączenie z określonym sterownikiem. Jeśli nazwa sterownika zostanie zmieniona, staje się od razu nową nazwą grupy.

Tu można aktywować/dezaktywować WBM jako stronę startową, pokazującą się przy uruchomieniu produktu.

Tu aktywuje się/dezaktywuje przeglądarkę MicroBrowser dla danego sterownika.

Tabela 87: Strona WBM „Favorites” – grupy „Favorite n“

Parametr	Znaczenie
Startpage	Tu można aktywować/dezaktywować tę stronę jako stronę startową, pokazującą się przy uruchomieniu produktu.
Name	Tu należy podać dowolną nazwę sterownika.
URL	Tu należy podać URL, pod którym dostępna jest wizualizacja internetowa sterownika.
Virtual Keyboard	Tu można zdefiniować, czy przy wyświetleniu URL tego sterownika ma być użyta wirtualna klawiatura panela. Ma to sens, gdy ma być wyświetlona np. WebVisu, która wymaga własnej wirtualnej klawiatury.
WebVisu	Tu można zdefiniować, czy podany URL dotyczy WebVisu czy nie.
MicroBrowser	Tu można aktywować/dezaktywować MicroBrowser dla sterownika.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Aby zresetować wszystkie pola edycji, należy kliknąć przycisk **[Clear]**. Reset należy potwierdzić przyciskiem **[Submit]**.

Aktywacja/dezaktywacja MicroBrowser zostanie zrealizowana dopiero po następnym restarcie produktu. W tym celu należy skorzystać z funkcji Reboot WBM. Nie należy wyłączać produktu zbyt wcześnie!

Wskazówka

Aplikacja CODESYS V3 zapobiega wizualizacji internetowej przez przeglądarkę MicroBrowser!
W celu aktywacji MicroBrowser do produktu nie może być wgrywana aplikacja CODESYS V3.

W przypadku zakłóceń lub przerwania połączenia przeglądarki ze sterownikiem, w przeglądarce MicroBrowser wyświetlany jest pomarańczowy prostokąt ze znakiem wykrzyknika.

Jeśli przy uruchomieniu produktu urządzenie partnerskie (PLC) nie jest jeszcze dostępne, wyświetlany jest ekran startowy.

Dla przeglądarki MicroBrowser obowiązują standardowe dane logowania:

Tabela 88: MicroBrowser – dane logowania

Użytkownik	Standardowe hasło
admin	wago

15.1.1.2.27 Strona „Autostart“

Na tej stronie można ustawić opcje automatycznego startu dla runtime'u.

Grupa „Autostart“

Tu ustawia się licznik, który przy uruchamianiu jest wyświetlany przed wyświetleniem strony startowej. W trakcie zdefiniowanego okresu istnieje możliwość wyłączenia automatycznej zmiany na stronę startową i bezpośredniego przejścia do WBM. Delay „0“ wyświetla bezpośrednio stronę startową.

15.1.1.2.28 Strona „Monitoring“

Na stronie „Monitoring“ znajdują się ustawienia do monitorowania produktu.

Grupa „Monitoring“

Tabela 89: Strona WBM „Monitoring” – grupa „Monitoring“

Parametr	Znaczenie
Reconnect	Tu można zdefiniować, czy po przerwaniu połączenia z produktem ma być podjęta automatycznie próba ponownego nawiązania połączenia.
Interval (s)	Tu podaje się interwał tych prób.

15.1.1.2.29 Strona „Browser Security“

Na stronie „Browser Security“ ustawia się poziom bezpieczeństwa przeglądarki.

Grupa „Browser Security“

Tu wybiera się żądany poziom bezpieczeństwa (Low lub High).

Tabela 90: Strona WBM „Browser Security” – grupa „Browser Security“

Parametr	Znaczenie
Browser Security	• Low: w tym poziomie bezpieczeństwa dozwolone są połączenia HTTPS z: •• certyfikatami, które nie są jeszcze ważne, •• certyfikatami, które są już nieważne, •• certyfikatami samodzielnie podpisanymi oraz •• certyfikatami z niezgodnymi nazwami hosta. • High: w tym poziomie bezpieczeństwa wymienione wyżej i dozwolone w „Low“ połączenia są odrzucane.

15.1.1.2.30 Strona „Docker Settings“

Na stronie „Docker Settings“ znajdują się ustawienia dla usługi „Docker®“.

Grupa „Docker Status“

Tabela 91: Strona WBM „Docker Settings“ – grupa „Docker Status“

Parametr	Znaczenie	
Current State	Tu wyświetlany jest aktualny status usługi „Docker®“.	
	stopped	Usługa „Docker®“ nie jest aktywna.
	running	Usługa „Docker®“ jest aktywna.
Service Enabled	To pole wyboru należy zaznaczyć, gdy ma być aktywowana usługa „Docker®“.	

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiany zostają zrealizowane natychmiast.

15.1.1.2.31 Strona „Fonts“

Na tej stronie można pobierać lub usuwać czcionki z komputera.

Należy kliknąć pole „Choose file…“. Następnie można wybrać żądany plik True Type Font (*.ttf).

Kliknięcie przycisku **[Upload]** powoduje pobranie czcionkę. Na liście powyżej pola „Choose file…“ pojawia się pobrana czcionki. Czcionka jest dostępna dopiero po następnym restarcie.

Aby usunąć czcionkę, należy kliknąć przycisk **[Delete]**.

15.1.1.2.32 Strona „Display Orientation“

Na stronie „Display Orientation“ można zdefiniować pozycję wyświetlacza.

Grupa „Display Orientation“

Tu definiuje się, czy obraz ma być wyświetlany w pionie czy w poziomie.
Dostępne opcje: landscape, portrait, landscape rotated i portrait rotated.

15.1.1.2.33 Strona „Screensaver“

Na stronie „Screensaver“ można ustawić wygaszacz ekranu (screensaver).

Grupa „Screensaver Settings“

Tu można zdecydować, czy ma być zastosowany wygaszacz ekranu.

Tabela 92: Strona WBM „Screensaver ” – grupa „Screensaver Settings“

Parametr	Znaczenie
Enabled	Tu można aktywować lub dezaktywować wygaszacz ekranu.
Setting	Tu definiuje się, czy obraz, godzina, tekst i „Backlight” mają być wyświetlane, czy też ma być zastosowana funkcja „Screen care“ (pielęgnacja ekranu). • Image: wygaszacz ekranu ustawiony jest na wyświetlanie logo WAGO i aktywowany jest po upływie czasu zdefiniowanego w punkcie „Duration“. • Text: należy podać tekst, który będzie wyświetlany jako wygaszacz ekranu po upływie czasu zdefiniowanego w punkcie „Duration“. • Time: jako wygaszacz ekranu ustawiona zostaje aktualna godzina. • Backlight: jasność zmniejsza się do jasności wygaszonego ekranu i wyświetlane jest logo WAGO. • Screen care: w celu pielęgnacji ekranu następuje inwersja wszystkich pikseli na kilka milisekund (niewidoczna). • Off: wygaszacz ekranu nie ma być wyświetlany.
Text	Tu należy podać dowolny tekst, który ma pojawiać się na wygaszaczu ekranu. (możliwość edycji przy opcji „Text“.)
Duration (s)	Gdy wyświetlacz jest nieużywany, po upływie ustawionego tu czasu aktywowany jest wygaszacz ekranu.

