WAGO-I/O-SYSTEM 750

750-332
FC BACnet/IP; G4
Fieldbus Coupler BACnet/IP; Generation 4

Version 1.0.1
Every conceivable measure has been taken to ensure the accuracy and completeness of this documentation. However, as errors can never be fully excluded, we always appreciate any information or suggestions for improving the documentation.

E-Mail: documentation@wago.com

We wish to point out that the software and hardware terms as well as the trademarks of companies used and/or mentioned in the present manual are generally protected by trademark or patent.

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.
Table of Contents

1 Notes about this Documentation .............................................................. 9
  1.1 Validity of this Documentation............................................................. 9
  1.2 Copyright............................................................................................ 9
  1.3 Property rights.................................................................................... 10
  1.4 Symbols ............................................................................................. 11
  1.5 Number Notation................................................................................ 13
  1.6 Font Conventions................................................................................ 13

2 Important Notes ........................................................................................ 14
  2.1 Legal Bases ........................................................................................ 14
    2.1.1 Subject to Changes ..................................................................... 14
    2.1.2 Personnel Qualifications............................................................. 14
    2.1.3 Use of the 750 Series in Compliance with Underlying Provisions .... 14
    2.1.4 Technical Condition of Specified Devices ..................................... 15
      2.1.4.1 Disposal ............................................................................ 15
      2.1.4.1.1 Electrical and Electronic Equipment ................................ 15
      2.1.4.1.2 Packaging ..................................................................... 16
    2.2 Safety Advice (Precautions) ............................................................. 17
    2.3 Special Use Conditions for ETHERNET Devices ................................. 20

3 System Description .................................................................................. 21
  3.1 Labeling ............................................................................................. 22
    3.1.1 Labeling Symbols ....................................................................... 22
    3.1.2 Manufacturing Number ............................................................... 23
    3.1.3 Hardware Address (MAC-ID) ....................................................... 24
    3.1.4 Update Matrix ............................................................................ 25
  3.2 Storage, Assembly and Transport ....................................................... 26
  3.3 Assembly Guidelines/Standards ............................................................ 26
  3.4 Power Supply ..................................................................................... 27
    3.4.1 Overcurrent Protection ............................................................... 27
    3.4.2 Isolation ....................................................................................... 28
    3.4.3 System Supply ............................................................................. 29
      3.4.3.1 Connection ........................................................................ 29
      3.4.3.2 Dimensioning .................................................................... 30
    3.4.4 Field Supply ............................................................................... 34
      3.4.4.1 Connection ........................................................................ 34
      3.4.4.2 Fusing via Power Supply Module ......................................... 36
      3.4.4.3 Fusing external ................................................................... 38
    3.4.5 Supplementary Power Supply Regulations .................................... 40
    3.4.6 Supply Example .......................................................................... 41
    3.4.7 Power Supply Unit ....................................................................... 43
  3.5 Grounding ........................................................................................... 44
    3.5.1 Grounding the DIN Rail ............................................................... 44
      3.5.1.1 Framework Assembly .......................................................... 44
      3.5.1.2 Insulated Assembly ............................................................... 44
    3.5.2 Grounding Function .................................................................... 45
  3.6 Shielding ............................................................................................. 46
    3.6.1 General ....................................................................................... 46
Table of Contents

4  Device Description ................................................................. 48
   4.1 View ...................................................................................... 51
   4.2 Connectors ............................................................................... 53
   4.2.1 Device Supply ...................................................................... 53
   4.2.2 Fieldbus Connection .............................................................. 54
   4.3 Display Elements ........................................................................ 55
   4.4 Operating Elements ................................................................. 56
   4.4.1 Service Interface .................................................................. 56
   4.4.2 Mode Selector Switch ............................................................ 57
   4.4.3 Address Selection Switch ....................................................... 58
   4.4.4 Memory Card Slot .................................................................. 59
   4.4.4.1 Inserting a Memory Card .................................................. 60
   4.4.4.2 Removing the Memory Card ............................................. 60
   4.5 Technical Data ........................................................................... 61
   4.5.1 Device Data ............................................................................ 61
   4.5.2 System Data ............................................................................ 61
   4.5.3 Supply ..................................................................................... 62
   4.5.4 Fieldbus BACnet/IP ................................................................. 62
   4.5.5 Accessories ............................................................................ 63
   4.5.6 Connection Type ..................................................................... 63
   4.5.7 Climatic Environmental Conditions ....................................... 64
   4.5.8 Mechanical Strength .............................................................. 65
   4.5.9 Software Compatibility .......................................................... 65
   4.6 Approvals .................................................................................. 66
   4.7 Standards and Guidelines .......................................................... 67
   4.8 BACnet-Building-Controller (B-BC) .......................................... 68
   4.8.1 BIBBs (BACnet Interoperability Building Blocks) ..................... 69
   4.8.2 Data Sharing BIBBs ................................................................. 71
   4.8.3 Alarm and Event Management BIBBs ..................................... 73
   4.8.4 Scheduling BIBBs ................................................................. 75
   4.8.5 Trending BIBBs ..................................................................... 75
   4.8.6 Device- und Network-Management-BIBBs .............................. 77
   4.8.7 „Native“ Operation of the B-BC .......................................... 80
5  Mounting ....................................................................................... 82
   5.1 Installation Position .................................................................... 82
   5.2 Overall Configuration .............................................................. 82
   5.3 Mounting onto Carrier Rail ...................................................... 84
   5.3.1 Carrier Rail Properties ......................................................... 84
   5.3.2 WAGO DIN Rails ................................................................. 85
   5.4 Spacing ...................................................................................... 85
   5.5 Mounting Sequence ................................................................... 86
   5.6 Inserting and Removing Devices .............................................. 87
   5.6.1 Inserting the Fieldbus Coupler/Controller .............................. 88
   5.6.2 Removing the Fieldbus Coupler/Controller ............................ 88
   5.6.3 Inserting the I/O Module ....................................................... 89
   5.6.4 Removing the I/O Module ..................................................... 90
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Connect Devices</td>
<td>91</td>
</tr>
<tr>
<td>6.1</td>
<td>Data Contacts/Local Bus</td>
<td>91</td>
</tr>
<tr>
<td>6.2</td>
<td>Power Contacts/Field Supply</td>
<td>92</td>
</tr>
<tr>
<td>6.3</td>
<td>Connecting a Conductor to the CAGE CLAMP®</td>
<td>93</td>
</tr>
<tr>
<td>7</td>
<td>Function Description</td>
<td>94</td>
</tr>
<tr>
<td>7.1</td>
<td>Operating System</td>
<td>94</td>
</tr>
<tr>
<td>7.2</td>
<td>Process Data Architecture</td>
<td>95</td>
</tr>
<tr>
<td>7.2.1</td>
<td>Basic Setup</td>
<td>95</td>
</tr>
<tr>
<td>7.2.2</td>
<td>MODBUS Process Data</td>
<td>97</td>
</tr>
<tr>
<td>7.3</td>
<td>Data Exchange</td>
<td>98</td>
</tr>
<tr>
<td>7.3.1</td>
<td>Memory Space</td>
<td>99</td>
</tr>
<tr>
<td>7.3.2</td>
<td>Addressing</td>
<td>99</td>
</tr>
<tr>
<td>7.3.2.1</td>
<td>Addressing of I/O Modules</td>
<td>100</td>
</tr>
<tr>
<td>7.3.3</td>
<td>Data Exchange between MODBUS/TCP Master and I/O Modules</td>
<td>101</td>
</tr>
<tr>
<td>7.4</td>
<td>Memory Card Function</td>
<td>103</td>
</tr>
<tr>
<td>7.4.1</td>
<td>Transfer of Configuration Data and Automatic System Start</td>
<td>105</td>
</tr>
<tr>
<td>7.4.2</td>
<td>Back-up Function (Storing Device-internal Data and Settings on the Memory Card)</td>
<td>107</td>
</tr>
<tr>
<td>7.4.3</td>
<td>Restore Function (Loading Device-internal Data and Settings from the Memory Card)</td>
<td>109</td>
</tr>
<tr>
<td>7.4.4</td>
<td>Saving BACnet Trend Data</td>
<td>111</td>
</tr>
<tr>
<td>7.4.5</td>
<td>Inserting a Memory Card during Operation</td>
<td>112</td>
</tr>
<tr>
<td>7.4.6</td>
<td>Removing the Memory Card During Operation</td>
<td>113</td>
</tr>
<tr>
<td>7.4.7</td>
<td>FTP Network Access to the File System of the Memory Card</td>
<td>114</td>
</tr>
<tr>
<td>7.4.8</td>
<td>Directory Structure</td>
<td>115</td>
</tr>
<tr>
<td>8</td>
<td>Commissioning</td>
<td>116</td>
</tr>
<tr>
<td>8.1</td>
<td>Connecting Client PC and Fieldbus Nodes</td>
<td>117</td>
</tr>
<tr>
<td>8.2</td>
<td>Determining the IP Address of the PC</td>
<td>117</td>
</tr>
<tr>
<td>8.3</td>
<td>Assigning the IP Address to the Fieldbus Node</td>
<td>118</td>
</tr>
<tr>
<td>8.3.1</td>
<td>Information about the Starting Behavior regarding BACnet</td>
<td>119</td>
</tr>
<tr>
<td>8.3.2</td>
<td>Assigning IP Address via Address Selection Switch</td>
<td>120</td>
</tr>
<tr>
<td>8.3.3</td>
<td>Assigning IP Address via DHCP</td>
<td>121</td>
</tr>
<tr>
<td>8.3.3.1</td>
<td>Enable DHCP via &quot;WAGO Ethernet Settings&quot; (without existing IP address)</td>
<td>123</td>
</tr>
<tr>
<td>8.3.3.2</td>
<td>Enable DHCP via WBM (with existing IP address)</td>
<td>124</td>
</tr>
<tr>
<td>8.3.4</td>
<td>Assigning IP Address via &quot;WAGO Ethernet Settings&quot;</td>
<td>125</td>
</tr>
<tr>
<td>8.3.5</td>
<td>Assigning the IP Address via BootP</td>
<td>127</td>
</tr>
<tr>
<td>8.3.5.1</td>
<td>Reasons for Failed IP Address Assignment</td>
<td>129</td>
</tr>
<tr>
<td>8.4</td>
<td>Apply IP address permanently (option &quot;static&quot;)</td>
<td>130</td>
</tr>
<tr>
<td>8.5</td>
<td>Testing the Function of the Fieldbus Node</td>
<td>131</td>
</tr>
<tr>
<td>8.6</td>
<td>Preparing the Flash File System</td>
<td>132</td>
</tr>
<tr>
<td>8.7</td>
<td>Synchronizing the System Time</td>
<td>134</td>
</tr>
<tr>
<td>8.8</td>
<td>Restoring Factory Settings</td>
<td>136</td>
</tr>
<tr>
<td>9</td>
<td>Configuring via the Web-Based Management System (WBM)</td>
<td>137</td>
</tr>
<tr>
<td>9.1</td>
<td>WBM User Groups</td>
<td>137</td>
</tr>
<tr>
<td>9.2</td>
<td>Open WBM</td>
<td>138</td>
</tr>
<tr>
<td>9.3</td>
<td>WBM Pages</td>
<td>139</td>
</tr>
<tr>
<td>9.4</td>
<td>Information</td>
<td>140</td>
</tr>
</tbody>
</table>
Table of Contents

9.5 Administration ........................................................................................................ 141
9.6 Backup & Restore ................................................................................................. 144
9.7 Clock ..................................................................................................................... 147
9.8 Miscellaneous ........................................................................................................ 149
9.9 SD Card .................................................................................................................. 150
9.10 Storage Media ...................................................................................................... 150
9.11 Update ................................................................................................................... 151
9.12 Ethernet ............................................................................................................... 152
9.13 Protocols .............................................................................................................. 156
9.14 SNMP ................................................................................................................... 157
9.14.1 SNMP v1/v2c ............................................................................................... 158
9.14.2 SNMP V3 ...................................................................................................... 159
9.15 SNTP ..................................................................................................................... 160
9.16 TCP/IP .................................................................................................................. 161
9.17 BACnet .................................................................................................................. 162
9.18 BACnet Information ............................................................................................ 163
9.19 MODBUS ............................................................................................................. 165
9.20 I/O Config ............................................................................................................. 167

10 Diagnostics .............................................................................................................. 168
10.1 LED Signaling ..................................................................................................... 168
10.1.1 Evaluating Fieldbus Status .......................................................................... 169
10.1.2 Evaluating Node Status – I/O LED (Blink Code Table) .............................. 170
10.1.3 Evaluating Memory Card Status .................................................................. 180
10.1.4 Evaluating Power Supply Status .................................................................. 180
10.2 Fault Behavior .................................................................................................... 181
10.2.1 Fieldbus Failure ......................................................................................... 181
10.2.2 Local Bus Failure ....................................................................................... 181

11 Fieldbus Communication ......................................................................................... 183
11.1 Implemented Protocols ....................................................................................... 183
11.1.1 Communication Protocols ........................................................................... 183
11.1.1.1 IP (Internet Protocol) ............................................................................ 183
11.1.1.2 TCP (Transmission Control Protocol) ............................................... 188
11.1.1.3 UDP (User Datagram Protocol) .......................................................... 188
11.1.2 Configuration and Diagnostics Protocols ..................................................... 189
11.1.2.1 BootP (Bootstrap Protocol) .................................................................. 189
11.1.2.2 DHCP (Dynamic Host Configuration Protocol) .................................. 190
11.1.2.3 HTTP (Hypertext Transfer Protocol) ............................................... 193
11.1.2.4 DNS (Domain Name Systems) .............................................................. 193
11.1.2.5 FTP-Server (File Transfer Protocol) .................................................. 193
11.1.2.6 SNMP (Simple Network Management Protocol) ................................ 194
11.1.2.6.1 MIB II Description ........................................................................ 195
11.1.2.6.2 Traps ......................................................................................... 196
11.1.3 Application Protocols ..................................................................................... 197
11.2 BACnet/IP ............................................................................................................. 198
11.3 Modbus Functions ............................................................................................... 199
11.3.1 General .......................................................................................................... 199
11.3.2 Use of the MODBUS Functions .................................................................. 202
11.3.3 Description of the MODBUS Functions ....................................................... 203
11.3.3.1 Function Code FC1 (Read Coils) ....................................................... 204
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3.3.2 Function Code FC2 (Read Discrete Inputs)</td>
<td>206</td>
</tr>
<tr>
<td>11.3.3.3 Function Code FC3 (Read Multiple Registers)</td>
<td>208</td>
</tr>
<tr>
<td>11.3.3.4 Function Code FC4 (Read Input Registers)</td>
<td>209</td>
</tr>
<tr>
<td>11.3.3.5 Function Code FC5 (Write Coil)</td>
<td>210</td>
</tr>
<tr>
<td>11.3.3.6 Function Code FC6 (Write Single Register)</td>
<td>211</td>
</tr>
<tr>
<td>11.3.3.7 Function Code FC11 (Get Comm Event Counter)</td>
<td>212</td>
</tr>
<tr>
<td>11.3.3.8 Function Code FC15 (Write Multiple Coils)</td>
<td>213</td>
</tr>
<tr>
<td>11.3.3.9 Function Code FC16 (Write Multiple Registers)</td>
<td>215</td>
</tr>
<tr>
<td>11.3.3.10 Function Code FC22 (Mask Write Register)</td>
<td>216</td>
</tr>
<tr>
<td>11.3.3.11 Function Code FC23 (Read/Write Multiple Registers)</td>
<td>217</td>
</tr>
<tr>
<td>11.3.4 MODBUS Register Mapping</td>
<td>219</td>
</tr>
<tr>
<td>11.3.5 Modbus Registers</td>
<td>222</td>
</tr>
<tr>
<td>11.3.5.1 Accessing Register Values</td>
<td>224</td>
</tr>
<tr>
<td>11.3.5.2 Modbus-Watchdog</td>
<td>224</td>
</tr>
<tr>
<td>11.3.5.3 Modbus Watchdog Register</td>
<td>225</td>
</tr>
<tr>
<td>11.3.5.4 Diagnostic Registers</td>
<td>230</td>
</tr>
<tr>
<td>11.3.5.5 Configuration Registers</td>
<td>231</td>
</tr>
<tr>
<td>11.3.5.6 Constant Registers</td>
<td>233</td>
</tr>
<tr>
<td>11.3.5.7 Firmware Information Registers</td>
<td>235</td>
</tr>
<tr>
<td>12 I/O Modules</td>
<td>240</td>
</tr>
<tr>
<td>12.1 Overview</td>
<td>240</td>
</tr>
<tr>
<td>12.2 Process Data Architecture for Modbus TCP</td>
<td>240</td>
</tr>
<tr>
<td>13 Application Examples</td>
<td>242</td>
</tr>
<tr>
<td>13.1 Test of Modbus protocol and fieldbus nodes</td>
<td>242</td>
</tr>
<tr>
<td>13.2 Visualization and Control using SCADA Software</td>
<td>242</td>
</tr>
<tr>
<td>14 Use in Hazardous Environments</td>
<td>245</td>
</tr>
<tr>
<td>14.1 Marking Configuration Examples</td>
<td>246</td>
</tr>
<tr>
<td>14.1.1 Marking for Europe According to ATEX and IECEx</td>
<td>246</td>
</tr>
<tr>
<td>14.1.2 Marking for the United States of America (NEC) and Canada (CEC)</td>
<td>250</td>
</tr>
<tr>
<td>14.2 Installation Regulations</td>
<td>253</td>
</tr>
<tr>
<td>14.2.1 Special Notes including Explosion Protection</td>
<td>253</td>
</tr>
<tr>
<td>14.2.2 Special Notes Regarding ANSI/ISA Ex</td>
<td>255</td>
</tr>
<tr>
<td>15 Appendix</td>
<td>256</td>
</tr>
<tr>
<td>15.1 MIB II Groups</td>
<td>256</td>
</tr>
<tr>
<td>15.1.1 System Group</td>
<td>256</td>
</tr>
<tr>
<td>15.1.2 Interface Group</td>
<td>257</td>
</tr>
<tr>
<td>15.1.3 IP Group</td>
<td>259</td>
</tr>
<tr>
<td>15.1.4 IpRoute Table Group</td>
<td>260</td>
</tr>
<tr>
<td>15.1.5 ICMP Group</td>
<td>261</td>
</tr>
<tr>
<td>15.1.6 TCP Group</td>
<td>262</td>
</tr>
<tr>
<td>15.1.7 UDP Group</td>
<td>263</td>
</tr>
<tr>
<td>15.1.8 SNMP Group</td>
<td>264</td>
</tr>
<tr>
<td>15.2 WAGO MIB Groups</td>
<td>265</td>
</tr>
<tr>
<td>15.2.1 Company Group</td>
<td>265</td>
</tr>
<tr>
<td>15.2.2 Product Group</td>
<td>265</td>
</tr>
<tr>
<td>15.2.3 Versions Group</td>
<td>266</td>
</tr>
<tr>
<td>15.2.4 Real-Time Clock Group</td>
<td>267</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>15.2.5</td>
<td>Ethernet Group</td>
</tr>
<tr>
<td>15.2.6</td>
<td>Actual Error Group</td>
</tr>
<tr>
<td>15.2.7</td>
<td>PLC Project Group</td>
</tr>
<tr>
<td>15.2.8</td>
<td>Http Group</td>
</tr>
<tr>
<td>15.2.9</td>
<td>Ftp Group</td>
</tr>
<tr>
<td>15.2.10</td>
<td>Snmp Group</td>
</tr>
<tr>
<td>15.2.11</td>
<td>Snmp Trap String Group</td>
</tr>
<tr>
<td>15.2.12</td>
<td>Snmp User Trap String Group</td>
</tr>
<tr>
<td>15.2.13</td>
<td>Plc Connection Group</td>
</tr>
<tr>
<td>15.2.15</td>
<td>Modbus Group</td>
</tr>
<tr>
<td>15.2.16</td>
<td>Process Image Group</td>
</tr>
<tr>
<td>15.2.17</td>
<td>Plc Data Group</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Literature List</strong></td>
<td></td>
</tr>
<tr>
<td><strong>List of Figures</strong></td>
<td></td>
</tr>
<tr>
<td><strong>List of Tables</strong></td>
<td></td>
</tr>
</tbody>
</table>
1 Notes about this Documentation

**Note**

Always retain this documentation!
This documentation is part of the product. Therefore, retain the documentation during the entire service life of the product. Pass on the documentation to any subsequent user. In addition, ensure that any supplement to this documentation is included, if necessary.