Grupa „Screen Care“

Tu definiuje się, przez jaki czas wyświetlacz ma być nieaktywny podczas czyszczenia.

Tabela 93: Strona WBM „Screensaver ” – grupa „Screen Care“

Parametr	Znaczenie
Enabled	Tu można aktywować/dezaktywować pielęgnację ekranu.
Time (hh:mm:ss)	Tu definiuje się godzinę, w której ma być przeprowadzona pielęgnacja ekranu. (możliwość edycji przy opcji „Screen care“.)

15.1.1.2.34 Strona „WBM User Configuration“

Na stronie „WBM User Configuration“ można znaleźć ustawienia dla User-Aministration.

Grupa „Change Password“

Wskazówka

Zmienić hasła
Ustawione fabrycznie hasła inicjalne podane są w niniejszej instrukcji obsługi i dlatego nie stanowią wystarczającego zabezpieczenia! Należy zmienić te hasła stosownie do potrzeb!

Tabela 94: Strona „WBM User Configuration” – grupa „Change Password“

Parametr	Znaczenie
Old Password	Tu należy podać stosowane aktualnie hasło.
New Password	Tu wpisuje się nowe hasło. W haśle dopuszczalne są następujące znaki ASCII: a … z, A … Z, 0 … 9, i znaki specjalne: !"#$%&'()*+,./:;<=>?@[]^_`{}|~-.
Confirm Password	Tu wpisuje się jeszcze raz nowe hasło w celu sprawdzenia.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

Wskazówka

W hasłach WBM używać dopuszczalnych znaków!
Jeśli poza WBM (np. przez klawiaturę USB) tworzone są hasła zawierające znaki niedopuszczalne w WBM, dostęp do stron WBM bezpośrednio na wyświetlaczu nie będzie możliwy, ponieważ dopuszczalne znaki dostępne są tylko przy użyciu wirtualnej klawiatury!

Wskazówka

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

Zarządzanie użytkownikami dla aplikacji sterowania ustalane i realizowane jest osobno.

15.1.1.3 Zakładka „Fieldbus“

15.1.1.3.1 Strona „OPC UA Configuration“

Na stronie „OPC UA Configuration“ znajdują się ustawienia dla usługi OPA UA.

Grupa „OPC UA Server Configuration“

Tabela 95: Strona WBM „OPC UA Configuration“ – grupa „OPC UA Server Configuration“

Parametr	Znaczenie
Enabled	Tu aktywuje się i dezaktywuje serwer OPC UA.
Log Level	Tu wybiera się poziom rejestrowania. Można ustawić następujące wartości: Error / Warning / Info / Debug. Poziom rejestrowania „Error“ wysyła komunikaty o błędzie, a poziom rejestrowania „Info“ także komunikaty o statusie. Wybór poziomu rejestrowania ma wpływ na czas reakcji serwera. Dlatego należy wybrać najniższy niezbędny poziom, np. „Debug“ dla dogłębnych analiz.
Ctrl Configuration name	Tu podaje się nazwę konfiguracji, którą otrzymuje sterownik wewnątrz PLC Open Device Set.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**.

Grupa „OPC UA Server Security Settings“

Tabela 96: Strona WBM „OPC UA Configuration“ – grupa „OPC UA Server Security Settings“

Parametr	Znaczenie
Anonymous Access	Zezwolenie na anonimowy dostęp serwera Zakłada się, że nie jest/będzie zaznaczone uwierzytelnianie portu runtime.
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: Dostępne są punkty końcowe **None**, **Sign** i **SignAndEncrypt**. **Sign** udostępnia punkt końcowy, który jest chroniony hasłem. **SignAndEncrypt** udostępnia punkt końcowy, który oprócz hasła udostępnia również szyfrowanie. Sign + SignAndEncrypt: Dostępne są punkty końcowe **Sign** oraz **SignAndEncrypt**. SignAndEncrypt: Dostępny jest tylko punkt końcowy **SignAndEncrypt**.
Security Policies	Wybór polityki bezpieczeństwa Tu ustawia się moc szyfrowania serwera OPC UA. Do wyboru są: Aes128Sha256RsaOaep and better, Basic256Sha256 and better, Aes256Sha256RsaPss.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**.

15.1.1.3.2 Strona „BACnet Status“

Na stronie „BACnet Status” wyświetlane są informacje o sterowniku specyficzne dla sieci obiektowej BACnet i licencji BACnet.

Grupa „BACnet Information“

Tabela 97: Strona WBM „BACnet Status” – grupa „BACnet Information“

Parametr	Znaczenie
State	Tu wyświetlana jest informacja, czy sieć obiektowa BACnet jest aktywna (enabled), czy nieaktywna (disabled).
Status Info	Tu wyświetlany jest status sieci obiektowej BACnet.
Device-ID	Tu wyświetlany jest aktualny Device-ID sterownika.

Grupa „BACnet License“

Tabela 98: Strona WBM „BACnet Status” – grupa „BACnet License“

Parametr	Znaczenie
Type	Tu wyświetlany jest typ licencji.
User Objects	Tu wyświetlana jest liczba obiektów BACnet możliwych do uzyskania w ramach licencji.

15.1.1.3.3 Strona „BACnet Configuration“

Na tej stronie można wprowadzić ustawienia specyficzne dla sieci obiektowej BACnet.

Aby przejąć ustawienia, należy kliknąć przycisk **[Submit]**.
Zmiany w konfiguracji BACnet zostaną zastosowane dopiero po restarcie. W celu restartu stosu/sterownika należy skorzystać z funkcji Reboot WBM. Aby ponownie uruchomić runtime, należy użyć przycisku **[Restart]**. Nie należy wyłączać sterownika zbyt wcześnie!

Grupa „BACnet Service“

Grupa ta zawiera aktywację i dezaktywację dla sieci obiektowej.

Aby można było korzystać z protokołu BACnet, musi być zaznaczony parametr „Service active“ (ustawienie standardowe).

Przy restarcie runtime ze względów bezpieczeństwa pojawi się okno z pytaniem, czy restart jest pożądany.

Tabela 99: Strona WBM „BACnet Configuration” – grupa „BACnet Service“

Parametr	Znaczenie
Service active	Tu można aktywować/dezaktywować sieć obiektową BACnet.
Runtime restart **[Restart]**	Za pomocą tego przycisku można przeprowadzić restart runtime.

Grupa „BACnet Settings“

Grupa ta zawiera podstawowe ustawienia sieci obiektowej.