1.1 Validity of this Documentation

This documentation is only applicable to the “FC BACnet/IP; G4” (750-332).

The product “FC BACnet/IP; G4” (750-332) shall only be installed and operated according to the instructions in this manual and the system description for the WAGO-I/O-SYSTEM 750.

**NOTICE**

Consider power layout of the WAGO-I/O-SYSTEM 750!
In addition to these operating instructions, you will also need the system description for the WAGO-I/O-SYSTEM 750, which can be downloaded at [www.wago.com](http://www.wago.com). There, you can obtain important information including information on electrical isolation, system power and supply specifications.

1.2 Copyright

This Manual, including all figures and illustrations, is copyright-protected. Any further use of this Manual by third parties that violate pertinent copyright provisions is prohibited. Reproduction, translation, electronic and phototechnical filing/archiving (e.g., photocopying) as well as any amendments require the written consent of WAGO Kontaktechnik GmbH & Co. KG, Minden, Germany. Non-observance will involve the right to assert damage claims.
1.3 **Property rights**

Third-party trademarks are used in this documentation. This section contains the trademarks used. The “®” and “TM” symbols are omitted hereinafter.

- Adobe® and Acrobat® are registered trademarks of Adobe Systems Inc.
- AS-Interface® is a registered trademark of AS-International Association.
- BACnet® is a registered trademark of American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc. (ASHRAE).
- Bluetooth® is a registered trademark of the Bluetooth SIG, Inc.
- CiA® and CANopen® are registered trademarks of CAN in AUTOMATION – International Users and Manufacturers Group e. V.
- DALI is a registered trademark of Digital Illumination Interface Alliance (DiiA).
- EtherCAT® is a registered trademark and patented technology of Beckhoff Automation GmbH.
- EtherNet/IP™ is a registered trademark of Open DeviceNet Vendor Association, Inc (ODVA).
- EnOcean® is a registered trademark of EnOcean GmbH.
- IO-Link is a registered trademark of PROFIBUS Nutzerorganisation e.V.
- KNX® is a registered trademark of KNX Association cvba.
- Linux® is a registered trademark of Linus Torvalds.
- LON® is a registered trademark of Echelon Corporation.
- Modbus® is a registered trademark of Schneider Electric, licensed to the Modbus Organization, Inc.
- PROFIBUS® is a registered trademark of Siemens AG.
- PROFINET® is a registered trademark of Siemens AG.
- Subversion® is a registered trademark of Apache Software Foundation.
- Windows® is a registered trademark of Microsoft Corporation.
## 1.4 Symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![DANGER]</td>
<td>Personal Injury! Indicates a high-risk, imminently hazardous situation which, if not avoided, will result in death or serious injury.</td>
</tr>
<tr>
<td>![DANGER]</td>
<td>Personal Injury Caused by Electric Current! Indicates a high-risk, imminently hazardous situation which, if not avoided, will result in death or serious injury.</td>
</tr>
<tr>
<td>![WARNING]</td>
<td>Personal Injury! Indicates a moderate-risk, potentially hazardous situation which, if not avoided, could result in death or serious injury.</td>
</tr>
<tr>
<td>![CAUTION]</td>
<td>Personal Injury! Indicates a low-risk, potentially hazardous situation which, if not avoided, may result in minor or moderate injury.</td>
</tr>
<tr>
<td>![NOTICE]</td>
<td>Damage to Property! Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.</td>
</tr>
<tr>
<td>![NOTICE]</td>
<td>Damage to Property Caused by Electrostatic Discharge (ESD)! Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.</td>
</tr>
<tr>
<td>![Note]</td>
<td>Important Note! Indicates a potential malfunction which, if not avoided, however, will not result in damage to property.</td>
</tr>
</tbody>
</table>
Information

Additional Information:
Refers to additional information which is not an integral part of this documentation (e.g., the Internet).
1.5 Number Notation

Table 1: Number Notation

<table>
<thead>
<tr>
<th>Number Code</th>
<th>Example</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decimal</td>
<td>100</td>
<td>Normal notation</td>
</tr>
<tr>
<td>Hexadecimal</td>
<td>0x64</td>
<td>C notation</td>
</tr>
<tr>
<td>Binary</td>
<td>'100'</td>
<td>In quotation marks, nibble separated with dots(.)</td>
</tr>
<tr>
<td></td>
<td>'0110.0100'</td>
<td></td>
</tr>
</tbody>
</table>

1.6 Font Conventions

Table 2: Font Conventions

<table>
<thead>
<tr>
<th>Font Type</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>italic</td>
<td>Names of paths and data files are marked in italic-type. e.g.: C:\Program Files\WAGO Software</td>
</tr>
<tr>
<td>Menu</td>
<td>Menu items are marked in bold letters. e.g.: Save</td>
</tr>
<tr>
<td>&gt;</td>
<td>A greater-than sign between two names means the selection of a menu item from a menu. e.g.: File &gt; New</td>
</tr>
<tr>
<td>Input</td>
<td>Designation of input or optional fields are marked in bold letters, e.g.: Start of measurement range</td>
</tr>
<tr>
<td>&quot;Value&quot;</td>
<td>Input or selective values are marked in inverted commas. e.g.: Enter the value “4 mA” under Start of measurement range</td>
</tr>
<tr>
<td>[Button]</td>
<td>Pushbuttons in dialog boxes are marked with bold letters in square brackets. e.g.: [Input]</td>
</tr>
<tr>
<td>[Key]</td>
<td>Keys are marked with bold letters in square brackets. e.g.: [F5]</td>
</tr>
</tbody>
</table>
2 Important Notes

This section includes an overall summary of the most important safety requirements and notes that are mentioned in each individual section. To protect your health and prevent damage to devices as well, it is imperative to read and carefully follow the safety guidelines.

2.1 Legal Bases

2.1.1 Subject to Changes

WAGO Kontakttechnik GmbH & Co. KG reserves the right to provide for any alterations or modifications. WAGO Kontakttechnik GmbH & Co. KG owns all rights arising from the granting of patents or from the legal protection of utility patents. Third-party products are always mentioned without any reference to patent rights. Thus, the existence of such rights cannot be excluded.

2.1.2 Personnel Qualifications

All sequences implemented on WAGO I/O SYSTEM 750 devices may only be carried out by electrical specialists with sufficient knowledge in automation. The specialists must be familiar with the current norms and guidelines for the devices and automated environments.

All changes to the coupler or controller should always be carried out by qualified personnel with sufficient skills in PLC programming.

2.1.3 Use of the 750 Series in Compliance with Underlying Provisions

Fieldbus couplers, controllers and I/O modules of the modular WAGO-I/O-SYSTEM 750 receive digital and analog signals from sensors and transmit them to actuators or higher-level control systems. Using controllers, the signals can also be (pre-) processed.

This product is designed for protection class IP20. There is protection against finger injury and solid impurities up to 12.5 mm diameter is assured; protection against water damage is not ensured.

The product represents an open-type device. It may only be installed in enclosures (tool-secured enclosures or operating rooms) which fulfil the listed requirements specified in the safety instructions in chapter “Safety Advice (Precautions)”.

The product is intended for installation in automation systems. It does not have its own integrated separator. A suitable separator must therefore be created on the plant side.
The operation of the product in residential areas without further measures is only permitted if the product complies with the emission limits (interference emissions) according to EN 61000-6-3.

Operating the product in home applications without further measures is only permitted if it meets the emission limits (emissions of interference) according to EN 61000-6-3.

You will find the relevant information in the section “Device Description” > “Standards and Guidelines” in the manual for the used fieldbus coupler/controller.

Appropriate housing (per 2014/34/EU) is required when operating the WAGO-I/O-SYSTEM 750 in hazardous environments. Please note that a prototype test certificate must be obtained that confirms the correct installation of the system in a housing or switch cabinet.

The implementation of safety functions such as EMERGENCY STOP or safety door monitoring must only be performed by the F I/O modules within the modular WAGO-I/O-SYSTEM 750. Only these safe F I/O modules ensure functional safety in accordance with the latest international standards. WAGO's interference-free output modules can be controlled by the safety function.

2.1.4 Technical Condition of Specified Devices

The devices to be supplied ex works are equipped with hardware and software configurations, which meet the individual application requirements. These modules contain no parts that can be serviced or repaired by the user. The following actions will result in the exclusion of liability on the part of WAGO Kontakttechnik GmbH & Co. KG:

- Repairs,
- Changes to the hardware or software that are not described in the operating instructions,
- Improper use of the components.

Further details are given in the contractual agreements. Please send your request for modified and new hardware or software configurations directly to WAGO Kontakttechnik GmbH & Co. KG.

2.1.4.1 Disposal

2.1.4.1.1 Electrical and Electronic Equipment

Electrical and electronic equipment may not be disposed of with household waste. This also applies to products without this symbol.

Electrical and electronic equipment contain materials and substances that can be harmful to the environment and health. Electrical and electronic equipment must
be disposed of properly after use. WEEE 2012/19/EU applies throughout Europe. Directives and laws may vary nationally.

Environmentally friendly disposal benefits health and protects the environment from harmful substances in electrical and electronic equipment.

- Observe national and local regulations for the disposal of electrical and electronic equipment.
- Clear any data stored on the electrical and electronic equipment.
- Remove any added battery or memory card in the electrical and electronic equipment.
- Have the electrical and electronic equipment sent to your local collection point.

Improper disposal of electrical and electronic equipment can be harmful to the environment and human health.

2.1.4.1.2 Packaging

Packaging contains materials that can be reused. PPWD 94/62/EU and 2004/12/EU packaging guidelines apply throughout Europe. Directives and laws may vary nationally.

Environmentally friendly disposal of the packaging protects the environment and allows sustainable and efficient use of resources.

- Observe national and local regulations for the disposal of packaging.
- Dispose of packaging of all types that allows a high level of recovery, reuse and recycling.

Improper disposal of packaging can be harmful to the environment and wastes valuable resources.
2.2 Safety Advice (Precautions)

For installing and operating purposes of the relevant device to your system the following safety precautions shall be observed:

---

**DANGER**

Do not work on devices while energized!
All power sources to the device shall be switched off prior to performing any installation, repair or maintenance work.

---

**DANGER**

Install device in only one suitable enclosure!
The device is an open system. Install the device in a suitable enclosure. This enclosure must:

- Guarantee that the max. permissible degree of pollution is not exceeded.
- Offer adequate protection against contact.
- Prevent fire from spreading outside of the enclosure.
- Offer adequate protection against UV irradiation.
- Guarantee mechanical stability
- Restrict access to authorized personnel and may only be opened with tools

---

**DANGER**

Ensure disconnect and overcurrent protection!
The device is intended for installation in automation technology systems. Disconnect protection is not integrated. Connected systems must be protected by a fuse.
Provide suitable disconnect and overcurrent protection on the system side!

---

**DANGER**

Ensure a standard connection!
To minimize any hazardous situations resulting in personal injury or to avoid failures in your system, the data and power supply lines shall be installed according to standards, with careful attention given to ensuring the correct terminal assignment. Always adhere to the EMC directives applicable to your application.
**NOTICE**

Do not use in telecommunication circuits!
Only use devices equipped with ETHERNET or RJ-45 connectors in LANs. Never connect these devices with telecommunication networks.

**NOTICE**

Ensure proper contact with the DIN-rail!
Proper electrical contact between the DIN-rail and device is necessary to maintain the EMC characteristics and function of the device.

**NOTICE**

Replace defective or damaged devices!
Replace defective or damaged device/module (e.g., in the event of deformed contacts).

**NOTICE**

Protect the components against materials having seeping and insulating properties!
The components are not resistant to materials having seeping and insulating properties such as: aerosols, silicones and triglycerides (found in some hand creams). If you cannot exclude that such materials will appear in the component environment, then install the components in an enclosure being resistant to the above-mentioned materials. Clean tools and materials are imperative for handling devices/modules.

**NOTICE**

Clean only with permitted materials!
Clean housing and soiled contacts with propanol.

**NOTICE**

Do not use any contact spray!
Do not use any contact spray. The spray may impair contact area functionality in connection with contamination.

**NOTICE**

Do not reverse the polarity of connection lines!
Avoid reverse polarity of data and power supply lines, as this may damage the devices involved.
Avoid electrostatic discharge!
The devices are equipped with electronic components that may be destroyed by electrostatic discharge when touched. Please observe the safety precautions against electrostatic discharge per DIN EN 61340-5-1/-3. When handling the devices, please ensure that environmental factors (personnel, work space and packaging) are properly grounded.
2.3 Special Use Conditions for ETHERNET Devices

If not otherwise specified, ETHERNET devices are intended for use on local networks. Please note the following when using ETHERNET devices in your system:

- Do not connect control components and control networks directly to an open network such as the Internet or an office network. WAGO recommends putting control components and control networks behind a firewall.

- In the control components (e.g., for WAGO I/-CHECK and CODESYS) close all ports and services not required by your application to minimize the risk of cyber attacks and to enhance cyber security. Only open ports and services during commissioning and/or configuration.

- Limit physical and electronic access to all automation components to authorized personnel only.

- Change the default passwords before first use! This will reduce the risk of unauthorized access to your system.

- Regularly change the passwords used! This will reduce the risk of unauthorized access to your system.

- If remote access to control components and control networks is required, use a Virtual Private Network (VPN).

- Regularly perform threat analyses. You can check whether the measures taken meet your security requirements.

- Use “defense-in-depth” mechanisms in your system's security configuration to restrict the access to and control of individual products and networks.
3 System Description

The WAGO-I/O-SYSTEM 750 is a modular, fieldbus-independent input/output system (I/O system). The configuration described here consists of a fieldbus coupler/controller (1) and the modular I/O modules (2) for any signal shapes that form the fieldbus node together. The end module (3) completes the node and is required for correct operation of the fieldbus node.

Fieldbus couplers/controllers are available for different fieldbus systems.

The extended ECO fieldbus couplers contain the fieldbus interface, electronics and a power supply terminal. The fieldbus interface forms the physical interface to the relevant fieldbus. The electronics process the data of the bus modules and make it available for the fieldbus communication. The 24 V system supply and the 24 V field supply are fed in via the integrated power supply terminal.

The fieldbus coupler/controller communicates via the relevant fieldbus. The programmable fieldbus controller (PFC) enables the implementation of additional PLC functions. Programming is done with the WAGO-I/O-PRO in accordance with IEC 61131-3.

I/O modules for diverse digital and analog I/O signals as well as special functions can be connected to the fieldbus coupler/controller. The communication between the fieldbus coupler/controller and the I/O modules is carried out via a local bus.

The components of the WAGO I/O SYSTEM 750 have clear termination points, light emitting diodes for status display, plug-in mini WSB tags and group marker cards for labeling.

The 1, 2 or 3 wire technology supplemented by a ground wire connection allows for direct sensor or actuator wiring.
3.1 Labeling

The front labeling includes:
- Device designation
- Name of the display elements, connections and control elements
- Serial number with hardware and firmware version

The side labeling includes:
- Manufacturer's identification
- Connector pin assignment
- Serial number
- Approval information

3.1.1 Labeling Symbols

Some general information and the respective product approvals are shown in the labeling as symbols.

Table 3: Labeling Symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Manufacturer's identification](Hansastr. 27 D-32423 Minden)</td>
<td>Manufacturer's identification</td>
<td>Manufacturer name and address</td>
</tr>
<tr>
<td>![Data matrix code](QR code)</td>
<td>Data matrix code</td>
<td>One-to-one product identification by means of UII (Unique Item Identifier)</td>
</tr>
<tr>
<td>![General warning label](exclamation mark)</td>
<td>General warning label</td>
<td>Read this manual carefully for safe use and proper handling</td>
</tr>
<tr>
<td>![ESD danger sign](triangle with lightning bolt)</td>
<td>ESD danger sign</td>
<td>Avoid electrostatic discharge! → See chapter “Safety Advice (Precautions)”</td>
</tr>
<tr>
<td><img src="cross" alt="WEEE label" /></td>
<td>WEEE label</td>
<td>Note on disposal → See chapter „Disposal”</td>
</tr>
</tbody>
</table>

Symbols of Approvals (Examples)

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="CE" alt="Conformity marking" /></td>
<td>Conformity marking</td>
<td>Approval information → See chapter “Approvals”</td>
</tr>
<tr>
<td><img src="KC" alt="Korean Certificate" /></td>
<td>Korean Certificate</td>
<td></td>
</tr>
<tr>
<td><img src="Ex" alt="Ex approvals" /></td>
<td>Ex approvals</td>
<td></td>
</tr>
<tr>
<td><img src="ship" alt="Ship approvals" /></td>
<td>Ship approvals</td>
<td></td>
</tr>
<tr>
<td><img src="T%C3%9CV" alt="TÜV symbol" /></td>
<td>TÜV symbol</td>
<td></td>
</tr>
</tbody>
</table>
3.1.2 Manufacturing Number

The serial number indicates the delivery status directly after production. This number is part of the labeling on the side of each component.