Tabela 100: Strona WBM „BACnet Configuration” – grupa „BACnet Settings“

Parametr	Znaczenie
Port number	Tu ustawia się port dla komunikacji w sieci obiektowej BACnet.
Who-Is online interval time (sec)	Tu ustawia się, w jakich interwałach czasowych sterownik wysyła zapytania do sieci obiektowej, które urządzenia są dostępne online (min. 60 s).

Grupa „BACnet Data Reset“

Grupa ta pozwala wybrać, które dane mają zostać usunięte lub zresetowane przy kolejnym restarcie.

Tabela 101: Strona WBM „BACnet Configuration” – grupa „BACnet Data Reset“

Parametr	Znaczenie
Delete Persistence Data	Przy kolejnym restarcie dane BACnet zostają trwale usunięte.
Reset all BACnet Data and Settings to Default	Przy kolejnym restarcie specyficzne ustawienia i dane BACnet zostają zresetowane do ustawień fabrycznych.

15.1.1.3.4 Strona „BACnet Storage Location“

Na tej stronie można wprowadzić ustawienia dla zapisu parametrów specyficznych dla BACnet.

Zmiany zostaną zastosowane bez restartu.

Grupa „BACnet Persistence“

Grupa ta umożliwia wybór miejsca zapisu danych trwałych (SD-Card/Internal-Flash).

Przy zmianie ustawień Persistent wyskakujące okno informuje, że może dojść do utraty danych, dopóki nie zostanie wykonane pełne następne zatrzymanie.

Tabela 102: Strona WBM „BACnet Storage Location” – grupa „BACnet Persistence“

Parametr	Znaczenie	
Storage location	Tu wybiera się miejsce zapisu danych trwałych. Wybór możliwy jest tylko wtedy, gdy istnieją oba nośniki pamięci.	
	Internal-Flash	Dane są zapisywane w wewnętrznej pamięci sterownika.
	SD-Card	Dane są zapisywane 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“.

Grupa „BACnet Trendlog”

Grupa ta umożliwia wybór miejsca zapisu danych trendu (SD-Card/Internal-Flash).

Tabela 103: Strona WBM „BACnet Storage Location” – grupa „BACnet Trendlog“

Parametr	Znaczenie	
Storage location	Tu wybiera się miejsce zapisu danych trendu. Wybór możliwy jest tylko wtedy, gdy istnieją oba nośniki pamięci.	
	Internal-Flash	Dane są zapisywane w wewnętrznej pamięci sterownika.
	SD-Card	Dane są zapisywane 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“.

Grupa „BACnet Eventlog”

Grupa ta umożliwia wybór miejsca zapisu danych Event Log (SD-Card/Internal-Flash).

Tabela 104: Strona WBM- „BACnet Storage Location” – grupa „BACnet Eventlog“

Parametr	Znaczenie	
Storage location	Tu wybiera się miejsce zapisu danych zdarzenia. Wybór możliwy jest tylko wtedy, gdy istnieją oba nośniki pamięci.	
	Internal-Flash	Dane są zapisywane w wewnętrznej pamięci sterownika.
	SD-Card	Dane są zapisywane 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“.

15.1.1.3.5 Strona „BACnet Files“

Na tej stronie można wymienić plik Override w sterowniku.

Zmiany zostaną zrealizowane dopiero po następnym restarcie sterownika. W tym celu należy skorzystać z funkcji Reboot WBM. Nie należy wyłączać sterownika zbyt wcześnie!

Grupa „BACnet override.xml“

Tabela 105: Strona WBM „BACnet Files” – grupa „BACnet override.xml“

Parametr	Znaczenie
Choose file...	Tu wybiera się żądany plik w sterowniku lub komputerze PC.
[Upload]	Za pomocą tego przycisku można przesłać wybrany plik z PC do sterownika.

15.1.1.4 Zakładka „Security“

15.1.1.4.1 Strona „OpenVPN / IPsec Configuration“

Na stronie „OpenVPN / IPsec Configuration“ znajdują się ustawienia OpenVPN i IPsec.

Grupa „OpenVPN“

Tabela 106: Strona WBM „OpenVPN / IPsec Configuration“ – grupa „OpenVPN“

Parametr	Znaczenie	
Current State	Tu wyświetlany jest aktualny status usługi OpenVPN.	
	stopped	Usługa nie jest aktywna.
	running	Usługa jest aktywna.
OpenVPN enabled	Tu można aktywować lub dezaktywować usługę OpenVPN.	
openvpn.config	Tu wybiera się plik konfiguracyjny OpenVPN, który należy przesłać z PC do produktu lub na odwrót.	

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**.

Aby wybrać plik na komputerze, należy kliknąć pole wyboru **Choose file …**.

Aby przesłać wybrany plik z PC do produktu, należy kliknąć przycisk **[Upload]**.

Aby przesłać plik z produktu do PC, należy kliknąć przycisk **[Download]**.

Zmiany zostaną zrealizowane dopiero po następnym restarcie produktu. W tym celu należy skorzystać z funkcji Reboot WBM. Nie należy wyłączać produktu zbyt wcześnie!

Grupa „IPsec“

Tabela 107: Strona WBM „OpenVPN / IPsec Configuration“ – grupa „IPsec“

Parametr	Znaczenie	
Current State	Tu wyświetlany jest aktualny status usługi IPsec.	
	stopped	Usługa nie jest aktywna.
	running	Usługa jest aktywna.
IPsec enabled	Tu można aktywować lub dezaktywować usługę IPsec.	
ipsec.conf	Tu wybiera się plik konfiguracyjny IPsec, który należy przesłać z PC do produktu lub na odwrót.	
ipsec.secrets	Tu wybiera się plik konfiguracyjny IPsec, który należy przesłać z PC do produktu.	

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**.

Aby wybrać plik na komputerze, należy kliknąć pole wyboru **Choose file …**.

Aby przesłać wybrany plik z PC do produktu, należy kliknąć przycisk **[Upload]**.

Aby przesłać plik z produktu do PC, należy kliknąć przycisk **[Download]**.

Zmiany zostaną zrealizowane dopiero po następnym restarcie produktu. W tym celu należy skorzystać z funkcji Reboot WBM. Nie należy wyłączać produktu zbyt wcześnie!

15.1.1.4.2 Strona „General Firewall Configuration“

Na stronie „General Firewall Configuration“ można znaleźć globalne ustawienia dla funkcji Firewall.

Grupa „Global Firewall Parameter“

Tabela 108: Strona WBM „General Firewall Configuration“ – grupa „Global Firewall Parameter“

Parametr	Znaczenie
Firewall enabled entirely	Tu aktywuje się i dezaktywuje wszystkie funkcje firewall. To ustawienie ma najwyższy priorytet. Gdy firewall jest wyłączony, wszystkie inne ustawienia nie mają bezpośredniego znaczenia. Mimo to konfiguracja pozostałych parametrów jest możliwa, w celu odpowiedniego ich ustawienia przed włączeniem funkcji firewall. To ustawienie jest niezależne od ustawienia „Filter enabled“ w grupie „MAC address filter state Bridge <n>“ na stronie „MAC address filter state Bridge <n>“.
ICMP echo broadcast protection	Tu aktywuje się i dezaktywuje zabezpieczenie „ICMP echo broadcast“.
Max. UDP datagrams per second	Tu wpisuje się maksymalną liczbę datagramów z tymi samymi portami źródłowymi i tymi samymi portami docelowymi między hostami na sekundę.
Max. TCP connections per second	Tu wpisuje się maksymalną liczbę połączeń ICP na sekundę.