![Figure 2: Marking Area for Serial Numbers](image)

There are two serial numbers in two rows in the side marking. They are left of the release tab. The first 10 positions in the longer row of the serial numbers contain version and date identifications.

Example structure of the rows: 0114010101…

<table>
<thead>
<tr>
<th>WW</th>
<th>14</th>
<th>FW --</th>
<th>01</th>
<th>01</th>
<th>FL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendar week</td>
<td>Year</td>
<td>Firmware version</td>
<td>Hardware version</td>
<td>Firmware loader version</td>
<td>Internal information</td>
</tr>
</tbody>
</table>

The row order can vary depending on the production year, only the longer row is relevant. The back part of this and the shorter row contain internal administration information from the manufacturer.

In addition, the serial number is printed on the front on the cover cap of the service interface, so that it can also be read when installed.
3.1.3 **Hardware Address (MAC-ID)**

Each **FC BACnet/IP; G4** has an internationally unambiguous physical address, referred to as the MAC-ID (Media Access Control Identity).

As part of the labeling on the right side of this component, the MAC ID is printed in the block diagram.
In addition, the MAC ID is located on the paper strip with two self-adhesive peel-off strips on its left side.
The MAC ID has a fixed length of 6 bytes (48 bits) which are presented hexadecimal. The first three bytes identify the manufacturer (e.g. 00:30 DE for WAGO). The second 3 bytes comprise the unique serial number of the hardware.
3.1.4 Update Matrix

For products that can be updated, the side inscription has a prepared matrix in which the current update data can be entered in columns.

The matrix has rows to enter the “FA” production or work order number and to enter the “PD” production date and “AZ” item number.

Figure 3: Update Matrix from 2016

Table 4: Legend for Figure “Update Matrix from 2016”

| Description     | |
|-----------------|--|---|
| **FA**          | Production order number, 10-digit |
| **PD**          | KW = calendar week               |
|                 | YY = year                        |
| **AZ**          | FW = firmware index              |
|                 | HW = hardware index              |
|                 | FL = firmware loader index       |

For factory updates to a head station, the current production or work order number is also printed on the cover cap of the service interface.

The original manufacturing information on the product housing remains unchanged.
3.2 Storage, Assembly and Transport

Whenever possible, the components are to be stored in their original packaging. Likewise, the original packaging provides optimal protection during transport.

When assembling or repacking the components, the contacts must not be soiled or damaged. The components must be stored and transported in appropriate containers/packaging. Thereby, the ESD information is to be regarded.

3.3 Assembly Guidelines/Standards

• DIN 60204  Electrical equipment of machines
• DIN EN 50178  Electronic equipment for use in power installations (replacement for VDE 0160)
• EN 60439  Low-voltage switchgear and controlgear assemblies
3.4 Power Supply

3.4.1 Overcurrent Protection

**WARNING**

Possible fire hazard due to insufficient overcurrent protection!

In the event of a fault, insufficient overcurrent protection can present a possible fire hazard. In the event of a fault, excessive current flow in the components can cause significant overheating. Therefore, you should always dimension the overcurrent protection according to the anticipated power usage.

The system and field voltage of the WAGO-I/O-SYSTEMs 750 is supplied on the head stations and bus supply modules.

For components that work with extra low voltage, only SELV/PELV voltage sources should be used.

A single voltage source supplying multiple components must be designed according to the component with the strictest electrical safety requirements.

For components which are only allowed to be supplied by SELV voltage sources, these requirements are listed in the technical data.

Most components in the WAGO-I/O-SYSTEM 750 have no internal overcurrent protection. Therefore, appropriate overcurrent protection must always be implemented externally for the power supply to these components, e.g. via fuses.

The maximum permissible current is listed in the technical data of the components used.

**NOTICE**

System supply only with appropriate fuse protection!

Without overcurrent protection, the electronics can be damaged.

For 24V system supply input voltage an external fuse, rated max. 2 A, slow acting, min. 30 VDC shall be used.

**NOTICE**

Field supply only with appropriate fuse protection!

Without overcurrent protection, the electronics can be damaged.

For 24V field supply input voltage an external fuse, rated max. 10 A, slow acting, min. 30 VDC shall be used.
3.4.2 Isolation

Within the fieldbus node, there are three electrically isolated potentials:

- Electrically isolated fieldbus interface via transformer
- Electronics of the fieldbus couplers/controllers and the I/O modules (local bus)
- All I/O modules have an electrical isolation between the electronics (local bus, logic) and the field electronics. Some digital and analog input modules have each channel electrically isolated, please see catalog.

Figure 4: Isolation for Fieldbus Couplers/Controllers (Example)
3.4.3 System Supply

3.4.3.1 Connection

The WAGO-I/O-SYSTEM 750 requires a 24 V direct current system supply. The power supply is provided via the fieldbus coupler/controller and, if necessary, in addition via internal system supply modules 750-613. The power supply is reverse voltage protected.

**NOTICE**

*Do not use an incorrect voltage/frequency!*

The use of an incorrect supply voltage or frequency can cause severe damage to the components.

The fed-in 24 VDC supplies all internal system components, e.g. fieldbus coupler/controller electronics, fieldbus interface and I/O modules via the local bus (5 VDC system voltage). The 5 VDC system voltage is galvanically connected to the 24 VDC supply voltage.
System Description

NOTICE
System supply only with appropriate fuse protection!
Without overcurrent protection, the electronics can be damaged.
For 24V system supply input voltage an external fuse, rated max. 2 A, slow acting, min. 30 VDC shall be used.

Figure 6: System Voltage for Standard Couplers/Controllers and Extended ECO Couplers

Note
Only reset the system simultaneously for all supply modules!
Reset the system by switching the system supply simultaneously at all supply modules (fieldbus coupler/controller and potential supply module with bus power supply) off and on again.

3.4.3.2 Dimensioning

Note
Recommendation
A stable power supply cannot always be assumed. Therefore, you should use regulated power supplies to ensure the quality of the supply voltage.

The supply capacity of the fieldbus coupler/controller or the internal system supply module can be taken from the technical data of the components.
### Table 6: Alignment

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal current consumption</strong>&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Current consumption via system voltage (5 V for electronics of I/O modules and fieldbus coupler/controller).</td>
</tr>
<tr>
<td><strong>Total current for I/O modules</strong>&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Available current for the I/O modules. Provided by the bus power supply unit. See fieldbus coupler/controller and internal system supply module.</td>
</tr>
</tbody>
</table>

<sup>1</sup> See current catalog, manuals, Internet.
Example:

Calculating the current consumption on an Example Coupler:

- **Internal current consumption**: 380 mA at 5 V
- **Residual current for bus modules**: 1620 mA at 5 V
- **Sum I(5 V) total**: 2000 mA at 5 V

The internal current consumption is indicated in the technical data for each bus terminal. In order to determine the total requirement, add together the values of all I/O modules in the node.

---

Note

**Please note the aggregate current for I/O modules. It may be necessary to supply potential!**

When the sum of the internal current consumption for the I/O modules exceeds their aggregate current, you must use a supply module with bus power supply. Install it before the position where the permissible aggregate current would be exceeded.

Example:

Calculating the total current on the example coupler described above:

A node with the example coupler, which is described above, consists of:
20 relay modules (750-517) and 10 digital input modules (750-405).

- **Internal current consumption**: $20 \times 90 \text{ mA} = 1800 \text{ mA at 5 V}$
- **Residual current for bus modules**: $10 \times 2 \text{ mA} = 20 \text{ mA at 5 V}$

**Sum**: 1820 mA at 5 V

The example coupler can only provide 1620 mA (see previous example) for the I/O modules. This value is given in the associated data sheet. Consequently, an internal system supply module with bus power supply (750-613), e. g. in the middle of the node, should be added.

---

Note

**Recommendation**

Utilize the **smartDESIGNER** feature WAGO ProServe® software to configure fieldbus node assembly. You can test the configuration via the integrated plausibility check.

The maximum input current of the 24 V system supply is 500 mA. The exact electrical consumption ($I_{\text{V_2}}$) can be determined with the following formulas:
**Fieldbus coupler or controller**

\[ I_{(5 \text{ V}) \text{ total}} = \text{Sum of all the internal current consumption of the}\]
\[ \text{connected I/O modules + internal current consumption of}\]
\[ \text{the fieldbus coupler/controller}\]

**Internal system supply module**

\[ I_{(5 \text{ V}) \text{ total}} = \text{Sum of all the internal current consumption of the}\]
\[ \text{connected I/O modules at internal system supply module}\]

**Input current**

\[ I_{(24 \text{ V})} = \frac{5 \text{ V}}{24 \text{ V}} \times \frac{I_{(5 \text{ V}) \text{ total}}}{\eta}\]

\[ \eta = 0.87\]

(87 % Efficiency of the power supply at nominal load 24 V)

---

**Note**

Activate all outputs when testing the current consumption!

If the electrical consumption of a power supply point for the 24 V system supply exceeds 500 mA, then the cause may be an improperly dimensioned node or a defect.

During the test, you must activate all outputs.
3.4.4 Field Supply

3.4.4.1 Connection

Sensors and actuators can be directly connected to the relevant channel of the I/O module in 1, 2, 3 or 4 conductor connection technology. The I/O module supplies power to the sensors and actuators. The input and output drivers of some I/O modules require the field side supply voltage.

The fieldbus coupler/controller provides field side power (DC 24 V). In this case it is a passive power supply without protection equipment.

Power supply modules with or without fuse holder and diagnostic capability are available for the power supply of other field potentials (24 VDC, 0 … 230 VAC/DC, 120 VAC, 230 VAC). The power supply modules can also be used to set up various potential groups. The connections are connected in pairs to a power contact.

![Diagram](image)

Figure 7: Field Supply for Standard Couplers/Controllers and Extended ECO Couplers

<table>
<thead>
<tr>
<th>Field supply</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>24 V (-15% / +20%)</td>
</tr>
<tr>
<td>2</td>
<td>0 V</td>
</tr>
<tr>
<td>3</td>
<td>Optional ground potential (functional earth)</td>
</tr>
<tr>
<td>4</td>
<td>Potential distribution to adjacent I/O modules</td>
</tr>
</tbody>
</table>

Table 7: Legend for Figure “Field Supply for Standard Couplers/Controllers and Extended ECO Couplers”
The field-side power supply is automatically derived from the power jumper contacts when snapping an I/O module.

The current load of the power contacts must not exceed 10 A on a continual basis.

By inserting an additional power supply module, the field supply via the power contacts is disrupted. From there a new power supply occurs which may also contain a new voltage potential.

---

**Note**

Re-establish the ground connection when the connection to the power jumper contacts is disrupted!

Some I/O modules have no or very few power contacts (depending on the I/O function). Due to this, the passing through of the relevant potential is disrupted. If you require a field supply via power jumper contacts for subsequent I/O modules, then you have to use a power supply module.

Note the data sheets of the I/O modules.

---

**Note**

Use a spacer module when setting up a node with different potentials!

In the case of a node setup with different potentials, e.g. the alteration from 24 VDC to 230 VAC, you should use a spacer module. The optical separation of the potentials acts as a warning to heed caution in the case of wiring and maintenance works. Thus, you can prevent the results of wiring errors.
3.4.4.2 Fusing via Power Supply Module

Internal fusing of the field supply is possible for various field voltages via an appropriate power supply module.

Table 8: Power Supply Modules

<table>
<thead>
<tr>
<th>Order No.</th>
<th>Field Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>750-601</td>
<td>24 V DC, Supply/Fuse</td>
</tr>
<tr>
<td>750-609</td>
<td>230 V AC, Supply/Fuse</td>
</tr>
<tr>
<td>750-615</td>
<td>120 V AC, Supply/Fuse</td>
</tr>
<tr>
<td>750-617</td>
<td>24 V AC, Supply/Fuse</td>
</tr>
<tr>
<td>750-610</td>
<td>24 V DC, Supply/Fuse/Diagnosis</td>
</tr>
<tr>
<td>750-611</td>
<td>230 V AC, Supply/Fuse/Diagnosis</td>
</tr>
<tr>
<td>750-606</td>
<td>Supply Module 24 V DC, 1,0 A, Ex i</td>
</tr>
<tr>
<td>750-625/000-001</td>
<td>Supply Module 24 V DC, 1,0 A, Ex i (without diagnostics)</td>
</tr>
</tbody>
</table>

Figure 8: Supply Module with Fuse Carrier (Example 750-610)

**NOTICE**

Observe the maximum power dissipation and, if required, UL requirements! In the case of power supply modules with fuse holders, you must only use fuses with a maximum dissipation of 1.6 W (IEC 127). For UL approved systems only use UL approved fuses.
In order to insert or change a fuse, or to switch off the voltage in succeeding I/O modules, the fuse holder may be pulled out. In order to do this, use a screwdriver for example, to reach into one of the slits (one on both sides) and pull out the holder.

Figure 9: Removing the Fuse Carrier

Lifting the cover to the side opens the fuse carrier.

Figure 10: Opening the Fuse Carrier

Figure 11: Changing the Fuse

After changing the fuse, the fuse carrier is pushed back into its original position.
### 3.4.4.3 Fusing external

**NOTICE**

Field supply only with appropriate fuse protection!
Without overcurrent protection, the electronics can be damaged.
For 24V field supply input voltage an external fuse, rated max. 10 A, slow acting, min. shall be used.
The 24V input voltage for the field supply is provided with an external fuse with max. 10 A slow acting, min. 30 VDC, to be secured.

For the external fusing, the fuse modules of the WAGO series 282, 2006, 281 and 2002 are suitable for this purpose.

![Figure 12: Fuse Modules for Automotive Fuses, Series 282](image)

![Figure 13: Fuse Modules for Automotive Fuses, Series 2006](image)

![Figure 14: Fuse Modules with Pivotable Fuse Carrier, Series 281](image)
Figure 15: Fuse Modules with Pivotable Fuse Carrier, Series 2002
3.4.5 Supplementary Power Supply Regulations

The WAGO-I/O-SYSTEM 750 can also be used in shipbuilding or offshore and onshore areas of work (e.g., working platforms, loading plants). This is demonstrated by complying with the standards of influential classification companies such as Germanischer Lloyd and Lloyds Register.

Filter modules for 24 V supply are required for the certified operation of the system.

Table 9: Filter Modules for 24 V Supply

<table>
<thead>
<tr>
<th>Order No.</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>750-626</td>
<td>Supply Filter</td>
<td>Filter module for system supply and field supply (24 V, 0 V), i.e., for fieldbus coupler/controller and bus power supply (750-613)</td>
</tr>
<tr>
<td>750-624</td>
<td>Supply Filter</td>
<td>Filter module for the 24 V field supply (750-602, 750-601, 750-610)</td>
</tr>
</tbody>
</table>

Therefore, the following power supply concept must be absolutely complied with.

Figure 16: Power Supply Concept

**Note**

Use a supply module for equipotential bonding!

Use an additional 750-601/602/610 Supply Module behind the 750-626 Filter Module if you want to use the lower power jumper contact for equipotential bonding, e.g., between shielded connections and require an additional tap for this potential.
3.4.6 Supply Example

**Note**

The system supply and the field supply shall be separated!
You should separate the system supply and the field supply in order to ensure bus operation in the event of a short-circuit on the actuator side.

Figure 17: Supply Example for Standard Couplers/Controllers
Table 10: Legend for Figure “Supply Example for Fieldbus Coupler/Controller”

<table>
<thead>
<tr>
<th>Pos.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power Supply on fieldbus coupler/controller via external Supply Module</td>
</tr>
<tr>
<td>2</td>
<td>Power Supply with optional ground</td>
</tr>
<tr>
<td>3</td>
<td>Internal System Supply Module</td>
</tr>
<tr>
<td>4</td>
<td>Separation Module recommended</td>
</tr>
<tr>
<td>5</td>
<td>Supply Module passive</td>
</tr>
<tr>
<td>6</td>
<td>Supply Module with fuse carrier/diagnostics</td>
</tr>
</tbody>
</table>
3.4.7 Power Supply Unit

The WAGO-I/O-SYSTEM 750 requires a 24 VDC voltage (system supply).

### Note

#### Recommendation

A stable power supply cannot always be assumed everywhere. Therefore, you should use regulated power supplies to ensure the quality of the supply voltage.

### Note

#### Buffer for system power supply!

The system power supply must be buffered to bridge power outages. As the power demand depends on the respective node configuration, buffering is not implemented internally.

To achieve power outages of 1 ms to 10 ms according to IEC61131-2, determine the buffering appropriate for your node configuration and structure it as an external circuit.

The power demand must be determined individually depending on the entry point of the field supply. All loads through field devices and I/O modules must be taken into account. The field supply also impacts the I/O modules because the input and output drivers of some I/O modules require the voltage of the field supply.

### Note

#### System and field supply must be isolated!

The system supply and field supply must be isolated to ensure bus operation in the event of short circuits on the actuator side.

### Information

#### Power supply units are available in the eShop.

You can find suitable power supply units, e.g. from the EPSITRON series, in the eShop on [www.wago.com](http://www.wago.com).
3.5  Grounding

3.5.1  Grounding the DIN Rail

3.5.1.1  Framework Assembly

When setting up the framework, the carrier rail must be screwed together with the electrically conducting cabinet or housing frame. The framework or the housing must be grounded. The electrical connection is established via the screw. Thus, the carrier rail is grounded.

⚠️ DANGER ⚠️

Ensure sufficient grounding is provided!
You must take care to ensure the flawless electrical connection between the carrier rail and the frame or housing in order to guarantee sufficient grounding.

3.5.1.2  Insulated Assembly

Insulated assembly has been achieved when there is constructively no direct ohmic contact between the cabinet frame or machine parts and the carrier rail. Here, the earth ground must be set up via an electrical conductor in accordance with valid national safety regulations.

>Note

Recommendation
The optimal setup is a metallic assembly plate with grounding connection which is electrically conductive linked to the carrier rail.

The separate grounding of the carrier rail can be easily set up with the aid of the WAGO ground wire terminals.

Table 11: WAGO Ground Wire Terminals

<table>
<thead>
<tr>
<th>Order No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>283-609</td>
<td>1-conductor ground (earth) terminal block make an automatic contact to the carrier rail; conductor cross section: 0.2 mm² … 16 mm²</td>
</tr>
<tr>
<td></td>
<td>Note: Also order the end and intermediate plate (283-320).</td>
</tr>
</tbody>
</table>
3.5.2 Grounding Function

The grounding function increases the resistance against electro-magnetic interferences. Some components in the I/O system have a carrier rail contact that dissipates electro-magnetic interferences to the carrier rail.

![DIN rail contact](Figure 18: Carrier Rail Contact (Example))

**DANGER**

Ensure sufficient grounding is provided!
You must take care to ensure the direct electrical connection between the carrier rail contact and the carrier rail.
The carrier rail must be grounded.
For information on carrier rail properties, see section “Mounting” > … > “Carrier Rail Properties”.

The bottom CAGE CLAMP® connectors of the supply modules enable optional connection of a field-side functional ground. This potential is made available to the I/O module arranged on the right through the spring-loaded contact of the three power contacts. Some I/O modules are equipped with a knife-edge contact that taps this potential. This forms a potential group with regard to functional ground with the I/O module arranged on the left.
3.6 Shielding

3.6.1 General

Use of shielded cables reduces electromagnetic interference and thus increases signal quality. Measurement errors, data transmission errors and interference due to excessive voltage can be prevented.

---

**Note**

Connect the cable shield to the ground potential!

Integrated shielding is mandatory to meet the technical specifications in regards to measuring accuracy. Connect the cable shield and ground potential at the inlet to the cabinet or housing. This allows induced interference to dissipate and to be kept away from devices in the cabinet or housing.

![Figure 19: Cable Shield at Ground Potential](image)

---

**Note**

Improve shielding performance by placing the shield over a large area!

Higher shielding performance is achieved via low-impedance connection between shield and ground. For this purpose, connect the shield over a large surface area, e.g., WAGO shield connecting system. This is especially recommended for large-scale systems where equalizing current or high impulse-type currents caused by atmospheric discharge may occur.

---

**Note**

Keep data and signal lines away from sources of interference!

Route data and signal lines separately from all high voltage cables and other sources of high electromagnetic emission (e.g., frequency converter or drives).

---

3.6.2 Fieldbus Cables

The shielding of fieldbus lines is described in the respective configuration guidelines and standards of the fieldbus system. Information on this can be provided by the corresponding fieldbus organization or specialist literature.
3.6.3 Shielded Signal Lines

**Note**

Use shielded signal lines!
Always use shielded signal lines for analog signals and I/O modules which are equipped with shield clamps. Only then you can ensure that the accuracy and interference immunity specified for the respective I/O module can be achieved even in the presence of interference acting on the signal cable.

On some WAGO devices you can directly clamp the shield. For all other devices use the WAGO shield connecting system.

3.6.4 WAGO Shield Connecting System

The series 790 WAGO shield connecting system consists of shield clamping saddles, busbars and various mounting carriers. These components can be used to achieve many different configurations.

![Figure 20: Examples of the WAGO Shield Connecting System](image)

![Figure 21: Application of the WAGO Shield Connecting System](image)
4 Device Description

The FC BACnet/IP; G4 750-332 is the head station of the fieldbus node assembly and connects the WAGO I/O-SYSTEM 750 to the BACnet/IP fieldbus system.

The fieldbus coupler complies with the BACnet device profile "BACnet Building Controller" B-BC in accordance with DIN EN ISO 16484-5 and has 2 functions available internally:

1. **Native Server:** For each channel, appropriate BACnet objects are generated automatically for the digital, analog input and output modules that are connected to the coupler.

2. **BACnet-Client:** Using the client functionality, objects and their properties can be accessed by other BACnet devices.

The FC BACnet/IP; G4 can be used for applications in building automation.

Two RJ-45 ports and the integrated switch make possible the fieldbus to be wired in a line topology and allow access to BACnet/IP networks. This eliminates additional network devices, such as switches or hubs.

With the DIP switch the last byte of the IP address, as well as the assignment of the IP address (DHCP, BootP, firm setting) can be given.

In the head station, all input signals from the sensors are combined. After connecting the head station, the head station determines which I/O modules are on the node and creates a local process image from theirs data. Analog and specialty module data is sent via words and/or bytes; digital data is grouped bit-by-bit.

**Note!** The FC BACnet/IP; G4 750-332 does not support any function, system or special modules!

All sensor input signals are grouped in the coupler (slave) and transferred to the higher-order controller (master) via the fieldbus. Process data linking is performed in the higher-order controller. The higher-order controller puts out the resulting data to the actuators via the bus and the node.

The fieldbus connection consists of two ports (RJ-45). A integrated switch, which is operated in the store and forward mode, connects those fieldbus ports with the CPU.

Both ports support:

- 10BASE-T / 100BASE-TX
- Full / Half duplex
- Autonegotiation
- Auto-MDI(X)
The MODBUS TCP protocol and the BACnet/IP protocol are implemented for exchanging process data. Both of these communication protocols can be used either simultaneously or alternately.

Write access from the fieldbus coupler to the I/O modules is set via the Web-Based Management System.

The two communication protocols can be used optional or together.

Start-up and configuration of the FC BACnet/IP; G4 is performed using the WAGO BACnet Configurator.

For the management and diagnosis of the system, the HTTP(S), SNTP and SNMP protocols are available.

For the data transfer via ETHERNET the FTP and SFTP are available.

For the assignment of the IP address in the network DHCP, “WAGO Ethernet Settings” or BootP can be used.

An internal server is available for Web-based applications.

The internal file system supports two drives, an 1GB remanent memory, and a pluggable memory card (SD card).

---

**Note**

**Memory card is not included in the scope of delivery!**

Note, the FC BACnet/IP; G4 is delivered without memory card. To use a memory card, you must order one separately. The FC BACnet/IP; G4 can also be operated without memory card expansion, the use of a memory card is optional.

---

**Note**

**Only use recommended memory cards!**

Use only the SD memory card available from WAGO (order no. 758-879/000-001) since it is suitable for industrial applications under difficult environmental conditions and for use in the FC BACnet/IP; G4. The compatibility to other storage media available in trade cannot be ensured.

HTML pages stored in the head station allow access to information about the configuration, the status and the I/O data of the fieldbus node via Web browsers. It is also possible to store individual HTML pages using the implemented file system, store custom HTML pages.
**Information**

**Additional Information about BACnet-Configurator**

The BACnet Configurator and the documentation for this can be downloaded from the website for this BACnet product under [http://www.wago.com](http://www.wago.com).
4.1 View

The view below shows the three parts of the device:

- The fieldbus connection is on the left side.
- LEDs for operation status, bus communication, error messages and diagnostics, as well as the SD card slot and service interface are in the middle area.
- The right side shows the power supply unit for the system supply and for the field supply of the attached I/O modules via power jumper contacts. LEDs show the status of the operating voltage for the system and field supply (jumper contacts).

Abbildung 22: Ansicht BACnet/IP-Koppler
### Table 12: Legend for Figure “View FC BACnet/IP; G4 750-332”

<table>
<thead>
<tr>
<th>Pos.</th>
<th>Designation</th>
<th>Meaning</th>
<th>Details see Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>LINK ACT 1, LINK ACT 2, MS/ BT, NS, I/O, USR</td>
<td>Status LEDs Fieldbus</td>
<td>&quot;Device Description&quot; &gt; &quot;Display Elements&quot;</td>
</tr>
<tr>
<td>2</td>
<td>---</td>
<td>Group marking carrier (retractable) with additional marking possibility on two miniature WSB markers</td>
<td>---</td>
</tr>
<tr>
<td>3</td>
<td>A, B or C</td>
<td>Status LED’s system/field supply</td>
<td>&quot;Device Description&quot; &gt; &quot;Display Elements&quot;</td>
</tr>
<tr>
<td>4</td>
<td>---</td>
<td>Data contacts</td>
<td>&quot;Connect Devices” &gt; “Data Contacts/Local Bus”</td>
</tr>
<tr>
<td>5</td>
<td>24 V, 0 V</td>
<td>CAGE CLAMP® connections system supply</td>
<td>&quot;Connect Devices” &gt; &quot;Connecting a conductor to the CAGE CLAMP®&quot;</td>
</tr>
<tr>
<td>6</td>
<td>+</td>
<td>CAGE CLAMP® connections field supply 24 VDC</td>
<td>&quot;Connect Devices” &gt; &quot;Connecting a Conductor to the CAGE CLAMP®&quot;</td>
</tr>
<tr>
<td>7</td>
<td>---</td>
<td>Power jumper contact 24 VDC</td>
<td>&quot;Connect Devices” &gt; “Power Contacts/Field Supply”</td>
</tr>
<tr>
<td>8</td>
<td>---</td>
<td>Unlocking lug</td>
<td>&quot;Mounting” &gt; &quot;Inserting and Removing Devices”</td>
</tr>
<tr>
<td>9</td>
<td>-</td>
<td>CAGE CLAMP® connections field supply 0 V</td>
<td>&quot;Connect Devices” &gt; &quot;Connecting a Conductor to the CAGE CLAMP®”</td>
</tr>
<tr>
<td>10</td>
<td>---</td>
<td>Power jumper contact 0 V</td>
<td>&quot;Connect Devices” &gt; “Power Contacts/Field Supply”</td>
</tr>
<tr>
<td>11</td>
<td>(Ground)</td>
<td>CAGE CLAMP® connections field supply (ground)</td>
<td>&quot;Connect Devices” &gt; &quot;Connecting a Conductor to the CAGE CLAMP®”</td>
</tr>
<tr>
<td>12</td>
<td>---</td>
<td>Power jumper contact (ground)</td>
<td>&quot;Connect Devices” &gt; “Power Contacts/Field Supply”</td>
</tr>
<tr>
<td>13</td>
<td>---</td>
<td>Service interface (open flap)</td>
<td>&quot;Device Description” &gt; “Operating Elements”</td>
</tr>
<tr>
<td>14</td>
<td>X1, X2</td>
<td>Fieldbus connection 2 x RJ-45 as 2-Port Switch</td>
<td>&quot;Device Description” &gt; “Connectors”</td>
</tr>
<tr>
<td>15</td>
<td>---</td>
<td>SD card slot with cover lid</td>
<td>&quot;Device Description” &gt; “Operating Elements”</td>
</tr>
<tr>
<td>16</td>
<td>---</td>
<td>Locking Disc</td>
<td>&quot;Mounting” &gt; &quot;Inserting and Removing Devices”</td>
</tr>
<tr>
<td>17</td>
<td>---</td>
<td>Address Selection Switch</td>
<td>&quot;Device Description” &gt; “Operating Elements”</td>
</tr>
</tbody>
</table>
4.2 Connectors

4.2.1 Device Supply

The device is powered via terminal blocks with CAGE CLAMP® connections.

The device supply generates the necessary voltage to power the electronics of the device and the internal electronics of the connected I/O modules.

The fieldbus interface is galvanically separated to the electrical potential of the device.

Figure 23: Device Supply
4.2.2 Fieldbus Connection

The connection to the fieldbus is made via two RJ-45 plugs, which are connected to the fieldbus controller via an integrated switch. The integrated switch works in store-and-forward operation and for each port, supports the transmission speeds 10/100 Mbit as well as the transmission modes full and half-duplex and autonegotiation. The wiring of these plugs corresponds to the specifications for 100BaseTX, which prescribes a category 5 twisted pair cable as the connecting cable. Cable types S/UTP (Screened Unshielded Twisted Pair) and STP (Shielded Twisted Pair) with a maximum segment length of 100 m (approximately 328.08 feet) can be used. The socket is arranged physically lower, allowing the coupler to fit in an 80 mm high enclosure after plug connection.

Figure 24: RJ-45 Connector

<table>
<thead>
<tr>
<th>Contact</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TD +</td>
</tr>
<tr>
<td>2</td>
<td>TD −</td>
</tr>
<tr>
<td>3</td>
<td>RD +</td>
</tr>
<tr>
<td>4</td>
<td>free</td>
</tr>
<tr>
<td>5</td>
<td>free</td>
</tr>
<tr>
<td>6</td>
<td>RD −</td>
</tr>
<tr>
<td>7</td>
<td>free</td>
</tr>
<tr>
<td>8</td>
<td>free</td>
</tr>
</tbody>
</table>

Table 13: RJ-45 Connector and RJ-45 Connector Configuration

NOTICE

Do not use in telecommunication circuits!
Only use devices equipped with ETHERNET or RJ-45 connectors in LANs.
Never connect these devices with telecommunication networks.
4.3 Display Elements

The operating condition of the fieldbus coupler or the node is displayed with the help of illuminated indicators in the form of light-emitting diodes (LEDs). The LED information is routed to the top of the case by light guides. In some cases, the LEDs are multi-colored (red, green or orange).

Figure 25: Display Elements

For the diagnostics of the different domains fieldbus, node and supply voltage, the LEDs can be divided into three groups:

Table 14: Display Elements Fieldbus Status

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>LNK ACT 1</td>
<td>green</td>
<td>indicates a connection to the physical network at port 1</td>
</tr>
<tr>
<td>LNK ACT 2</td>
<td>green</td>
<td>indicates a connection to the physical network at port 2</td>
</tr>
<tr>
<td>MS/BT</td>
<td>green/ green blinking/ red/ red blinking</td>
<td>indicates the node or BACnet status</td>
</tr>
<tr>
<td>NS</td>
<td>red/green</td>
<td>indicates the network status</td>
</tr>
</tbody>
</table>

Table 15: Display Elements Node Status

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>I/O</td>
<td>red/green/orange</td>
<td>Indicates the operation of the node and signals via a blink code faults encountered.</td>
</tr>
<tr>
<td>SD</td>
<td>orange</td>
<td>indicates an access to the SD memory card</td>
</tr>
</tbody>
</table>

Table 16: Display Elements Supply Voltage

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>green</td>
<td>indicates the status of the operating voltage – system</td>
</tr>
<tr>
<td>B</td>
<td>green</td>
<td>indicates the status of the operating voltage – power jumper contacts</td>
</tr>
</tbody>
</table>

Information

More information about the LED Signaling
Read the detailed description for the evaluation of the displayed LED state in the section “Diagnostics” > … > “LED Signaling”.
4.4 Operating Elements

4.4.1 Service Interface

The service interface is located behind the flap.

It is used for the communication with the WAGO I/O-CHECK and WAGO Ethernet Settings.

![Service Interface (Closed and Opened Flap)](image)

Figure 26: Service Interface (Closed and Opened Flap)

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open closed</td>
</tr>
<tr>
<td>2</td>
<td>View Service Interface</td>
</tr>
</tbody>
</table>

Table 17: Legend for Figure “Service Interface (Closed and Opened Flap)”

---

**NOTICE**

Device must be de-energized!

To prevent damage to the device, unplug and plug in the communication cable only when the device is de-energized!

---

The connection to the 4-pin header under the cover flap can be realized via the communication cables with the item numbers 750-920 and 750-923 or via the WAGO radio adapter with the item number 750-921.
4.4.2 Mode Selector Switch

The mode selector switch is located behind the cover flap.

![Diagram of Mode Selector Switch](image)

Figure 27: Mode Selector Switch (Closed and Open Damper of the Service Port)

Table 18: Legend for Figure „Mode Selector Switch“

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open the damper</td>
</tr>
<tr>
<td>2</td>
<td>Mode selector switch</td>
</tr>
</tbody>
</table>

A hardware reset is performed when the mode selector switch is pressed down (e.g., with a screwdriver). All outputs are reset. The fieldbus coupler restarts. The switch position is irrelevant for fieldbus couplers. A hardware reset can be performed at any position of the mode selector switch.
4.4.3 Address Selection Switch

The 8-pole DIP switch is used to set the IP address and to select the protocol for setting the IP address.

The IP address is composed of a network component and a host component.

The network component is configurable and in delivery status 192.168.1.
The host component is set via the DIP switch.

The individual DIP switches 1 to 8 represent a bit mask corresponding to the values 0 to 255. Switch 1 corresponds to the lowest bit ($2^0$) and switch 8 corresponds to the highest bit ($2^7$).

Table 19: Meaning of DIP Switch Positions

<table>
<thead>
<tr>
<th>Host Component of the IP Address</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (WBM)</td>
<td>The IP configuration set in the WBM on the &quot;Port&quot; page is used (default DHCP, but can be changed to BootP or EEPROM).</td>
</tr>
<tr>
<td>1 … 254</td>
<td>Host component by switch position Example of setting the DIP switch: For the IP address 192.168.1.33, the 1st and 6th switches must be set: $2^0$ (1st switch) + $2^5$ (6th switch) = 33</td>
</tr>
<tr>
<td>255 (DHCP)</td>
<td>The DHCP protocol is used to configure the IP parameters.</td>
</tr>
</tbody>
</table>
4.4.4 Memory Card Slot

The memory card slot accommodates a secure digital memory card (or SD card for short) or an SD card with a higher storage capacity (SD high capacity, or SDHC for short).

**Note**
Only use recommended memory cards!
Use only the SD memory card available from WAGO (order no. 758-879/000-001) since it is suitable for industrial applications under difficult environmental conditions and for use in the fieldbus coupler. The compatibility to other storage media available in trade cannot be ensured.

The memory card slot has a transparent protective flap that is folded upwards to open it.

**Note**
Memory card is not included in the scope of delivery!
Note, the fieldbus coupler is delivered without memory card. To use a memory card, you must order one separately. The fieldbus coupler can also be operated without memory card expansion, the use of a memory card is optional.

**Information**
Additional information about the memory card
For technical information about the memory card, see the data sheet for the SD memory card (order no. 758-879/000-001). The data sheet is on the Internet at: [www.wago.com](http://www.wago.com)

![Figure 29: Opening the Memory Card Slot, Inserting an SD/SDHC Memory Card](image)
4.4.4.1 Inserting a Memory Card

1. Use an activation tool or a screwdriver to open the transparent cover flap by folding it upwards.

2. Hold the memory card so that the contacts are visible on the right side and the sloping edge is towards the bottom, as depicted in the figure above.