Aby przejąć zmiany, należy kliknąć odpowiedni przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

15.1.1.4.3 Strona „Interface Configuration“

Na stronie „Interface Configuration“ znajdują się ustawienia funkcji firewall dla poszczególnych złącz.

Grupa „Firewall Configuration Bridge <n> / VPN / WAN“

Dla każdego skonfigurowanego bridge'a wyświetlana jest osobna grupa. Ustawienia w tej grupie dotyczą konfiguracji funkcji firewall na poziomie IP.

Tabela 109: Strona WBM „Interface Configuration“ – grupa „Firewall Configuration Bridge <n> / VPN / WAN“

Parametr	Znaczenie
Firewall enabled for Interface	Tu aktywuje się i dezaktywuje funkcję firewall dla poszczególnych bridge'ów.
ICMP echo protection	Tu aktywuje się i dezaktywuje zabezpieczenie „ICMP echo“ dla poszczególnych bridge'ów. Po aktywowaniu ochrony „ICMP echo“ wszystkie „ICMP Echo Requests“ (Pings) zostają odrzucone, a wartości wprowadzone w „ICMP echo limit per second“ i „ICMP burst limit“ są nieskuteczne.
ICMP echo limit per second	Tu wpisuje się maksymalną liczbę „ICMP pings“ na sekundę. Wprowadzanie danych jest skuteczne tylko przy dezaktywowanej ochronie „ICMP echo protection“. „0“ = „Disabled“
ICMP burst limit (0 = disabled)	Tu wpisuje się maksymalną liczbę „ICMP echo burst“ na sekundę. Wprowadzanie danych jest skuteczne tylko przy dezaktywowanej ochronie „ICMP echo protection“. „0“ = „Disabled“
Service Configuration	Tu aktywuje się i dezaktywuje funkcję firewall dla poszczególnych usług.
FTP/FTPES	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)	
DNP3 (port 20000)	
IEC60870-5-104 (port 2404)	
IEC61850 (port 102)	

Aby przejąć zmiany, należy kliknąć odpowiedni przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

15.1.1.4.4 Strona „Configuration of MAC address filter“

Na stronie „Configuration of MAC address filter“ ustawia się konfigurację funkcji firewall na poziomie sieci ETHERNET.

„MAC Address Filter Whitelist“ otrzymuje dwa domyślne wpisy o następujących wartościach:

Description:	All WAGO devices
MAC address:	00:30:DE:00:00:00
MAC mask:	ff:ff:ff:00:00:00

Description:	Enable docker bridge
MAC address:	02:42:00:00:00:00
MAC mask:	ff:ff:00:00:00:00

Po włączeniu pierwszego domyślnego wpisu można komunikować ze sobą w sieci różne urządzenia 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 urządzenia przez sieć ETHERNET. Dotyczy to także innych usług, wykorzystywanych przez urządzenie, np. konfiguracji IP przez DHCP.
Jeśli adresu MAC serwera DHCP nie ma na „MAC Address Filter Whitelist“, urządzenie po następnej aktualizacji straci swoje ustawienia IP i nie będzie już dostępne.
Dopóki „MAC Address Filter Whitelist“ będzie pusta, nie będzie można włączyć filtra.
Jeśli będzie na niej co najmniej jeden włączony adres, przed włączeniem zostanie jeszcze raz wysłane odpowiednie ostrzeżenie, które należy potwierdzić.
Opisany powyżej test przeprowadzany jest tylko w WBM, ale nie w CBM!

Grupa „Global MAC address filter state“

Tabela 110: Strona WBM „Configuration of MAC address filter“ – grupa „Global MAC address filter state“

Parametr	Znaczenie
Filter enabled	Tu aktywuje się i dezaktywuje globalny filtr adresów MAC.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

Grupa „MAC address filter state Bridge <n>“

Dla każdego skonfigurowanego bridge'a wyświetlana jest osobna grupa.

Tabela 111: Strona WBM „Configuration of MAC address filter“ – grupa „MAC address filter state Bridge <n>“

Parametr	Znaczenie
Filter enabled	Tu aktywuje się i dezaktywuje filtr adresów MAC dla poszczególnych bridge'ów. To ustawienie jest niezależne od ustawienia „Firewall enabled entirely“ na stronie „General Firewall Configuration“.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

Grupa „MAC address filter whitelist“

Dla każdej pozycji na liście wyświetlany jest osobny obszar.

Tabela 112: 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	Tu wyświetlany jest adres MAC danej pozycji na liście.
MAC mask	Tu wyświetlana jest maska MAC każdej danej na liście.
Filter enabled	Tu aktywuje się i dezaktywuje filtr dla danej pozycji na liście.
Add filter to whitelist	Tu tworzy się nową pozycję na liście.
MAC address	Tu wpisuje się adres MAC dla nowej pozycji na liście. Można wpisać 10 filtrów.
MAC mask	Tu wpisuje się maskę MAC dla nowej pozycji na liście.
Filter enabled	Tu aktywuje się i dezaktywuje filtr dla nowej pozycji na liście.

Aby przejąć zmiany, należy kliknąć odpowiedni przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

Aby usunąć pozycję na liście, należy kliknąć odpowiedni przycisk **[Delete]**. Zmiana zostaje zrealizowana natychmiast.

Aby przejąć nową pozycję na liście, należy kliknąć przycisk **[Add]**. Można wpisać 10 filtrów. Zmiana zostaje zrealizowana natychmiast.

15.1.1.4.5 Strona „Configuration of User Filter“

Na stronie „Configuration of User Filter“ znajdują się ustawienia specyficznych dla użytkownika filtrów funkcji firewall.

Grupa „User filter“

Dla każdego skonfigurowanego filtra wyświetlany jest osobny obszar.

Tabela 113: Strona WBM „Configuration of User Filter“ – grupa „User filter“

Parametr	Znaczenie	
Policy	Tu wyświetlana jest informacja, czy dane urządzenie sieciowe jest przez filtr dopuszczone czy wykluczone.	
Source IP address	Tu wyświetlany jest źródłowy adres IP dla danego filtra.	
Source Netmask	Tu wyświetlana jest maska sieci źródłowej dla danego filtra.	
Source Port	Tu wyświetlany jest numer portu źródłowego dla danego filtra.	
Destination IP address	Tu wyświetlany jest docelowy adres IP dla danego filtra.	
Destination Netmask	Tu wyświetlana jest maska sieci docelowej dla danego filtra.	
Destination Port	Tu wyświetlany jest numer portu docelowego dla danego filtra.	
Protocol	Tu wyświetlane są dopuszczalne protokoły dla danego filtra.	
Input interface	Tu wyświetlane są dopuszczalne interfejsy dla danego filtra.	
Add new user filter	Maksymalnie można utworzyć 10 filtrów. W polach należy wpisać wartości, które mają być użyte dla filtra. Należy wpisać co najmniej 1 wartość, pozostałe pola mogą zostać puste.	
Policy	Tu definiuje się, czy dane urządzenie sieciowe ma być przez filtr dopuszczone czy wykluczone.	
	Allow	Urządzenie sieciowe jest dopuszczone.
	Drop	Urządzenie sieciowe jest wykluczone.
Source IP address	Tu wpisuje się źródłowy adres IP dla nowego filtra.	
Source netmask	Tu wpisuje się maskę sieci źródłowej dla nowego filtra.	
Source port	Tu wpisuje się numer portu źródłowego dla nowego filtra.	
Destination IP address	Tu wpisuje się docelowy adres IP dla nowego filtra.	
Destination subnet mask	Tu wpisuje się maskę sieci docelowej dla nowego filtra.	
Destination port	Tu wpisuje się numer portu docelowego dla nowego filtra.	
Protocol	Tu wpisuje się protokoły dla nowego filtra.	
	TCP/ UDP	Serwisy TCP i UDP są filtrowane.
	TCP	Serwis TCP jest filtrowany.
	UDP	Serwis UDP jest filtrowany.
Input interface	Tu wpisuje się interfejsy dla nowego filtra.	
	Any	Wszystkie interfejsy są filtrowane.

Tabela 113: Strona WBM „Configuration of User Filter“ – grupa „User filter“

Parametr	Znaczenie	
	Bridge <n>	Filtrowane są interfejsy przypisane do bridge'a <n>. Wyświetlane są tylko skonfigurowane bridge.
	VPN	Interfejs VPN jest filtrowany.

Aby przejąć nowy filtr, należy kliknąć przycisk **[Add]**. Zmiana zostaje zrealizowana natychmiast.

Aby usunąć istniejący filtr, należy kliknąć przycisk **[Delete]**. Zmiana zostaje zrealizowana natychmiast.

15.1.1.4.6 Strona „Certificates“

Na stronie „Certificates“ można dokonać wyboru, czy dane certyfikaty i klucze zainstalować, czy usunąć.

Grupa „Installed Certificates“

Tabela 114: Strona WBM „Certificates“ – grupa „Certificate List“

Parametr	Znaczenie
<certificate name>	Tu wyświetlane są załadowane certyfikaty. Jeśli brak załadowanych certyfikatów, wyświetlana jest informacja „No certificates existing“.

Aby wybrać plik na komputerze, należy kliknąć pole wyboru **Choose file …**.

Aby przesłać wybrany plik do produktu, należy kliknąć przycisk **[Upload]**. Zmiany zostają zrealizowane natychmiast.

Certyfikaty zapisywane są w katalogu „/etc/certificates/“, a klucze w katalogu „/etc/certificates/keys/“.

Aby usunąć daną pozycję, należy kliknąć przycisk **[Delete]**. Zmiany zostają zrealizowane natychmiast.

Grupa „Installed Private Keys“

Tabela 115: Strona WBM „Certificates“ – grupa „Private Key List“

Parametr	Znaczenie
<private key name>	Tu wyświetlane są załadowane klucze. Jeśli brak załadowanych kluczy, wyświetlana jest informacja „No privace keys existing“.

Aby wybrać plik na komputerze, należy kliknąć pole wyboru **Choose file …**.

Aby przesłać wybrany plik do produktu, należy kliknąć przycisk **[Upload]**. Zmiany zostają zrealizowane natychmiast.

Certyfikaty zapisywane są w katalogu „/etc/certificates/“, a klucze w katalogu „/etc/certificates/keys/“.

Aby usunąć daną pozycję, należy kliknąć przycisk **[Delete]**. Zmiany zostają zrealizowane natychmiast.

15.1.1.4.7 Strona „Boot mode configuration“

Na stronie „Boot mode configuration“ znajdują się ustawienia opcji bootowania.

Grupa „Force internal boot“

Tabela 116: Strona WBM „Boot mode configuration” – grupa „Force internal boot“

Parametr	Znaczenie	
Boot mode	Tu ustawia się opcję bootowania dla produktu.	
	Memory card or internal flash	Bootowanie możliwe jest z wewnętrznej pamięci flash lub z karty pamięci.
	Internal flash only	Bootowanie możliwe jest tylko z wewnętrznej pamięci flash.

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“.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

15.1.1.4.8 Grupa „Security Settings“

Na stronie „Security Settings“ znajdują się ustawienia dotyczące bezpieczeństwa sieci.

Grupa „TLS Configuration“

Tabela 117: Strona WBM „Security Settings“ – grupa „TLS Configuration“

Parametr	Znaczenie	
TLS Configuration	Tu ustawia się dopuszczalne wersje TLS i procedur kryptograficznych dla HTTPS.	
	Standard	Serwer WWW zezwala na wersje TLS 1.0, TLS 1.1, TLS 1.2, a także metody kryptograficzne, które obecnie nie są już uważane za bezpieczne.
	Strong	Serwer WWW zezwala tylko na wersję TLS 1.2 i na silne algorytmy. Starsze oprogramowanie i starsze systemy operacyjne mogą nie obsługiwać protokołu TLS 1.2.

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

Informacja

Techniczna dyrektywa TR-02102 BSI
Zasady dotyczące ustawienia „Strong“ są oparte na wytycznej technicznej TR-02102 Federalnego Urzędu ds. Bezpieczeństwa Informacji.
Wytyczne można znaleźć na stronie: https://www.bsi.bund.de > „Publikacje“ > „Wytyczne techniczne“.

15.1.1.4.9 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 118: Strona WBM „Advanced Intrusion Detection Environment (AIDE)” – grupa „Run AIDE check at startup“

Parametr	Znaczenie
Service active	Tu można aktywować/dezaktywować „AIDE check“ przy starcie sterownika.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiany zostaną zrealizowane przy następnym restarcie.

Grupa „Refresh Options“

Tabela 119: Strona WBM „Advanced Intrusion Detection Environment (AIDE)” – grupa „Control AIDE and show log“

Parametr	Znaczenie	
Select Action	Tu wybiera się działanie do wykonania.	
	readlog	Wyświetlane są dane logowania.
	init	Instalowana jest baza danych, która uzupełniana jest aktualnymi wartościami.
	check	Aktualne wartości zostają porównane z wartościami zapisanymi w bazie danych.
	update	Aktualne wartości zostają porównane z wartościami zapisanymi w bazie danych, a następnie baza danych jest aktualizowana.
Read only the last n	Tu włącza się wyświetlanie ostatnich n komunikatów. Dodatkowo wpisuje się liczbę wyświetlonych komunikatów.	
Automatic refresh interval (sec)	Aby włączyć cykliczną aktualizację, należy zaznaczyć odpowiednie pole. Należy wpisać odstęp czasowy (w sekundach) cyklicznych aktualizacji. W zależności od statusu zmienia się opis przycisku („Refresh“/„Start“/„Stop“).	