3. Insert the memory card into the slot of the fieldbus coupler.

4. Push the memory card all the way in. When you let go, the memory card will move back a little and then snap in.

5. Push the cover flap back in by folding it downwards until it snaps in.

4.4.4.2 Removing the Memory Card

1. Use an activation tool or a screwdriver to open the transparent cover flap by folding it upwards.

2. To remove the memory card, first press it into the slot. This loosens the mechanical locking.

3. As soon as you let go of the memory card, the memory card is pushed out a bit and you can remove it.

4. Push the cover flap back in by folding it downwards until it snaps in.
4.5 Technical Data

4.5.1 Device Data

Table 20: Technical Data - Device

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Width</td>
<td>62 mm</td>
</tr>
<tr>
<td>High (from upper edge of DIN 35 rail)</td>
<td>65* mm (*from upper edge of DIN 35 rail)</td>
</tr>
<tr>
<td>Length</td>
<td>100 mm</td>
</tr>
<tr>
<td>Weight</td>
<td>152 g</td>
</tr>
</tbody>
</table>

4.5.2 System Data

Table 21: Technical Data - System

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of fieldbus nodes per master</td>
<td>Limited by ETHERNET specification</td>
</tr>
<tr>
<td>Transmission medium</td>
<td>Twisted Pair CAT 5e (S/UTP)</td>
</tr>
<tr>
<td>Fieldbus coupler connection</td>
<td>2 x RJ-45</td>
</tr>
<tr>
<td>Max. cable length</td>
<td>100 m</td>
</tr>
<tr>
<td>Max. network length</td>
<td>2000 m</td>
</tr>
<tr>
<td>Baud rate</td>
<td>10/100 Mbit/s</td>
</tr>
<tr>
<td>Transmission performance</td>
<td>Class D acc. to EN 50173</td>
</tr>
<tr>
<td>Communication</td>
<td>BACnet/IP, Modbus (TCP, UDP)</td>
</tr>
<tr>
<td>Ethernet Protocols</td>
<td>HTTP, HTTPS, BootP, DHCP, DNS, (S)FTP, SNMP</td>
</tr>
<tr>
<td>SD memory card slot</td>
<td>push/push mechanism, cover cap lead-sealable</td>
</tr>
<tr>
<td>Memory card type</td>
<td>SD and SDHC up to 32 Gbyte *)</td>
</tr>
<tr>
<td>Number of I/O modules</td>
<td>64</td>
</tr>
<tr>
<td>- with bus extension</td>
<td>250</td>
</tr>
<tr>
<td>Configuration</td>
<td>WAGO-I/O-CHECK, Web-Based-Management, WAGO BACnet Konfigurator</td>
</tr>
<tr>
<td>Internal file system</td>
<td>1 GB</td>
</tr>
</tbody>
</table>

*) Use only the SD memory card available from WAGO (order no. 758-879/000-001) since it is suitable for industrial applications under difficult environmental conditions and for use in the fieldbus controller. The compatibility to other storage media available in trade cannot be ensured.
4.5.3 Supply

Table 4: Technical Data - Supply

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voltage supply system</td>
<td>24 V DC (-25 % ... +30 %)</td>
</tr>
<tr>
<td>Typ. input current at 24 V</td>
<td>500 mA</td>
</tr>
<tr>
<td>Power failure time acc. IEC 61131-2</td>
<td>Depending on external buffering</td>
</tr>
<tr>
<td>Efficiency of the power supply</td>
<td>90 %</td>
</tr>
<tr>
<td>Internal current consumption at 5 V</td>
<td>440 mA</td>
</tr>
<tr>
<td>Total current for I/O modules at 5 V</td>
<td>1700 mA</td>
</tr>
<tr>
<td>Overvoltage category</td>
<td>II</td>
</tr>
<tr>
<td>Isolation</td>
<td>500 V system/supply</td>
</tr>
<tr>
<td>Voltage supply field</td>
<td>DC 24 V (-25 % ... +30 %); incoming via wiring level (CAGE CLAMP® connection); 24 VDC; outgoing via power jumper contacts</td>
</tr>
<tr>
<td>Number of outgoing power jumper contacts</td>
<td>3</td>
</tr>
<tr>
<td>Current carrying capacity (power jumper contacts)</td>
<td>10 A DC</td>
</tr>
</tbody>
</table>

**Note**

Buffer for system power supply!
The system power supply must be buffered to bridge power outages. As the power demand depends on the respective node configuration, buffering is not implemented internally.
To achieve power outages of 1 ms to 10 ms according to IEC61131-2, determine the buffering appropriate for your node configuration and structure it as an external circuit.

4.5.4 Fieldbus BACnet/IP

Table 5: Technical Data - Fieldbus BACnet/IP

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Process Image (\text{max})</td>
<td>1020 words</td>
</tr>
<tr>
<td>Output Process Image (\text{max})</td>
<td>1020 words</td>
</tr>
<tr>
<td>BACnet Implementation acc.</td>
<td>ISO 16484-5:2010</td>
</tr>
<tr>
<td>BACnet Protocol Revision 12</td>
<td>BACnet Protocol Revision 12</td>
</tr>
<tr>
<td>BACnet Device Profile</td>
<td>BACnet-Building-Controller (B-BC)</td>
</tr>
</tbody>
</table>
### 4.5.5 Accessories

Table 22: Technical data – Accessories

| Miniature WSB Quick marking system | 248-501 |
| SD Memory Card                  | 758-879/000-001 |

### 4.5.6 Connection Type

Table 23: Technical Data – Field Wiring

<table>
<thead>
<tr>
<th>Wire connection</th>
<th>CAGE CLAMP®</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross section, solid wire</td>
<td>0.08 mm² … 2.5 mm² / AWG 28 … 14</td>
</tr>
<tr>
<td>Cross section, fine-stranded wire</td>
<td>0.25 mm² … 2.5 mm² / AWG 28 … 12</td>
</tr>
<tr>
<td>Stripped lengths</td>
<td>8 mm … 9 mm / 0.33 in</td>
</tr>
</tbody>
</table>

Table 24: Technical Data – Data Contacts

<table>
<thead>
<tr>
<th>Data contacts</th>
<th>Slide contact, hard gold plated, self-cleaning</th>
</tr>
</thead>
</table>
### 4.5.7 Climatic Environmental Conditions

Table 25: Technical Data – Climatic Environmental Conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surrounding air temperature, operation</td>
<td>0 °C … 55 °C</td>
</tr>
<tr>
<td>Surrounding air temperature, storage</td>
<td>−25 °C … +85 °C</td>
</tr>
<tr>
<td>Operating altitude</td>
<td>0 … 2000 m</td>
</tr>
<tr>
<td>Relative humidity</td>
<td>Max. 5 % … 95 % without condensation</td>
</tr>
<tr>
<td>Pollution degree</td>
<td>2</td>
</tr>
<tr>
<td>Protection type</td>
<td>IP20</td>
</tr>
<tr>
<td>Resistance to harmful substances</td>
<td>Acc. to IEC 60068-2-42 and IEC 60068-2-43</td>
</tr>
</tbody>
</table>
| Maximum pollutant concentration at relative humidity < 75 % | SO$_2$ ≤ 25 ppm  
          | H$_2$S ≤ 10 ppm                      |
| Special conditions                            | • Ensure that additional measures for components are taken, which are used in an environment involving: – dust, caustic vapors or gases – ionizing radiation  
          | • Ensure that the permissible temperature range of the connecting cable is correct dimensioned depending on the installation position and current intensity, because the clamping point temperature at 10 A can be up to 25 °C above the expected surrounding air temperature. |
4.5.8 Mechanical Strength

Table 26: Technical Data – Mechanical Strength

<table>
<thead>
<tr>
<th></th>
<th>Vibration resistance</th>
<th>Shock resistance</th>
<th>Free fall</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Acc. to IEC 60068-2-6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment to the vibration resistance:</td>
<td></td>
<td>Acc. to IEC 60068-2-27</td>
<td>Acc. IEC 60068-2-32</td>
</tr>
<tr>
<td>a) Type of oscillation:</td>
<td></td>
<td></td>
<td>( \leq 1 ) m  (module in original packing)</td>
</tr>
<tr>
<td>sweep with a rate of change of 1 octave per minute</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 Hz ( \leq f &lt; 57 ) Hz, const. Amplitude 0.075 mm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>57 Hz ( \leq f &lt; 150 ) Hz, const. Acceleration 1 g</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Period of oscillation:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 sweep per axis in each of the 3 vertical axes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) Type of impulse: half sinusoidal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Intensity of impulse:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 g peak value, 11 ms maintenance time</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c) Route of impulse:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 impulses in each pos. And neg. direction of the 3 vertical axes of the test object, this means 18 impulses in all.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.5.9 Software Compatibility

Table 27: Technical Data – Software Compatibility

<table>
<thead>
<tr>
<th>Software</th>
<th>Version Number</th>
<th>Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAGO-I/O-CHECK</td>
<td>(759-302)</td>
<td>starting from version 3.20.01(01)</td>
</tr>
<tr>
<td>WAGO Ethernet Settings</td>
<td>(759-316)</td>
<td>starting from version 6.10.04.10</td>
</tr>
<tr>
<td>WAGOupload</td>
<td>(<a href="http://www.wago.com">www.wago.com</a>)</td>
<td>starting from version 1.10.0.0</td>
</tr>
<tr>
<td>WAGO BACnet Configurator</td>
<td>(759-321)</td>
<td>starting from version 1.12.0.0</td>
</tr>
</tbody>
</table>
4.6 Approvals

**Information**

More information about approvals.
Detailed references to the approvals are listed in the document “Overview Approvals WAGO I/O SYSTEM 750”, which you can find via the internet under: www.wago.com → DOWNLOADS → Documentation → System Description.

The following approvals have been granted to 750-332 fieldbus coupler:

- Conformity Marking

The following BACnet approvals have been granted to the respective software versions (SW):

<table>
<thead>
<tr>
<th>BACnet Approvals</th>
<th>750-332</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACnet conformance test acc. ISO 16484-5:2012</td>
<td>Passed SW 01.01.20(02)</td>
</tr>
<tr>
<td>BTL Certification</td>
<td>Passed SW 01.01.20(02)</td>
</tr>
<tr>
<td>AMEV attestation</td>
<td>Passed SW 01.01.20(02)</td>
</tr>
<tr>
<td>AMEV Profile AS-B</td>
<td>Passed SW 01.01.20(02)</td>
</tr>
</tbody>
</table>

* Status as of 8/2019
4.7 Standards and Guidelines

750-332 meets the following requirements on emission and immunity of interference:

EMC CE-Immunity to interference EN 61000-6-2
EMC CE-Emission of interference EN 61000-6-3
4.8 BACnet-Building-Controller (B-BC)

The 750-332 WAGO FC BACnet/IP; G4 represents the device profile of the BACnet Building Controllers (B-BC). As such, the fieldbus coupler serves as an automation system that can take over a multitude of different building automation and control tasks.

The BACnet Standard 135-2012 describes six BACnet device profiles. Any device that implements all the required BACnet capabilities for a particular device type and interoperability area may claim to be a device of that particular device profile. Devices may also provide additional capabilities. All supported capabilities of the fieldbus coupler must be indicated in the protocol implementation confirmation (PICS). This is a document that represents and compares the capabilities of the device.

Information

Additional Information
You can download the appropriate PICS document on the product page of your fieldbus coupler at: www.wago.com.

As a B-BC the fieldbus coupler „FC BACnet/IP; G4“ (750-332) supports the following parameters:

Data Sharing

- Ability to provide the values of any of its BACnet objects
- Ability to retrieve the values of BACnet objects from other devices
- Ability to allow modification of some or all of its BACnet objects by another device
- Ability to modify some BACnet objects in other devices

Alarm and Event Management

- Generation of alarm/event notifications and the ability to direct them to recipients
- Maintain a list of unacknowledged alarms/events
- Notifying other recipients that the acknowledgment has been received
- Adjustment of alarm and event parameters, scheduling
- Ability to schedule output actions, both in the local device and in other devices, both binary and analog, based on date and time

Trending

- Collection and delivery of (time, value) pairs
Device und Network Management

- Ability to respond to queries about its status
- Ability to respond to requests for information about any of its objects
- Ability to respond to communication control messages
- Ability to synchronize its internal clock upon request
- Ability to perform re-initialization upon request
- Ability to upload its configuration and allow it to be subsequently restored

4.8.1 BIBBs (BACnet Interoperability Building Blocks)

The following table shows the minimum requirement of the BACnet features ("BACnet Interoperability Building Blocks" - BIBBs) for the B-BC in general and the additionally implemented BIBBs in the fieldbus coupler FC BACnet/IP; G4.
### Table 29: BIBBs of the B-BC

<table>
<thead>
<tr>
<th>IOB</th>
<th>BIBBs of the B-BC&lt;sup&gt;1&lt;/sup&gt; (Minimum requirements)</th>
<th>Additional BIBBs of the FC BACnet/IP; G4&lt;sup&gt;2&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling</td>
<td>SCHED-E-B</td>
<td>SCHED-I-B</td>
</tr>
</tbody>
</table>

<sup>1</sup> As of BACnet Standard 135-2012

<sup>2</sup> As of 08/2019 (For currently supported BIBBs of the FC BACnet/IP; G4, please refer to the “PICS” document at [http://www.wago.com](http://www.wago.com) in the Documentation area.)
Data Sharing BIBBs

These BIBBs prescribe the BACnet capabilities required to interoperably perform the data sharing functions.

Data Sharing - ReadProperty-A (DS-RP-A)

The A device is a user of data from device B.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReadProperty</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Data Sharing - ReadProperty-B (DS-RP-B)

The B device is a provider of data to device A.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReadProperty</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Data Sharing-ReadPropertyMultiple-A (DS-RPM-A)

The A device is a user of data from device B and requests multiple values at one time.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReadPropertyMultiple</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Data Sharing-ReadPropertyMultiple-B (DS-RPM-B)

The B device is a provider of data to device A and returns multiple values at one time.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReadPropertyMultiple</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Data Sharing-WriteProperty-A (DS-WP-A)

The A device sets a value in device B.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>WriteProperty</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
**Data Sharing-WriteProperty-B (DS-WP-B)**

The B device allows a value to be changed by device A.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>WriteProperty</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

**Data Sharing-WritePropertyMultiple-B (DS-WPM-B)**

The B device allows multiple values to be changed by device A at one time.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>WritePropertyMultiple</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

**BIBB - Data Sharing-COV-A (DS-COV-A)**

Device A is a user of the COV data from device B.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>SubscribeCOV</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>ConfirmedCOVNotification</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>UnconfirmedCOVNotification</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

The support of subscriptions with limited lifetime is necessary; the support of subscriptions with unlimited lifetime is optional.

**Data Sharing-COV-B (DS-COV-B)**

Device B is a provider of COV data for device A.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>SubscribeCOV</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>ConfirmedCOVNotification</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>UnconfirmedCOVNotification</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Devices that comply with DS-COV-B must support at least five simultaneous subscriptions. The support of subscriptions with a limited lifetime is necessary; the support of subscriptions with an unlimited lifetime is optional.
Data Sharing- COVP-B (DS-COVP-B)

Device B is a provider of COV data for device A.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>SubscribeCOVProperty</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>ConfirmedCOVNotification</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>UnconfirmedCOVNotification</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Devices that comply with DS-COV-B must support at least five simultaneous subscriptions. The support of subscriptions with a limited lifetime is necessary; the support of subscriptions with an unlimited lifetime is optional.

4.8.3 Alarm and Event Management BIBBs

These BIBBs prescribe the BACnet capabilities required to interoperably perform the alarm and event management functions.

Alarm and Event-Notification Internal-B (AE-N-I-B)

Device B generates notifications about alarms and other events.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConfirmedEventNotification</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>UnconfirmedEventNotification</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Devices claiming conformance to AE-N-I-B must also support either Intrinsic or Algorithmic reporting. Any device that supports the generation of event notifications that require operator acknowledgment must support AE-ACK-B.

Alarm and Event-Notification External-B (AE-N-E-B)

Device B contains an Event Enrollment object that monitors values in another device. Device B is capable of generating event notifications for alarm conditions based on value(s) in another device. Devices confirming to the BIBB shall confirm to DS-RP-A, AE-N-I-B, and shall support at least 1 Event Enrollment object. With an Object_Property_Reference property that supports references to properties in objects contained in other devices. Any devices that supports the generation of event notifications that require operator acknowledgment shall support AE-ACK-B and AE-INFO-B. Any devices that supports the generation of TO-FAULT or TO-OFFNORMAL event notifications shall support AE-INFO-B.

Devices that only support Event Enrollment objects that only support generation of CHANGE_OF_LIFE_SAFETY and/or BUFFER_READY notifications shall not claim support for this BiBB.
Alarm and Event-ACK-B (AE-ACK-B)

Device B processes acknowledgments of previously transmitted alarm/event notifications.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>AcknowledgeAlarm</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

To support this BIBB the device must also support acknowledgeable alarms.

Alarm and Event-Information-B (AE/INFO-B)

Device B provides event information to device A.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetEventInformation</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Alarm and Event-Alarm Summary-B (AE-ASUM-B)

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetAlarmSummary</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Device B provides summaries of alarms to device A.

Alarm and Event-Enrollment Summary-B (AE-ESUM-B)

Device B provides event enrollments to device A.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetEnrollmentSummary</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Alarm and Event Management-Event Log Internal-B (AE-EL-I-B)

Device B collects the event notifications in an internal buffer. Each device claiming conformance to AE-EL-I-B must be able to support at least one Event Log object.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReadRange</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
4.8.4 Scheduling BIBBs

These BIBBs prescribe the BACnet capabilities required to interoperably perform the scheduling functions.

Scheduling-Internal-B (SCHED-I-B)

Device B indicates time and data for the scheduling of values of a certain property of certain objects of the device. Each SCHED-I-B compliant device also has at least one Calendar and Schedule Object for the support of the BIBBs DS-RP-B and DS-WP-B. SCHED-I-B compliant devices must also support DM-TS-B and DM-UTC-B.

The Schedule Object must support at least six entries per day. The property List_Of_Object_Property_Reference must support at least one entry. The Schedule Object must support a non-empty property Exception_Schedule. The property Priority_For_Writing of the Schedule Object must be writable.

Scheduling-External-B (SCHED-E-B)

The B device provides date and time scheduling of the values of specific properties of specific objects in other devices. Devices claiming conformance to SCHED-E-B shall also support SCHED-I-B and DS-WP-A. The List_Of_Object_Property_References property shall support references to objects in external devices.

4.8.5 Trending BIBBs

These BIBBs prescribe the BACnet capabilities required to interoperably perform the trend value processing.

Trending-Viewing and Modifying Trends Internal-B (T-VMT-I-B)

The B device collects the trend log data records in an internal buffer. Each device-claiming conformance to T-VMT-I-B must be able to support at least one Trend Log object.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReadRange</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Trending-Automated Trend Retrieval-B (T-ATR-B)

The B device notifies the A device that a trending buffer has acquired a predetermined number of data samples using the BUFFER_READY event algorithm either intrinsically in the Trend Log object or algorithmically using an Event Enrollment object.
T-ATR-B compliant devices must support the Trend Log Object.

**Trending-Viewing and Modifying Trends External-B (T-VMT-E-B)**

The B device is capable of trending properties of objects contained in other devices. The B device shall support T-VMT-I-B and DS-RP-A. The Log_Interval and Log_DeviceObjectProperty properties must be writable.

The Trend Log objects must be capable of trending REAL, Unsigned, INTEGER, BOOLEAN, Bit String, Enumerated and NULL values.

**Trending-Viewing and Modifying Multiple Values Internal-B (T-VMMV-I-B)**

The device B collects the multiple-data log records in an internal buffer. Each device claiming conformance to T-VMMV-I-B shall be able to support at least one Trend Log Multiple object.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReadRange</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

**Trending-Viewing and Modifying Multiple Values External-B (T-VMMV-E-B)**

The B device is capable of logging multiple properties of multiple objects contained in other devices. The B device shall support T-VMMV-I-B and DS-RPMA. The Log_Interval and Log_DeviceObjectProperty properties shall be writable.