Aby zaktualizować wyświetlenie, należy kliknąć przycisk **[Refresh]**. Przycisk jest widoczny tylko wtedy, gdy cykliczna aktualizacja nie jest włączona.

Aby aktywować cykliczną aktualizację, należy kliknąć przycisk **[Start]**. Przycisk ten jest widoczny tylko wtedy, gdy cykliczna aktualizacja jest włączona, ale jeszcze nie została uruchomiona.

Aby zakończyć cykliczną aktualizację, należy kliknąć przycisk **[Stop]**. Przycisk ten jest widoczny tylko wtedy, gdy cykliczna aktualizacja jest aktywna.

Cykliczną aktualizację można przeprowadzić tylko wtedy, jeśli otwarta jest strona „Advanced Intrusion Detection Environment (AIDE)“. Przy zmianie strony WBM aktualizacja zostaje zatrzymana do momentu, aż strona „Advanced Intrusion Detection Environment (AIDE)“ zostanie ponownie otwarta.

Komunikaty wyświetlane są pod ustawieniami.

15.1.1.4.10 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 „WAGO Device Access“ znajduje się jeszcze w statusie beta!

Grupa „Unauthenticated Requests“

Tabela 120: 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. Aby zwiększyć poziom bezpieczeństwa, można wymusić uwierzytelnienie dla skanowania węzła. W aktualnym statusie beta przy skanowaniu rozpoznawane są tylko jednostki bazowe, ale nie moduły I/O!

Aby przejąć zmianę, należy kliknąć przycisk **[Submit]**. Zmiana zostaje zrealizowana natychmiast.

15.1.1.5 Zakładka „Diagnostic“

15.1.1.5.1 Strona „Log Message Viewer“

Na stronie „Log Message Viewer“ znajdują się ustawienia do wyświetlania komunikatów diagnostycznych.

Grupa „Refresh Options“

Tabela 121: Strona WBM „Log Message Viewer“ – grupa „Refresh Options“

Parametr	Znaczenie	
Read only the last	Tu włącza się wyświetlanie ostatnich n komunikatów. Dodatkowo wpisuje się liczbę wyświetlonych komunikatów.	
Automatic refresh interval (sec)	Aby włączyć cykliczną aktualizację, należy zaznaczyć odpowiednie pole. Należy wpisać odstęp czasowy (w sekundach) cyklicznych aktualizacji. W zależności od statusu zmienia się opis przycisku („Refresh“/„Start“/„Stop“).	
Source	Tu wybiera się źródło komunikatów diagnostycznych. Lista rozwijalna zależy od zalogowanego użytkownika.	
	user	Tylko standardowe komunikaty diagnostyczne
	admin	Standardowe komunikaty diagnostyczne i wszystkie dane logowania w folderze `/var/log/*`

Aby zaktualizować wyświetlenie lub aktywować cykliczną aktualizację, należy kliknąć przycisk **[Refresh]**. Przycisk ten jest widoczny tylko wtedy, gdy cykliczna aktualizacja nie jest włączona.

Aby aktywować cykliczną aktualizację, należy kliknąć przycisk **[Start]**. Przycisk ten jest widoczny tylko wtedy, gdy cykliczna aktualizacja jest włączona, ale jeszcze nie została uruchomiona.

Aby zakończyć cykliczną aktualizację, należy kliknąć przycisk **[Stop]**. Przycisk ten jest widoczny tylko wtedy, gdy cykliczna aktualizacja jest aktywna.

Cykliczną aktualizację można przeprowadzić tylko wtedy, jeśli otwarta jest strona „Diagnostic Information“. Przy zmianie strony WBM aktualizacja zostaje zatrzymana do momentu, aż strona „Diagnostic Information“ zostanie ponownie otwarta.

Komunikaty wyświetlane są pod ustawieniami.

15.1.1.5.2 Strona „Download“

Grupa „Diagnostic Information“

Aby pobrać informacje diagnostyczne z urządzenia, należy kliknąć przycisk **[Download]**.
Od razu tworzony jest plik archiwalny, zawierający komunikaty dziennika zdarzeń, wersję firmware'u i listę zainstalowanych pakietów. Plik ten zostanie zapisany w katalogu rzeczy pobranych na komputerze.

15.1.1.5.3 Strona „Network Capture“

Na stronie „Network Capture“ znajdują się ustawienia niezbędne do rejestracji i pobierania komunikacji sieciowej na urządzeniu.
Zostaje wyświetlony aktualny status rejestracji sieci.

Grupa „State“

Tabela 122: Strona WBM „Network Capture“ – grupa „State“

Parametr	Znaczenie
Current State	Tu wyświetlany jest aktualny status rejestracji sieci.
Last Captured Package Count	Tu wyświetlane są już zarejestrowane pakiety sieciowe.
Last Refresh Time	Tu wyświetlany jest czas ostatniej aktualizacji Current State i Last Captured Package Count.

Grupa „Configuration“

Tabela 123: Strona WBM „Network Capture“ – grupa „Configuration“

Parametr	Znaczenie	
Enable	Tu włącza się i wyłącza rejestrację.	
Rotate Log Files	Tu włącza się i wyłącza rejestrację rotacyjną. Gdy ta opcja jest włączona, komunikacja sieciowa jest zapisywany w maksymalnie trzech plikach o ustawionym maksymalnym rozmiarze. Po osiągnięciu maksymalnego rozmiaru pierwszego pliku dane są nadal zapisywane w drugim pliku itd. Jeśli maksymalny rozmiar trzeciego pliku zostanie osiągnięty, dane pierwszego pliku zostaną nadpisane.	
Max. Filesize	Tu wpisuje się maksymalny rozmiar pliku do rejestracji danych.	
Storage Location	Tu wybiera się miejsce rejestracji danych. Wybór możliwy jest tylko wtedy, gdy istnieją obie pamięci.	
	Internal-Flash	Dane są zapisywane w wewnętrznej pamięci sterownika.
	SD-Card	Dane są zapisywane 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	Tu wybiera się interfejs sieciowy, z którego ma być wybrana komunikacja sieciowa. Do wyboru są dostępne interfejsy sieciowe urządzenia.	

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiany zostają zrealizowane natychmiast.

Grupa „Filter Configuration“

Tabela 124: Strona WBM „Network Capture“ – grupa „Filter Configuration“

Parametr	Znaczenie
Capture Filter	Tu można podać filtry rejestracji. Służą one do wybierana tylko istotnych lub pożądanych danych. W ten sposób możliwa jest na przykład rejestracja tylko komunikacji z tylko jednego portu lub z określonego adresu IP. Więcej informacji na temat możliwych ustawień filtra można znaleźć w objaśnieniach „Capture Filter“ w dokumentacji „Wireshark“.

Aby sprawdzić poprawność podanego „Capture Filter“, należy kliknąć przycisk **[Check]**.

Aby przejąć zmiany, należy kliknąć przycisk **[Submit]**. Zmiany zostają zrealizowane natychmiast.

Grupa „Log Download“

Tabela 125: Strona WBM „Network Capture“ – grupa „Log Download“

Parametr	Znaczenie
Select Log File	Tu wybiera się plik dziennika zdarzeń, który można pobrać przy pomocy przycisku **[Download]**.

Aby pobrać wybrany plik dziennika zdarzeń z urządzenia, należy kliknąć przycisk **[Download]**.

Aby pobrać wszystkie istniejące pliki dziennika zdarzeń z urządzenia, należy kliknąć przycisk **[Download All]**.

Spis ilustracji

Ilustracja 1: Widok z przodu 19
Ilustracja 2: Widok z góry 19
Ilustracja 3: Nadruk (przykład) 20
Ilustracja 4: Tabliczka znamionowa (przykład) 21
Ilustracja 5: Podłączenie przy połączeniu DTE-DCE (1:1) 24
Ilustracja 6: Podłączenie przy połączeniu DCE-DCE (cross-over) 24
Ilustracja 7: Terminacja sieci RS-485 25
Ilustracja 8: Złącza DIO X11 (przykład) 28
Ilustracja 9: Schemat połączeń wewnętrznych 32
Ilustracja 10: Przykład hasła Linux® 41
Ilustracja 11: Reakcja przy starcie 45
Ilustracja 12: Przebieg procesu przeglądarki 46
Ilustracja 13: „WAGO Ethernet Settings“ – ekran startowy (przykład) 54
Ilustracja 14: „WAGO Ethernet Settings“ – zakładka „Network“ (przykład) 55
Ilustracja 15: „Open DHCP, przykład widoku“ 57
Ilustracja 16: Wpisywanie uwierzytelnienia (przykład) 60
Ilustracja 17: Przypomnienie o konieczności zmiany hasła 62
Ilustracja 18: Okno przeglądarki WBM (przykład) 67
Ilustracja 19: Wiesz nagłówkowy WBM z niewyświetlanymi zakładkami (przykład) 67
Ilustracja 20: Wiersz statusu WBM (przykład) 68
Ilustracja 21: Demontaż z szyny 79

Indeks tabel

Tabela 1: Zastosowane systemy liczbowe....12
Tabela 2: Sposoby zapisu....12
Tabela 3: Nadruk....20
Tabela 4: Tabliczka znamionowa....20
Tabela 5: Złącza z przodu obudowy....22
Tabela 6: Złącza u góry....22
Tabela 7: Znaczenie pinów X3....23
Tabela 8: Funkcja sygnałów RS-232 przy DTE/DCE....24
Tabela 9: Znaczenie pinów X4....25
Tabela 10: Znaczenie pinów X5....26
Tabela 11: Znaczenie pinów X11....27
Tabela 12: LED SYS....30
Tabela 13: LED RUN....30
Tabela 14: LED CAN....30
Tabela 15: Ustawienia przełącznika trybu pracy....31
Tabela 16: Dane techniczne – urządzenie....33
Tabela 17: Dane techniczne – warunki klimatyczne....33
Tabela 18: Dane techniczne – zasilanie....33
Tabela 19: Dane techniczne – sprzęt....34
Tabela 20: Dane techniczne – komunikacja....34
Tabela 21: Dane techniczne − złącza....34
Tabela 22: Dane techniczne – złącza....35
Tabela 23: Użytkownicy WBM....39
Tabela 24: Użytkownicy Linux® 40
Tabela 25: Fabryczne ustawienie dla adresowania IP interfejsu ETHERNET....53
Tabela 26: Maska sieci 255.255.255.0....53
Tabela 27: Fabryczne ustawienia użytkownika....62
Tabela 28: Prawa dostępu dla stron WBM....64
Tabela 29: Priorytety CODESYS V3....71
Tabela 30: Sygnalizacja LED....74
Tabela 31: Akcesoria – karty pamięci....82
Tabela 32: Akcesoria – przewody przyłączeniowe i wtyki....82
Tabela 33: Strona WBM „Device Status“ – grupa „Device Details“....83
Tabela 34: Strona WBM „Device Status“ – grupa „Network TCP/IP Details“....84
Tabela 35: Strona WBM „PLC Runtime Information” – grupa „Runtime“....86
Tabela 36: Strona WBM „PLC Runtime Configuration” – grupa „General PLC Runtime Configuration“....92
Tabela 37: Strona WBM „PLC Runtime Configuration” – grupa „Webserver Configuration“....93
Tabela 38: Strona WBM „TCP/IP Configuration“ – grupa „TCP/IP Configuration“....94
Tabela 39: Strona WBM „TCP/IP Configuration“ – grupa „DNS Server“....95
Tabela 40: Strona WBM „Ethernet Configuration“ – grupa „Bridge Configuration“....96
Tabela 41: Strona WBM „Ethernet Configuration“ – grupa „Switch Configuration“....97
Tabela 42: Strona WBM „Ethernet Configuration“ – grupa „Dummy Interfaces“..98