**Trending-Automated Multiple Value Retrieval-B (T-AMVR-B)**

The B device notifies the A device that a Trend Log Multiple object's buffer has acquired a predetermined number of data samples using the BUFFER_READY event algorithm either intrinsically in the Trend Log Multiple object or algorithmically using an Event Enrollment object.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConfirmedEventNotification</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>UnconfirmedEventNotification</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>ReadRange</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Devices claiming conformance to T-AMVR-B shall support the Trend Log Multiple object.
4.8.6 Device- und Network-Management-BIBBs

These Device Management BIBBs prescribe the BACnet capabilities required to interoperably perform the device management functions. The network management BIBBs prescribe the BACnet capabilities required to interoperably perform network management functions.

Device Management-Dynamic Device Binding-A (DM-DDB-A)

The A device searches for information on the device properties of other devices and evaluates their notices.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who-Is</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>I-Am</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Device Management-Dynamic Device Binding-B (DM-DDB-B)

The B device provides information about its device properties and responds to requests to identify itself.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who-Is</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>I-Am</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Device Management-Dynamic Object Binding-B (DM-DOB-B)

The B device provides address information about its objects upon request.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who-Has</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>I-Have</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Device Management-DeviceCommunicationControl-B (DM-DCC-B)

The B device responds to communication control exercised by the A device.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeviceCommunicationControl</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Support for requests of a limited duration is required, and support for requests of
Device Description

an indefinite duration is optional.

Device Management-Restart-A (DM-R-A)
The A device processes restart notifications.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>UnconfirmedCOVNotification</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Device Management-Restart-B (DM-R-B)
The B device informs the A device(s) each time it restarts.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>UnconfirmedCOVNotification</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Devices claiming conformance to DM-R-B shall support the Last_Restart_Reason, Restart_Notification_Recipients, and Time_Of_Device_Restart properties of the Device object.

Device Management-TimeSynchronization-B (DM-TS-B)
The B device interprets time synchronization messages from the A device.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>TimeSynchronization</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

DM-TS-B compliant devices must support the Local_Time and Local_Date properties of the Device object.

Device Management-UTCTimeSynchronization-B (DM-UTC-B)
The B device interprets time synchronization messages from the A device.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTCTimeSynchronization</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

DM-TS-B compliant devices must support the Local_Time, Local_Date, UTC_Offset, and Daylight_Savings_Status properties of the Device object.

Device Management-ReinitializeDevice-B (DM-RD-B)
The B device performs reinitialization requests from the A device. The optional password field shall be supported.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReinitializeDevice</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Device Management-Backup and Restore-B (DM-BR-B)

The B device provides its configuration file to the A device and allows the A device to write this file to recover its configuration in the event of a failure.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>AtomicReadFile</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>AtomicWriteFile</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>ReinitializeDevice</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

DM-BR-B compliant devices must support the features of device B. Once a Restore procedure has been initiated on the device, the Read_Only property of configuration File objects shall contain the value FALSE and the File_Size property of the configuration File objects shall be writable if the size of the configuration file can change based on the device’s configuration.

If the configuration file objects are not guaranteed to exist once a Restore procedure has been initiated, then the device must support execution of the CreateObject service.

Device Management-List Manipulation-B (DM-LM-B)

The B device responds to requests to add or remove list elements.

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddListElement</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>RemoveListElement</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Device Management-Object Creation and Deletion-B (DM-OCD-B)

The B device creates and deletes object instances based on requests from the A device. The object types whose dynamic creation and deletion is supported shall be enumerated in the Standard Object Types Supported section of the device B’s PICS.
### 4.8.7 „Native“ Operation of the B-BC

When the 750-332 is switched on, not all objects supported by the system are present. However, in this still unconfigured state, the appropriate objects for the digital and analog hardware data points of all connected I/O modules are automatically created:

- Analog Input Object
- Analog Output Object
- Binary Input Object
- Binary Output Object
- Calendar Object
- Device Object
- File Object
- Schedule Object

The analog and digital input and output objects are linked to the I/O module data. No configuration or programming is required in native operation.

In native mode, the object name is formed from the object type, an underscore and the instance number. For example, instance number 2 indicates that this is the second object created.

**Example:**

An analog output object with instance number 4 is given the object name "ANALOG_OUTPUT_4".

These object names can be changed in the WAGO BACnet Configurator as required. They should be uniquely selected within a device.

---

<table>
<thead>
<tr>
<th>BACnet Service</th>
<th>Requests</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateObject</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>DeleteObject</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

---

**Note**

**Note the maximum of supported objects!**

For the 750-332 BACnet/IP fieldbus coupler a maximum amount of 256 objects can be created.
Information

Information about the objects in the PICS!
All supported objects are listed in the document of the corresponding BACnet Protocol Implementation Conformance Statement (PICS).
You can find the corresponding PICS document as a download for your product at: www.wago.com.
5 Mounting

5.1 Installation Position

Along with horizontal and vertical installation, all other installation positions are allowed.

---

**Note**

Use an end stop in the case of vertical mounting!

In the case of vertical assembly, an end stop has to be mounted as an additional safeguard against slipping.

<table>
<thead>
<tr>
<th>WAGO order no.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>249-116</td>
<td>End stop for DIN 35 rail, 6 mm wide</td>
</tr>
<tr>
<td>249-117</td>
<td>End stop for DIN 35 rail, 10 mm wide</td>
</tr>
</tbody>
</table>

---

5.2 Overall Configuration

The maximum total length of a fieldbus node without fieldbus coupler/controller is 780 mm including end module. The width of the end module is 12 mm. When assembled, the I/O modules have a maximum length of 768 mm.

**Examples:**

- 64 I/O modules with a 12 mm width can be connected to a fieldbus coupler/controller.
- 32 I/O modules with a 24 mm width can be connected to a fieldbus coupler/controller.

**Exception:**

The number of connected I/O modules also depends on the type of fieldbus coupler/controller is used. For example, the maximum number of stackable I/O modules on one PROFIBUS DP/V1 fieldbus coupler/controller is 63 with no passive I/O modules and end module.

---

**NOTICE**

Observe maximum total length of a fieldbus node!

The maximum total length of a fieldbus node without fieldbus coupler/controller and without using a 750-628 I/O Module (coupler module for internal data bus extension) may not exceed 780 mm. Also note the limitations of individual fieldbus couplers/controllers.
Increase the total length using a coupler module for internal data bus extension!

You can increase the total length of a fieldbus node by using a 750-628 I/O Module (coupler module for internal data bus extension). For such a configuration, attach a 750-627 I/O Module (end module for internal data bus extension) after the last I/O module of a module assembly. Use an RJ-45 patch cable to connect the I/O module to the coupler module for internal data bus extension of another module block. This allows you to segment a fieldbus node into a maximum of 11 blocks with maximum of 10 I/O modules for internal data bus extension. The maximum cable length between two blocks is five meters. More information is available in the manuals for the 750-627 and 750-628 I/O Modules.
5.3 Mounting onto Carrier Rail

5.3.1 Carrier Rail Properties

All system components can be snapped directly onto a carrier rail in accordance with the European standard EN 60175 (DIN 35).

---

**NOTICE**

*Do not use any third-party carrier rails without approval by WAGO!*

WAGO Kontakttechnik GmbH & Co. KG supplies standardized carrier rails that are optimal for use with the I/O system. If other carrier rails are used, then a technical inspection and approval of the rail by WAGO Kontakttechnik GmbH & Co. KG should take place.

Carrier rails have different mechanical and electrical properties. For the optimal system setup on a carrier rail, certain guidelines must be observed:

- The material must be non-corrosive.
- Most components have a contact to the carrier rail to ground electromagnetic disturbances. In order to avoid corrosion, this tin-plated carrier rail contact must not form a galvanic cell with the material of the carrier rail which generates a differential voltage above 0.5 V (saline solution of 0.3 % at 20°C).
- The carrier rail must optimally support the EMC measures integrated into the system and the shielding of the I/O module connections.
- A sufficiently stable carrier rail should be selected and, if necessary, several mounting points (every 20 cm) should be used in order to prevent bending and twisting (torsion).
- The geometry of the carrier rail must not be altered in order to secure the safe hold of the components. In particular, when shortening or mounting the carrier rail, it must not be crushed or bent.
- The base of the I/O components extends into the profile of the carrier rail. For carrier rails with a height of 7.5 mm, mounting points are to be riveted under the node in the carrier rail (slotted head captive screws or blind rivets).
- The metal springs on the bottom of the housing must have low-impedance contact with the DIN rail (wide contact surface is possible).
5.3.2 WAGO DIN Rails

WAGO carrier rails meet the electrical and mechanical requirements shown in the table below.

<table>
<thead>
<tr>
<th>Item No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>210-112</td>
<td>35 × 7.5; 1 mm; steel; bluish, tinned, chromed; slotted</td>
</tr>
<tr>
<td>210-113</td>
<td>35 × 7.5; 1 mm; steel; bluish, tinned, chromed; unslotted</td>
</tr>
<tr>
<td>210-197</td>
<td>35 × 15; 1.5 mm; steel; bluish, tinned, chromed; slotted</td>
</tr>
<tr>
<td>210-114</td>
<td>35 × 15; 1.5 mm; steel; bluish, tinned, chromed; unslotted</td>
</tr>
<tr>
<td>210-118</td>
<td>35 × 15; 2.3 mm; steel; bluish, tinned, chromed; unslotted</td>
</tr>
<tr>
<td>210-198</td>
<td>35 × 15; 2.3 mm; copper; unslotted</td>
</tr>
<tr>
<td>210-196</td>
<td>35 × 8.2; 1.6 mm; aluminum; unslotted</td>
</tr>
</tbody>
</table>

5.4 Spacing

The spacing between adjacent components, cable conduits, casing and frame sides must be maintained for the complete fieldbus node.

The spacing creates room for heat transfer, installation or wiring. The spacing to cable conduits also prevents conducted electromagnetic interferences from influencing the operation.
5.5 Mounting Sequence

Fieldbus couplers, controllers and I/O modules of the WAGO I/O SYSTEM 750 are snapped directly on a carrier rail in accordance with the European standard EN 60175 (DIN 35).

The reliable positioning and connection is made using a tongue and groove system. Due to the automatic locking, the individual devices are securely seated on the rail after installation.

Starting with the fieldbus coupler or controller, the I/O modules are mounted adjacent to each other according to the project design. Errors in the design of the node in terms of the potential groups (connection via the power contacts) are recognized, as the I/O modules with power contacts (blade contacts) cannot be linked to I/O modules with fewer power contacts.

⚠️ CAUTION

Risk of injury due to sharp-edged blade contacts!
The blade contacts are sharp-edged. Handle the I/O module carefully to prevent injury. Do not touch the blade contacts.

NOTICE

Insert I/O modules only from the proper direction!
All I/O modules feature grooves for power jumper contacts on the right side. For some I/O modules, the grooves are closed on the top. Therefore, I/O modules featuring a power jumper contact on the left side cannot be snapped from the top. This mechanical coding helps to avoid configuration errors, which may destroy the I/O modules. Therefore, insert I/O modules only from the right and from the top.

Note

Don't forget the bus end module!
Always plug a bus end module (750-600) onto the end of the fieldbus node! You must always use a bus end module at all fieldbus nodes with WAGO I/O SYSTEM 750 fieldbus couplers or controllers to guarantee proper data transfer.
5.6 Inserting and Removing Devices

⚠️ DANGER

Do not work when devices are energized!
High voltage can cause electric shock or burns.
Switch off all power to the device prior to performing any installation, repair or maintenance work.
5.6.1 Inserting the Fieldbus Coupler/Controller

1. When replacing the fieldbus coupler/controller for an already available fieldbus coupler/controller, position the new fieldbus coupler/controller so that the tongue and groove joints to the subsequent I/O module are engaged.

2. Snap the fieldbus coupler/controller onto the carrier rail.

3. Use a screwdriver blade to turn the locking disc until the nose of the locking disc engages behind the carrier rail (see the following figure). This prevents the fieldbus coupler/controller from canting on the carrier rail.

With the fieldbus coupler/controller snapped in place, the electrical connections for the data contacts and power contacts (if any) to the possible subsequent I/O module are established.

![Figure 31: Release Tab of Extended ECO Fieldbus Coupler (Example)](image)

5.6.2 Removing the Fieldbus Coupler/Controller

1. Use a screwdriver blade to turn the locking disc until the nose of the locking disc no longer engages behind the carrier rail.

2. Remove the fieldbus coupler/controller from the assembly by pulling the release tab.

Electrical connections for data or power contacts to adjacent I/O modules are disconnected when removing the fieldbus coupler/controller.
5.6.3 Inserting the I/O Module

1. Position the I/O module so that the tongue and groove joints to the fieldbus coupler or controller or to the previous or possibly subsequent I/O module are engaged.

![Figure 32: Insert I/O Module (Example)](image)

2. Press the I/O module into the assembly until the I/O module snaps into the carrier rail.

![Figure 33: Snap the I/O Module into Place (Example)](image)

With the I/O module snapped in place, the electrical connections for the data contacts and power jumper contacts (if any) to the fieldbus coupler or controller or to the previous or possibly subsequent I/O module are established.
5.6.4 Removing the I/O Module

1. Remove the I/O module from the assembly by pulling the release tab.

![Figure 34: Removing the I/O Module (Example)]

Electrical connections for data or power jumper contacts are disconnected when removing the I/O module.
6 Connect Devices

6.1 Data Contacts/Local Bus

Communication between the fieldbus coupler/controller and the I/O modules as well as the system supply of the I/O modules is carried out via the local bus. The contacting for the local bus consists of 6 data contacts, which are available as self-cleaning gold spring contacts.

![Figure 35: Data Contacts](image)

**NOTICE**

Do not place the I/O modules on the gold spring contacts!
Do not place the I/O modules on the gold spring contacts in order to avoid soiling or scratching!

**NOTICE**

Ensure that the environment is well grounded!
The devices are equipped with electronic components that may be destroyed by electrostatic discharge. When handling the devices, ensure that the environment (persons, workplace and packing) is well grounded. Avoid touching conductive components, e.g. data contacts.
6.2 Power Contacts/Field Supply

⚠️ CAUTION
Risk of injury due to sharp-edged blade contacts!
The blade contacts are sharp-edged. Handle the I/O module carefully to prevent injury. Do not touch the blade contacts.

Self-cleaning power jumper contacts used to supply the field side are located on the right side of most of the fieldbus couplers/controllers and on some of the I/O modules. These contacts come as touch-proof spring contacts. As fitting counterparts the I/O modules have male contacts on the left side.

![Power Jumper contacts diagram](image)

Figure 36: Example for the Arrangement of Power Contacts

**Note**
Field bus node configuration and test via smartDESIGNER
With the WAGO ProServe® Software smartDESIGNER, you can configure the structure of a fieldbus node. You can test the configuration via the integrated accuracy check.


6.3 Connecting a Conductor to the CAGE CLAMP®

The WAGO CAGE CLAMP® connection is appropriate for solid, stranded and finely stranded conductors.

**Note**

Only connect one conductor to each CAGE CLAMP®!
Only one conductor may be connected to each CAGE CLAMP®.
Do not connect more than one conductor at one single connection!

If more than one conductor must be routed to one connection, these must be connected in an up-circuit wiring assembly, for example using WAGO feed-through terminals.

1. For opening the CAGE CLAMP® insert the actuating tool into the opening above the connection.

2. Insert the conductor into the corresponding connection opening.

3. For closing the CAGE CLAMP® simply remove the tool. The conductor is now clamped firmly in place.

![Figure 37: Connecting a Conductor to a CAGE CLAMP®](image)
7 Function Description

7.1 Operating System

After master configuration and electrical installation of the fieldbus station, the system is operative.

The coupler begins running up after switching on the power supply or after a reset.

Upon initialization, the fieldbus coupler determines the I/O modules and configuration. The ‘I/O’ LED flashes red. After a trouble-free start-up, the coupler enters “Fieldbus start” mode and the ‘I/O’ LED lights up green.

In the event of a failure, the ‘I/O’ LED will blink continuously. Detailed error messages are indicated by blinking codes; an error is indicated cyclically by up to 3 blinking sequences.

Figure 38: Operating System

More information about the LED Signaling

Read the detailed description for the evaluation of the displayed LED state in the section “Diagnostics” > … > “LED Signaling”.
7.2 Process Data Architecture

The following sections provide a glimpse of the internal functioning, data processing and addressing in MODBUS communication.

BACnet process data, on the other hand, are not stored in a fixed, internal process image. Using the connected modules, the FC BACnet/IP; G4 creates BACnet objects that represent the process data and that are not located in any directly addressable or visible process image.

7.2.1 Basic Setup

After switching on the fieldbus coupler, it identifies all I/O modules of the node that send or expect to receive data (data/bit width > 0). Any number of analog input/output modules and digital input/output modules can be arranged within a node.

**Information**

Additional Information

For the number of input and output bits or bytes of the individual I/O modules, refer to the corresponding description of the I/O modules.

The coupler creates an internal local process image on the basis of the data width, the type of I/O module and the position of the module in the node. This process image is separated into input and output data range.

For both, the local input and output process image, the I/O module data is stored in the corresponding process image depending on the order in which the modules are connected to the coupler.

First, all the byte-oriented (analog) IO modules are filed in the process image, then the bit-oriented (digital) IO modules. The bits of the digital modules are grouped into bytes. If the amount of digital information exceeds 8 bits, the coupler automatically starts with a new byte.

**Note**

Hardware changes can result in changes of the process image!

If the hardware configuration is changed by adding, changing, removing or reparametrisation of I/O modules with a data width > 0 bit, this result in a new process image structure. The process data addresses would then change. If adding I/O modules, the process data of all previous I/O modules has to be taken into account.

A memory range of 256 words (word 0...255) is initially available in the fieldbus coupler for the process image of the physical input and output data.
If the quantity of module data is greater than 256 words, all the physical input and output data above this value is added to the end of the current process image in a memory range (word 512…1275).

The range from word 1276 to word 1531 is not available to the user.

A MODBUS/TCP Master can access the data for the FC BACnet/IP; G4 via implemented MOFBUS functions.

**Information**

Additional Information

For a detailed description of these fieldbus-specific data access methods, refer to the Section "MODBUS Functions."
7.2.2 MODBUS Process Data

For some I/O modules (and their variations), the structure of the process data depends on the fieldbus.

When applying the MODBUS protocol, the process image has a word structure (with word alignment). The internal mapping method for data greater than one byte conforms to the Intel format. The modules can be mapped directly via addresses with MODBUS.

Information

Additional Information

For the fieldbus-specific structure of the process values of any I/O module within the 750 or 753 Series of the WAGO-I/O-SYSTEM, refer to Section "Structure of process data for MODBUS/TCP".
7.3 Data Exchange

Exchange of process data takes place with FC BACnet/IP; G4 using the BACnet/IP protocol or the MODBUS protocol.