Tabela 43: Strona WBM „Ethernet Configuration“ – grupa „VLAN Interfaces“ 98
Tabela 44: Strona WBM „Ethernet Configuration“ – grupa „Ethernet Interface Configuration“ 99
Tabela 45: Strona WBM „Configuration of Host and Domain Name“ – grupa „Hostname“ 100
Tabela 46: Strona WBM „Configuration of Host and Domain Name“ – grupa „Domain Name“....100
Tabela 47: Strona WBM „Routing“ – grupa „IP Forwarding through multiple interfaces“ 102
Tabela 48: Strona WBM „Routing“ – grupa „Custom Routes“....103
Tabela 49: Strona WBM „Routing“ – grupa „IP-Masquerading“ 105
Tabela 50: Strona WBM „Routing“ – grupa „Port Forwarding“ 106
Tabela 51: Strona „Clock Setting“ – grupa „Timezone and Format“....107
Tabela 52: Strona WBM „Clock Settings“ – grupa „UTC Time and Date“....107
Tabela 53: Strona WBM „Clock Settings“ – grupa „Local Time and Date“ 108
Tabela 54: Strona WBM „Configuration of Serial Interface RS232” – grupa „Assign Owner of Serial Interface“....109
Tabela 55: Strona WBM „Configuration of Serial Interface RS232” – grupa „Assign Owner of Serial Interface“....109
Tabela 56: Strona WBM „Configuration of Service Interface” – grupa „ Assign Owner of Service Interface“....111
Tabela 57: Strona WBM „Create bootable Image” – grupa „Create bootable image from boot device“....112
Tabela 58: Strona WBM „Firmware Backup“ – grupa „Firmware Backup“....113
Tabela 59: Strona WBM „Firmware Restore“ – grupa „Firmware Restore“ 115
Tabela 60: Strona WBM „Active System“ – grupa "Boot Device"....117
Tabela 61: Strona WBM „Active System“ – grupa „System <n> (Internal Flash)“ 117
Tabela 62: Strona WBM „Mass Storage“ – grupa „Devices"....118
Tabela 63: Strona WBM „Mass Storage“ – grupa "Create new Filesystem on Memory Card“....118
Tabela 64: Strona WBM „Software Uploads“ – grupa „Upload new Software“ ..119
Tabela 65: Strona WBM „Configuration of Network Services“ – grupa „FTP“ ...120
Tabela 66: Strona WBM „Configuration of Network Services“ – grupa „FTPES (explicit FTPS)“ 120
Tabela 67: Strona WBM „Configuration of Network Services“ – grupa „HTTP“.121
Tabela 68: Strona WBM „Configuration of Network Services“ – grupa „HTTPS“ 121
Tabela 69: Strona WBM „Configuration of Network Services“ – grupa „I/O-*CHECK*“ 121
Tabela 70: Strona WBM „Configuration of NTP Client“ – grupa „NTP Client Configuration“ 122
Tabela 71: Strona WBM „PLC Runtime Services“ – grupa „CODESYS V3“ 123
Tabela 72: Strona WBM „SSH Server Settings“ – grupa „SSH Server“ 124
Tabela 73: Strona WBM „DHCP Server Configuration“ – grupa „DHCP Configuration Bridge <n>“ 125
Tabela 74: Strona WBM „Configuration of DNS Server“ – grupa „DNS Server“ 126
Tabela 75: Strona WBM „Overview“ – grupa „Connection <n>“....127
Tabela 76: Strona WBM „Configuration of Connection <n>“ – grupa „Configuration“ 128

Tabela 77: Zależności między polami wyboru i edycji a poszczególnymi platformami chmury....131
Tabela 78: Możliwość wyboru protokołu danych dla poszczególnych platform chmury....133
Tabela 79: Zależności między polami wyboru i edycji a poszczególnymi protokołami danych....133
Tabela 80: Możliwość wyboru trybu pamięci podręcznej dla poszczególnych platform chmury....133
Tabela 81: Zależności między polami wyboru i edycji a poszczególnymi uwierzytelnieniami....134
Tabela 82: Strona WBM „Configuration of General SNMP Parameter“ – grupa „General SNMP Configuration“....135
Tabela 83: Strona WBM „Configuration of SNMP v1/v2c Parameters“ – grupa „Communities“....136
Tabela 84: Strona WBM „Configuration of SNMP v1/v2c Parameters“ – grupa „Trap Receivers“....137
Tabela 85: Strona WBM „Configuration of SNMP v3 Parameters“ – grupa „User“....138
Tabela 86: Strona WBM „Configuration of SNMP v3 Parameters“ – grupa „Trap Receivers“....140
Tabela 87: Strona WBM „Favorites” – grupy „Favorite n“....143
Tabela 88: MicroBrowser – dane logowania....143
Tabela 89: Strona WBM „Monitoring” – grupa „Monitoring“....145
Tabela 90: Strona WBM „Browser Security” – grupa „Browser Security“....146
Tabela 91: Strona WBM „Docker Settings“ – grupa „Docker Status“....147
Tabela 92: Strona WBM „Screensaver ” – grupa „Screensaver Settings“....150
Tabela 93: Strona WBM „Screensaver ” – grupa „Screen Care“....151
Tabela 94: Strona „WBM User Configuration” – grupa „Change Password“....152
Tabela 95: Strona WBM „OPC UA Configuration“ – grupa „OPC UA Server Configuration“....153
Tabela 96: Strona WBM „OPC UA Configuration“ – grupa „OPC UA Server Security Settings“....154
Tabela 97: Strona WBM „BACnet Status” – grupa „BACnet Information“....155
Tabela 98: Strona WBM „BACnet Status” – grupa „BACnet License“....155
Tabela 99: Strona WBM „BACnet Configuration” – grupa „BACnet Service“....156
Tabela 100: Strona WBM „BACnet Configuration” – grupa „BACnet Settings“....156
Tabela 101: Strona WBM „BACnet Configuration” – grupa „BACnet Data Reset“....157
Tabela 102: Strona WBM „BACnet Storage Location” – grupa „BACnet Persistence“....158
Tabela 103: Strona WBM „BACnet Storage Location” – grupa „BACnet Trendlog“....159
Tabela 104: Strona WBM- „BACnet Storage Location” – grupa „BACnet Eventlog“....159
Tabela 105: Strona WBM „BACnet Files” – grupa „BACnet override.xml“....160
Tabela 106: Strona WBM „OpenVPN / IPsec Configuration“ – grupa „OpenVPN“....161
Tabela 107: Strona WBM „OpenVPN / IPsec Configuration“ – grupa „IPsec“....162
Tabela 108: Strona WBM „General Firewall Configuration“ – grupa „Global Firewall Parameter“....163

Tabela 109: Strona WBM „Interface Configuration“ – grupa „Firewall Configuration Bridge <n> / VPN / WAN“....165
Tabela 110: Strona WBM „Configuration of MAC address filter“ – grupa „Global MAC address filter state“....167
Tabela 111: Strona WBM „Configuration of MAC address filter“ – grupa „MAC address filter state Bridge <n>“....167
Tabela 112: Strona WBM „Configuration of MAC address filter“ – grupa „MAC address filter whitelist“....168
Tabela 113: Strona WBM „Configuration of User Filter“ – grupa „User filter“....170
Tabela 114: Strona WBM „Certificates“ – grupa „Certificate List“....172
Tabela 115: Strona WBM „Certificates“ – grupa „Private Key List“....172
Tabela 116: Strona WBM „Boot mode configuration” – grupa „Force internal boot“....173
Tabela 117: Strona WBM „Security Settings“ – grupa „TLS Configuration“....174
Tabela 118: Strona WBM „Advanced Intrusion Detection Environment (AIDE)” – grupa „Run AIDE check at startup“....175
Tabela 119: Strona WBM „Advanced Intrusion Detection Environment (AIDE)” – grupa „Control AIDE and show log“....175
Tabela 120: Strona WBM „WAGO Device Access” – grupa „Unauthenticated Requests“....177
Tabela 121: Strona WBM „Log Message Viewer“ – grupa „Refresh Options“....178
Tabela 122: Strona WBM „Network Capture“ – grupa „State“....180
Tabela 123: Strona WBM „Network Capture“ – grupa „Configuration“....181
Tabela 124: Strona WBM „Network Capture“ – grupa „Filter Configuration“....182
Tabela 125: Strona WBM „Network Capture“ – grupa „Log Download“....182

WAGO GmbH & Co. KG
Postfach 2880 • 32385 Minden
Hansastraße 27 • 32423 Minden
Telefon: 0571/887 – 0
Faks: 0571/887 – 844169
e-mail: info@wago.com
Internet: www.wago.com