The FC BACnet/IP; G4 works according to the client server principle. The client requests services from the server. It subscribes, for example, to changes in value or sets limits for alarm/event reports. With its objects, the server maps and executes the service requests of the client.

A defined number of simultaneous connections (socket connections) with other network devices can be established to a fieldbus coupler:

- 3 connections for HTTP(S)  
  (to read HTML pages from the fieldbus coupler)
- 30 connections via MODBUS/TCP  
  (to read or write input and output data from the fieldbus coupler)
- 10 connections for (S)FTP
- 2 connections for SNMP

The maximum number of simultaneous connections can not be exceeded. Existing connections must first be terminated before new ones can be set up.

The FC BACnet/IP; G4 is essentially equipped with two interfaces for data exchange:

- the interface to the fieldbus (Master)
- the interface to the I/O modules.

Data exchange takes place between the fieldbus master and the I/O modules.

If MODBUS is used as the fieldbus, access is made to the data using a MODBUS function implemented in the fieldbus coupler.
7.3.1 Memory Space

The fieldbus coupler process image contains the physical data for the bus modules. These have a value of 0 ... 255 and word 512 ... 1275.

1. The input module data can be read by the CPU and by the fieldbus side.
2. Likewise, data can be written to the output modules from the CPU and the fieldbus side.

The memory area for word 1276 ... 1531 is adjacent to the physical I/O module data. This area is reserved and may not be used.

In addition, all output data is mirrored in the FC BACnet/IP; G4 to a memory area with the address offset 0x0200 and 0x1000. This allows output values to be read back in by adding 0x0200 or 0x1000 to the MODBUS address.

7.3.2 Addressing

Module inputs and outputs in a fieldbus coupler are addressed internally as soon as they are started. The order in which the connected modules are addressed depends on the type of module that is connected (input module, output module). The process image is formed from these addresses. The physical arrangement of the I/O modules in the fieldbus node is arbitrary.
7.3.2.1 Addressing of I/O Modules

Addressing first references complex modules (modules that occupy several bytes) in accordance with their physical order downstream of the fieldbus coupler/controller; i.e., they occupy addresses starting from word 0.

Following these is the data for the remaining modules, compiled in bytes (modules that occupy less than one byte). In this process, byte by byte is filled with this data in the physical order. As soon a complete byte is occupied by the bit oriented modules, the process begins automatically with the next byte.

Note

Hardware changes can result in changes of the process image!
If the hardware configuration is changed and/or expanded; this may result in a new process image structure. In this case, the process data addresses also change. If adding modules, the process data of all previous modules has to be taken into account.

Note

Observe process data quantity!
For the number of input and output bits or bytes of the individual IO modules please refer to the corresponding description of the IO modules.

<table>
<thead>
<tr>
<th>Data width &gt; 1 byte (channel)</th>
<th>Data width = 1 bit (channel)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analog input modules</td>
<td>Digital input modules</td>
</tr>
<tr>
<td>Analog output modules</td>
<td>Digital output modules</td>
</tr>
<tr>
<td>Input modules for thermocouples</td>
<td>Digital output modules with diagnostics (2 bits/channel)</td>
</tr>
<tr>
<td>Input modules for resistor sensors</td>
<td>Supply modules with fuse carrier/diagnostics</td>
</tr>
<tr>
<td>Pulse width output modules</td>
<td>Solid-state load relays</td>
</tr>
<tr>
<td>Interface modules</td>
<td>Relay output modules</td>
</tr>
<tr>
<td>Up/down counters</td>
<td></td>
</tr>
<tr>
<td>I/O modules for angle and distance measurement</td>
<td></td>
</tr>
</tbody>
</table>
7.3.3 Data Exchange between MODBUS/TCP Master and I/O Modules

Data exchange between the MODBUS/TCP Master and the I/O modules is conducted using the MODBUS functions implemented in the controller by means of bit-by-bit or word-by-word reading and writing routines.

There are 4 different types of process data in the controller:

- Input words
- Output words
- Input bits
- Output bits

Access by word to the digital I/O modules is carried out in accordance with the following table:

<table>
<thead>
<tr>
<th>Digital inputs/outputs</th>
<th>Process data word</th>
<th>Byte</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>16. 15. 14. 13. 12. 11. 10. 9. 8. 7. 6. 5. 4. 3. 2. 1.</td>
<td>Bit 15</td>
</tr>
<tr>
<td>High byte D1</td>
<td>Low byte D0</td>
<td></td>
</tr>
</tbody>
</table>

Output can be read back in by adding an offset of $200_{\text{hex}}$ ($0x0200$) to the MODBUS address.

**Note**

Data > 256 words can be read back by using the cumulative offset! All output data greater than 256 words and, therefore located in the memory range 0x6000 to 0x62FC, can be read back by adding an offset of $1000_{\text{hex}}$ ($0x1000$) to the MODBUS address.
Register functions start at address 0x1000. These functions can be addressed in a similar manner with the MODBUS function codes that are implemented (read/write). The specific register address is then specified instead of the address for a module channel.

**Information**

**Additional Information**

A detailed description of the MODBUS addressing may be found in Chapter "MODBUS Register Mapping".
7.4 Memory Card Function

The memory card is optional and serves as memory in addition to the internal memory in the fieldbus coupler. The device settings can be saved on the memory card and thus already-existing configurations can be copied to one or more fieldbus couplers(s).

**Note**

*Only use recommended memory cards!*

Use only the SD memory card available from WAGO (item no. 758-879/000-001) since it is suitable for industrial applications under difficult environmental conditions and for use in the fieldbus coupler. Compatibility with other commercially available storage media cannot be guaranteed.

If the memory card has been inserted, it is incorporated into the directory structure of the internal file system of the fieldbus coupler as drive S:. This way, the memory card can be addressed like a changeable medium on a PC.

**Note**

*Deactivate write protection!*

In order to be able to write data on the memory card, you must deactivate the small push switch for the write protection setting. This switch is on one of the long sides of the memory card.

The function of the memory card in normal operation and possible errors that can arise when using the memory card will be described in the following sections for various steps during operation:

- Transfer of configuration data and automatic system start
- Back-up function (Storing device-internal data and settings on the memory card)
- Restore function (Loading device-internal data and settings from the memory card)
- Saving of BACnet trend data
- Inserting a memory card during ongoing operation
- Removing the memory card during ongoing operation
- FTP network access to the file system of the memory card
- Directory structure
Note

Note the pre-formatting of SD card!

Note that SD cards ≤ 2 GB are often formatted with the file system type “FAT16”, and the creation of a maximum of 512 entries in the root directory is possible. For more than 512 entries, create them in a subdirectory, or format the SD card with "FAT32".
7.4.1 Transfer of Configuration Data and Automatic System Start

This function is useful for transferring configuration data between several fieldbus couplers using an SD card.

**Note**

Replication only possible between fieldbus couplers of the same type!

Make sure to execute the “Restore” function for replication between fieldbus couplers with identical item numbers only.

First, start the fieldbus coupler without the SD card being inserted.

The “Autorestore Global Enable” function is enabled in the Web-based Management on the “Backup & Restore” website. In this context, choose to restore after each reboot or in this case, to replicate (“Always restore settings from disk on reboot”) or to restore once on the next reboot only (“Restore settings from disk on next reboot only”).

![Restore Option Setting](image)

Figure 41: Restore Function

Select the data to be copied from the SD card of another fieldbus coupler in the “Settings” column. Only selected options are transferred (e.g., device settings, ports, file system, etc.).

Power supply is interrupted, allowing you to insert the SD card from a different fieldbus coupler.

Then switch on the power for the fieldbus coupler.

The fieldbus coupler is started and the data selected in “Settings” is copied from the S:/copy/xxx directories on the memory card to the respective directories of the internal file system.

Identical data that is already present in the internal file system is not copied.

The LED above the SD card flashes while copying is in progress.

The copied data is then loaded automatically. Device settings and other data are saved in the fieldbus coupler and are executed.
Note

Disable automatic restore function when not used!
If the “Autorestore Global Enable” function, as well as the associated “Always restore settings from SD card on reboot” or “Restore settings from disk on next reboot only” functions are enabled, then the fieldbus coupler is checked each time or on the next reboot if there is already a back-up on the SD card (“copy/xxx” directory). If there is a back-up, the selected parts of the back-up are loaded from the SD card to the fieldbus coupler (Restore). The internal file system is written using the data from the SD card. Disable the “Autorestore Global Enable” function if you do not want the automatic restore function to execute on each or the next reboot.

Table 33: Possible Errors on System Start

<table>
<thead>
<tr>
<th>Possible error</th>
<th>Procedure</th>
<th>Error message</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>No /copy/ and /settings/ directories on the memory card</td>
<td>System start of the fieldbus coupler is running as if no memory card were present.</td>
<td>No message.</td>
<td>If memory card use is desired, map the directory structure of the internal drive under /copy/ on the memory card on the PC. Then restart the fieldbus coupler.</td>
</tr>
<tr>
<td>Manual interrupt</td>
<td>If the /copy/ directory has not yet been copied in full, then the copy process is stopped on manual interrupt. The data is incomplete.</td>
<td>Blink code of the I/O LED for 30 seconds (error code 14, error argument 2) or until the error is eliminated.</td>
<td>Restart system.</td>
</tr>
<tr>
<td>Internal file system is full</td>
<td>As much data is copied until the file system is full. The copy function is cancelled. The data is incomplete.</td>
<td>Blink code of the I/O LED (error code 14, error argument 3) until the error is eliminated.</td>
<td>Check internal file system and /copy/ directory on the memory card and delete data if necessary (e.g. via FTP, formatting internal drive or cleaning the memory card on the PC).</td>
</tr>
<tr>
<td>General internal error</td>
<td>The copy function is cancelled. The data is incomplete.</td>
<td>Blink code of the I/O LED (error code 14, error argument 7).</td>
<td>If necessary, restart function and device.</td>
</tr>
</tbody>
</table>

Note

The file size may not be larger than the size of the internal drive!
Note that the amount of data in the /copy/ directory must not exceed the total size of the internal drive when restoring.
7.4.2 Back-up Function (Storing Device-internal Data and Settings on the Memory Card)

The fieldbus nodes are in operation and the memory card is plugged in.

On the “Backup & Restore” page in the Web-based management system start the function “Backup ALL device settings to removable disk” to save the data on the internal drive and the device settings to the memory card during operation.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>START</td>
<td>Backup ALL device settings to removable disk (77 kB needed).</td>
<td>OK</td>
</tr>
<tr>
<td>START</td>
<td>Restore device settings from removable disk using the option settings below.</td>
<td>OK</td>
</tr>
</tbody>
</table>

Figure 42: WBM Page “Backup & Restore”

In this process, the files from the internal drive are stored in the directory S:/copy/xxx and in the corresponding subdirectories on the memory card. The information that is not present as files on the fieldbus coupler is stored in XML format in the S:/settings/ directory.

Meanwhile, the SD-LED blinks yellow/orange.

The device settings and files of the internal drive are then saved on the memory card.
### Table 34: Possible Errors During the Backup Function

<table>
<thead>
<tr>
<th>Possible error</th>
<th>Procedure</th>
<th>Error message</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory card is full</td>
<td>The copy function is cancelled. Device settings and files in the /copy/ directory and the subdirectories are not saved completely on the memory card.</td>
<td>Blink code of the I/O LED (error code 14, error argument 4) until the error is eliminated.</td>
<td>Replace the memory card with a new one, then restart the backup function. Create storage space on the memory card with the PC.</td>
</tr>
<tr>
<td>Memory card is write-protected.</td>
<td>Copying is not possible, the backup function is cancelled and the memory card remains as it was.</td>
<td>Blink code of the I/O LED (error code 14, error argument 6) until the error is eliminated.</td>
<td>Remove the memory card, remove the write protection, insert the card again, then restart the backup function.</td>
</tr>
<tr>
<td>Manual interrupt</td>
<td>The copy function is cancelled. Device settings and files in the /copy/ directory and the subdirectories are not saved completely on the memory card.</td>
<td>Blink code of the I/O LED for 30 seconds (error code 14, error argument 2) or until the error is eliminated.</td>
<td>Insert memory card, then restart the backup function.</td>
</tr>
<tr>
<td>General internal error</td>
<td>The copy function is cancelled. Device settings and files in the /copy/ directory and the subdirectories are not saved completely on the memory card.</td>
<td>Blink code of the I/O LED (error code 14, error argument 6).</td>
<td>If necessary, restart function and device.</td>
</tr>
</tbody>
</table>
7.4.3 Restore Function (Loading Device-internal Data and Settings from the Memory Card)

The fieldbus nodes and the BACnet configuration are in operation and the memory card is plugged in.

On the “Backup & Restore” page in the Web-based management system, start the “Restore device settings to removable disk using the options below” function in order to load the device settings from the memory card to the internal drive during normal operation.

![Figure 43: WBM Page “Backup & Restore”](image)

For the Restore function, other options can be set that are described in the chapter “Configuring in the Web-based Management System (WBM)”.

![Figure 44: WBM Page “Backup & Restore”](image)

In this process of loading device settings from the Memory Card, the data are copied from the directory S:/copy/ on the memory card to the appropriate directories on the internal drive.

The SD LED flashes yellow/orange while this is in progress.
Note

In case of parameter changes, the device executes a restart!

Note that the device taking the data executes a restart if parameters in the internal drive are overwritten with other parameter settings from the memory card.

Table 35: Possible Errors During the Restore Function

<table>
<thead>
<tr>
<th>Possible error</th>
<th>Procedure</th>
<th>Error message</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>No /copy/ and /settings/ directories on the memory card</td>
<td>Fieldbus coupler is working as if no memory card were present.</td>
<td>No message.</td>
<td>If memory card use is desired, map the directory structure of the internal drive under /copy/ on the memory card on the PC. Then restart the fieldbus coupler.</td>
</tr>
<tr>
<td>Manual interrupt</td>
<td>If the /copy/ directory has not yet been copied in full, then the copy process is stopped on manual interrupt. The data is incomplete.</td>
<td>Blink code of the I/O LED for 30 seconds (error code 14, error argument 2) or until the error is eliminated.</td>
<td>Restart system.</td>
</tr>
<tr>
<td>Internal file system is full</td>
<td>As much data is copied until the file system is full. The copy function is cancelled. The data is incomplete.</td>
<td>Blink code of the I/O LED (error code 14, error argument 3) until the error is eliminated.</td>
<td>Check internal file system and /copy/ directory on the memory card and if necessary, delete files (e.g. through FTP, formatting internal drive or cleaning the memory card on the PC).</td>
</tr>
<tr>
<td>General internal error</td>
<td>The copy function is cancelled. The data is incomplete.</td>
<td>Blink code of the I/O LED (error code 14, error argument 7).</td>
<td>If necessary, restart function and device.</td>
</tr>
</tbody>
</table>

Note

The file size shall not be larger than the size of the internal drive!

During a restore, the file size in the folder S:/copy/ shall not exceed the internal drive’s storage capacity.
7.4.4 Saving BACnet Trend Data

A BACnet trend log object can monitor and detect properties of referenced objects and save them with a time flag. These trend logs are normally stored on the internal drive of the fieldbus coupler.

We recommend saving the BACnet trend data on the SD card in order to enhance storage capacity for extensive trend logs.

To do this, select the option “Save trendlog files on removable disk” on the “BACnet” Web page in the Web-based management system to define the SD card as the storage location. Existing trend logs are retained on the internal drive of the fieldbus coupler. New trend logs will be stored on the SD card after this setting is defined.

If the SD card is removed even though it is activated as the storage location and the fieldbus coupler is in normal operation, this setting is retained in the WBM. Saving of trend logs is then discontinued. The BACnet/IP protocol continues to run, however. The BACnet property “Reliability” for the trend log object, when available, is then set to “UNRELIABLE_OTHER”. No flash code is output in this case.

Saving of trend logs is resumed when the SD card is re-inserted.

Note limits when creating trend log objects!
To avoid filling the internal drive or SD card with BACnet trend data completely, the data volume is limited for this purpose.

The upper limit is:
• 60,000 trend logs when using the internal memory
• 4,000,000 trend logs when using an SD card

If the limit is exceeded, no further trend log objects can be created. No error is displayed.
7.4.5 Inserting a Memory Card during Operation

The fieldbus nodes and BACnet configuration are running.

Insert a memory card during ongoing operation.

During normal operation, the memory card is incorporated into the file system of the fieldbus coupler as a drive.
No automatic copy procedures are triggered.

The SD-LED blinks yellow/orange during the access.

The memory card is then ready for operation and available as drive S:

---

**Note**

BACnet functionality after re-inserting the SD card not active until after a restart!
If the “PLC Root Location” on the WBM page “PLC” is set to an external location (saving to the SD card), inserting the SD card during operation has no effect on the BACnet functionality. Not until the next restart of the device is the configuration loaded from the SD card and used.

<table>
<thead>
<tr>
<th>Possible error</th>
<th>Procedure</th>
<th>Error message</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to the memory card is not possible</td>
<td>The incorporation (mounting) of the memory card as drive is cancelled. The fieldbus coupler behaves as if no memory card were present.</td>
<td>Blink code of the I/O LED: error code 14, error argument 1, until the error is eliminated.</td>
<td>Replace the memory card with a new one.</td>
</tr>
<tr>
<td>Memory card cannot be read</td>
<td>The incorporation (mounting) of the memory card as drive is cancelled.</td>
<td>Blink code of the I/O LED: error code 14, error argument 1, until the error is eliminated.</td>
<td>Replace the memory card with a new one.</td>
</tr>
<tr>
<td>Memory card is not formatted</td>
<td>The incorporation (mounting) of the memory card as drive is cancelled.</td>
<td>Blink code of the I/O LED: error code 14, error argument 1, until the error is eliminated.</td>
<td>Replace memory card with a new one or format with PC.</td>
</tr>
<tr>
<td>Memory card is not in FAT or FAT32 format.</td>
<td>The incorporation (mounting) of the memory card as drive is cancelled.</td>
<td>Blink code of the I/O LED: error code 14, error argument 1, until the error is eliminated.</td>
<td>Replace memory card with a new one or format with PC.</td>
</tr>
</tbody>
</table>
7.4.6 Removing the Memory Card During Operation

The fieldbus nodes are in operation and the memory card is plugged in.

Remove the memory card during ongoing operation.

**Note**

Data can be lost during writing!
The SD-LED blinks yellow/orange during the access.
Note that if you pull the memory card out during a write procedure, data will be lost. Even persistent values for BACnet properties, objects added online or trend log entries can be lost.

The fieldbus coupler then works without memory card.

<table>
<thead>
<tr>
<th>Possible error</th>
<th>Procedure</th>
<th>Error message</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read procedure is running</td>
<td>Read access is cancelled. The fieldbus coupler then works without memory card.</td>
<td>Blink code of the I/O LED for 30 seconds: error code 14, error argument 2, if the backup or restore function is active.</td>
<td>If memory card usage is desired, insert the memory card, then restart the access function.</td>
</tr>
<tr>
<td>Write procedure is running</td>
<td>Write access is cancelled. The fieldbus coupler then works without memory card.</td>
<td>Blink code of the I/O LED for 30 seconds: error code 14, error argument 2, if the backup or restore function is active.</td>
<td>If memory card usage is desired, insert the memory card, then restart the access function.</td>
</tr>
</tbody>
</table>
7.4.7 FTP Network Access to the File System of the Memory Card

The fieldbus node is in operation and the memory card is plugged in.

The FTP client accesses the file system of the memory card (drive S:) via the network.

In normal operation, the FTP client writes data to the file system of the memory card or reads data from the file system of the memory card.

Meanwhile, the SD-LED blinks yellow/orange.

The data is then written or read.

Table 38: Possible Errors During the FTP Network Access on the File System of the Memory Card

<table>
<thead>
<tr>
<th>Possible error</th>
<th>Procedure</th>
<th>Error message</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>No memory card is plugged in.</td>
<td>Access function is cancelled.</td>
<td>Depending on the FTP client used, the error is reported.</td>
<td>If memory card usage is desired, insert a memory card, then if necessary, close the existing FTP connection and establish a new one, then restart FTP access.</td>
</tr>
<tr>
<td>Manual interrupt</td>
<td>Access function is cancelled.</td>
<td>Depending on the FTP client used, the error is reported.</td>
<td>If necessary, close existing FTP connection and establish a new one, then restart FTP access.</td>
</tr>
</tbody>
</table>

**Note**

Observe FTP access rights!

The FTP access rights correspond to those for the WBM. Note here that with “guest” access rights you are provided only with read access to the file system. Log in as “admin” to obtain write access.

**Note**

FTP connection must be closed and then re-established!

Note that if you pull the memory card out with an existing FTP connection and then insert it again, that you must then close the existing FTP connection and establish it again so that access to the memory card is possible.
7.4.8 Directory Structure

On the WBM page “Features”, you can create a backup copy of the internal drive using the function “Backup device settings to removable disk”. The folder “copy” is created for this on the SD card. All of the files and subdirectories on the internal drive “A:" will then be copied to this folder.

In addition, the device settings are also written to the directory “S:\settings” on the memory card.

On the WBM page “Features” you can restore the SD card data to the internal drive “A:" using the function “Restore device settings from removable disk”. All of the files and subdirectories are copied for this from the directory “S:/copy” on the memory card to the internal drive “A:".

In addition, the device settings are loaded from the directory “S:\settings” and activated.

![Figure 46: Example of Directory Structure on the SD Card](image)

Table 39: Data Saved in the Directory Structure

<table>
<thead>
<tr>
<th>Directory</th>
<th>Data saved</th>
</tr>
</thead>
<tbody>
<tr>
<td>S:\copy</td>
<td>The folder “copy” is created on the SD card via the backup function of the Web-based Management System (WBM page “Feature”). This folder contains a copy of the internal drive.</td>
</tr>
<tr>
<td>S:\copy\etc</td>
<td>Node configuration, BACnet files (backup)</td>
</tr>
<tr>
<td>S:\copy\PLC</td>
<td>-</td>
</tr>
<tr>
<td>S:\copy\webserv</td>
<td>WBM Web pages (backup)</td>
</tr>
<tr>
<td>S:\settings</td>
<td>All saved EEPROM parameters (backup)</td>
</tr>
</tbody>
</table>

If saving to an “External SD memory card” is activated in the WBM on the page “PLC”, the following directories will also be created in the SD card directory:

<table>
<thead>
<tr>
<th>Directory</th>
<th>Data saved</th>
</tr>
</thead>
<tbody>
<tr>
<td>S:\etc</td>
<td>BACnet configuration files (SYM_XML, Override, etc.)</td>
</tr>
<tr>
<td>S:\PLC</td>
<td>-</td>
</tr>
</tbody>
</table>
8 Commissioning

This section shows a step-by-step procedure for starting up exemplarily a WAGO fieldbus node.

**Note**

Good example!
This description is just an example and only serves to describe the procedure for a local start-up of a single fieldbus node with a PC under Windows.

In principle, only a few steps are required for start-up.

To enable communication from your PC to the fieldbus coupler/controller over network, both must be in the same network. This requires that you first determine the IP address of the PC and then assign a corresponding IP address to the fieldbus node. There are several options being available for IP address assignment.

The description of these single work steps can be found in the corresponding following chapters.

- Connecting PC and fieldbus node
- Determining IP address of the PC
- Assigning IP address to the fieldbus node
- Applying IP address permanently (option “static”)

Following the commissioning descriptions after which the fieldbus node is ready for communication, the following topics are described:

- Preparing the Flash File System
- Synchronizing the System Time
- Restoring Factory Settings
8.1 Connecting Client PC and Fieldbus Nodes

1. Mount the fieldbus node on the TS 35 carrier rail. Follow the mounting instructions found in the “Mounting” chapter.

2. Connect the 24 V power supply to the supply terminals.

3. Connect the PC’s ETHERNET interface to the head station’s ETHERNET interface (RJ-45) of your fieldbus node.

4. Turn the operating voltage on.

The head station is initialized. The head station determines the I/O module configuration of the fieldbus node and creates a process image. During start-up, the I/O LED (red) flashes. If the I/O LED lights up green after a brief period, the fieldbus node is operational.

If an error has occurred during initialization, it is red flashed with an error code by the I/O LED. If the I/O LED flashes 6 times (indicating error code 6) and then 4 times (indicating error argument 4), this indicates that an IP address has not been assigned yet.

8.2 Determining the IP Address of the PC

To determine the IP address of the PC (with Microsoft Windows operating system) using the MS DOS prompt, proceed as follows:

1. Go via "Start"> "Search programs/files".

2. Enter the command "cmd" in the input field.

3. Choose at (Windows 7): "cmd.exe" and (Windows 10): "Command Prompt".

4. Press [Enter] key to confirm the entry.

The MS DOS prompt window opens.

5. In the MS DOS prompt window enter the command “ipconfig”.

6. Press [Enter] key to confirm the entry.

The IP address, subnet mask and the default gateway with the corresponding parameters of the PC are displayed.
8.3 Assigning the IP Address to the Fieldbus Node

The IP address must occur in the network only once!
For error-free network communication, note that the assigned IP address must occur only once in the network!
In the event of an error, the error message “IP address configuration error” (error code 6 – error argument 7) is indicated by 'I/O' LED at the next power-on.

- Use **address selection switch** (DIP switch) to assign IP address (manually).
- **Automatic assignment of addresses via DHCP** (IP address via the fieldbus)
- **Assigning IP Address via “WAGO Ethernet Settings”** (static IP address via the serial communication port or the ETHERNET interface)
- **Assigning IP Address via BootP** (IP address via the fieldbus)
8.3.1 Information about the Starting Behavior regarding BACnet

The address selector switch is set to 0 by default, i.e. the IP configuration from the Web-based Management system (WBM) is used. The IP address assignment is again set to DHCP by default in the WBM.
8.3.2 Assigning IP Address via Address Selection Switch

Use the address selection switch to set the host ID, which is the last byte of the IP address, with values between 1 and 254 binary coded.

The first three bytes of the IP address are specified by the fieldbus coupler/controller. The fieldbus coupler/controller uses a static base IP address to assign the IP address via the address selector switch. The basic IP address can be changed via the Web-based management or WAGO Ethernet settings (in the delivery state: 192.168.1.0).

The subnet mask and default gateway values are taken from the static settings (as delivered: subnet mask = 255.255.255.0, default gateway = 0.0.0.0).

Example:

<table>
<thead>
<tr>
<th>Base IP address:</th>
<th>192.168.1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set DIP switch value:</td>
<td>50 (binary coded: 00110010)</td>
</tr>
<tr>
<td>Resulting IP address:</td>
<td>192.168.1.50</td>
</tr>
</tbody>
</table>

Table 40: Address selection switch values (host ID)

<table>
<thead>
<tr>
<th>Address selection switch</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ... 254</td>
<td>The host ID is set to a fixed value between 1 ... 254. The IP address consists of the static base address and the set host ID. The IP address set via the current device configuration (DHCP, BootP, static) is disabled.</td>
</tr>
<tr>
<td>0</td>
<td>Address selection switch is disabled. The IP address set via the current device configuration (DHCP, BootP, static) is used.</td>
</tr>
<tr>
<td>255</td>
<td>Address selection switch is disabled. The IP address is obtained from a DHCP server.</td>
</tr>
</tbody>
</table>

Information

More information about changing the static base address

You can also change the static base address currently saved in the fieldbus coupler/controller as required. Proceed as described for example in the section “Assigning IP Address via “WAGO Ethernet Settings”.”
1. To configure the IP address via the address selection switch by setting the host ID (last position of the IP address) to a value that does not equal 0/255, first convert the host ID to the binary representation. For example, host ID “50” results in a binary code of “00110010”.

2. Set the bits in sequence using the 8 address switches. Start with address switch 1 to set bit 0 (LSB) and end with address switch 8 for bit 7 (MSB).

![Address Selection Switch](image)

Figure 47: Address Selection Switch, for Example the Value Setting “50” (2^1 + 2^4 + 2^5)

3. Restart the fieldbus node after adjusting the address selection switch to apply the configuration changes.

8.3.3 Assigning IP Address via DHCP

**Note**

Set the address selection switch to 255 for assigning the IP address via DHCP!
Set the address selection switch to 255 to disable the DIP switch and to enable DHCP.
Restart the fieldbus node after adjusting the address selection switch to apply the configuration changes.

In delivery state of the head station, the dynamic assignment of the IP address is active by means of "Dynamic Host Configuration Protocol" (DHCP).

When the DHCP protocol is enabled the head station of fieldbus node expects the DHCP server to be permanently available. If there is no DHCP server available after a Power On reset, the network will remain inactive.

If DHCP is not active, it is necessary to enable DHCP, e. g. via "WAGO Ethernet Settings" or via the WBM (see chapters "Enable DHCP via "WAGO Ethernet Settings" (without existing IP address)" or "Enable DHCP via WBM (with existing IP address)"").

Then the IP address assignment with DHCP takes place automatically via a DHCP server in the network.
If there is no DHCP server on your local PC, you can download a DHCP server free of charge from the Internet and install it on your PC.

**Note**

**Total network failure when there are two DHCP servers in the network!**
To prevent network failure, never connect a PC, on which a DHCP server is installed, to a global network. In larger networks, there is usually a DHCP server already that can cause collisions and subsequent network failure.

**Note**

**Assign the DHCP server a fixed IP address and note common subnet!**
Note that the DHCP server must have a fixed IP address and that the fieldbus node and DHCP server must be in the same subnet.

After the IP address was assigned by means of DHCP, it can be determined via the settings or outputs of the respective DHCP server, such as via the output of "Open DHCP", for example.

**Note**

**Via DHCP assigned IP addresses are only temporarily valid!**
Note that an IP address assigned via DHCP is limited in time. If the DHCP server is not available at the end of its useful life, the fieldbus node sets the IP address free and then the fieldbus node is no longer accessible!

In order to use the IP address permanently, change it to “static” (see chapter "Apply IP address permanently (option "static "))."
8.3.3.1 Enable DHCP via "WAGO Ethernet Settings" (without existing IP address)"

**Note**

Note Software Compatibility!
Refer to the version of the software specified in "Software Compatibility" in the Technical Data.

In the delivery state of the head station, the dynamic assignment of the IP address is active by means of "Dynamic Host Configuration Protocol" (DHCP).

However, if DHCP is not active and you do not have access to your fieldbus node via an IP address, you can enable DHCP via "WAGO Ethernet Settings" in the Network tab.

WAGO communication cables or WAGO radio-link adapters can be used for data communication via the serial service interface.

**NOTICE**

Do not connect Communication Cable when energized!
To prevent damage to the service interface, do not connect or disconnect 750-920 respectively 750-923 Communication Cable when energized! The fieldbus coupler/controller must be de-energized!

1. Using a WAGO Communication cable 750-920 respectively 750-923, connect your PC with the service interface of the head station of the fieldbus node.

2. Start “WAGO Ethernet Settings” program.

3. Click on [Read] to read in and identify the connected fieldbus node.

4. Select the Network tab.

5. Select the option "DHCP" in the field Source.

6. Click on the [Write] button to apply the settings in the fieldbus node.

   The fieldbus node then starts with the new IP address assigned via DHCP.

7. Then You can use the [Read] button to read out the currently assigned IP address.

8. In order to use the IP address permanently, select on "TCP/IP" WBM page the option "static" in the field Source and apply the settings for "IP address", "Subnet mask" and "Gateway" from the currently used settings.

9. Click on the [Write] button to apply the settings.
### 8.3.3.2 Enable DHCP via WBM (with existing IP address)

In the delivery state of the head station, the dynamic assignment of the IP address is active by means of "Dynamic Host Configuration Protocol" (DHCP).

However, if DHCP is not active and you do already have access to your fieldbus node via an IP address, you can enable DHCP via WBM on "TCP/IP" WBM page.

1. Open the WBM (see chapter: "Configuring via the Web-Based Management System (WBM)") >> "Open WBM").
2. Change to the WBM page "TCP / IP".
3. Activate the “DHCP“ option to assign a new IP address via DHCP.
4. Confirm the change with the [SUBMIT] button.
5. Select the WBM page "Administration".
6. Click the [SOFTWARE RESET] button to apply the changed setting.

Alternatively, you can restart the fieldbus node.

The fieldbus node then starts with the new IP address assigned via DHCP. The connection to the browser is interrupted.

7. If you want to call the WBM again, you must use now the changed IP address.

8. In order to use the IP address permanently, select in the WBM on "TCP/IP" WBM page the option "IP configuration source: static" (see chapter "Apply IP address permanently (option "static ")").

9. In order to use the IP address permanently, select on "TCP/IP" WBM page the option "static" in the field Source and apply the settings for "IP address", “Subnet mask” and “Gateway” from the currently used settings.

10. Confirm the change with the [SUBMIT] button.
11. Click the [SOFTWARE RESET] button to apply the changed setting.
8.3.4 Assigning IP Address via “WAGO Ethernet Settings”

Note Software Compatibility!
Refer to the version of the software specified in "Software Compatibility" in the Technical Data.

This program is used to configure an IP address, to reset the fieldbus coupler/controller parameters to the factory settings and to restore the Flash File System in which the WBM pages of the fieldbus coupler/controller are stored. "WAGO Ethernet Settings" can be used via the serial service interface or via the ETHERNET interface.

For initial commissioning, however, the way via the serial service interface is described here, because for access via the ETHERNET interface the currently assigned IP address must already be known.

WAGO communication cables or WAGO radio-link adapters can be used for data communication via the serial service interface.

NOTICE
Do not connect Communication Cable when energized!
To prevent damage to the service interface, do not connect or disconnect 750-920 respectively 750-923 Communication Cable when energized! The fieldbus coupler/controller must be de-energized!

Note
Set the address selection switch to 0 for an IP assignment via software!
Set the address selection switch to “0” to disable the DIP switch. Restart the fieldbus node after adjusting the address selection switch to apply the configuration changes.

1. Using a WAGO Communication cable 750-920 respectively 750-923, connect your PC with the service interface of the head station of the fieldbus node.

2. Start “WAGO Ethernet Settings” program.

3. Click on [Read] to read in and identify the connected fieldbus node.

4. Select the Network tab.

5. To assign a permanent address, select the option "Static configuration" in the field Source.
6. Enter the required **IP Address** and, if applicable, the address of the subnet mask and gateway.

7. Click on the [Write] button to apply the settings in the fieldbus node.

8. You can now close "WAGO Ethernet Settings" or make other changes in the Web-based Management System as required. To open the Web-based Management System click on the button [Start WBM] on the right side.
8.3.5 Assigning the IP Address via BootP

A BootP server can be used to assign a fixed IP address.

Assigning the IP address using a BootP server depends on the respective BootP program. Handling is described in the respective manual for the program or in the respective integrated help texts.

**Note**

Set the address selection switch to 0 for an IP assignment via software!
Set the address selection switch to “0” to disable the DIP switch.
Restart the fieldbus node after adjusting the address selection switch to apply the configuration changes.

By default, DHCP is active in the delivery state of the head station.

Therefore it is necessary to enable BootP for IP address assignment via BootP, e.g. via "WAGO Ethernet Settings" or via the WBM (see analog the chapters "Activate DHCP via "WAGO Ethernet Settings" (without existing IP address)" or "Activate DHCP via WBM (with existing IP address)"").

Then the IP address assignment with BootP takes place automatically via a BootP server in the network.

If there is no BootP server on your local PC, you can download a BootP server free of charge from the Internet and install it on your PC.

**Information**

Additional Information
Assigning IP addresses using a BootP server can be carried out in any Windows and Linux operating system. Any BootP server may be used.

**Note**

IP address assignment is not possible via the router!
The IP address is assigned via patch cable, switches or hubs. Addresses cannot be assigned via routers.

When the BootP protocol is enabled the head station of fieldbus node expects the BootP server to be permanently available. If there is no BootP server available after a Power On reset, the network will remain inactive.

In order to use the IP address permanently, change it to “static” (see chapter "Apply IP address permanently (option "static ")").
1. Based on the handling, which depends on the BootP program set, assign the required IP address for your fieldbus node.

2. Enable the query/response mechanism of the BootP protocol based on the handling, which depends on the BootP program set or e.g. in "WAGO Ethernet Settings" (Network tab, Source "BootP").

3. To apply the new IP address, use e.g. a hardware reset to restart your fieldbus node by interrupt the voltage supply for approx. 2 seconds.

4. Restart the fieldbus node.

The fieldbus node then starts with the new IP address assigned via BootP.

5. In order to use the IP address permanently, select in the WBM on "TCP/IP" WBM page the option "IP configuration source: static" (see chapter "Apply IP address permanently (option "static ")").
8.3.5.1 Reasons for Failed IP Address Assignment

- The PC on whom the BootP server is running is not located in the network as the fieldbus coupler/controller; i.e., the IP addresses do not match.

  Example:
  
  Sub net mask: 255.255.255.0
  (default value for a fieldbus coupler/controller n)

  PC’s IP: 192.168.2.100
  fieldbus coupler/controller’s IP: 192.168.1.200

  Due to the sub net mask, the first 3 digits of the IP addresses must match.

- PC and/or head station is/are not linked to the ETHERNET
8.4 Apply IP address permanently (option “static“)

**Note**
For permanent address assignment, the IP stored in the EEPROM must be used!
To apply permanently the new IP address assigned via DHCP or BootP in the fieldbus coupler/controller, the assigned or desired settings for IP address, subnet mask and default gateway must be entered on the WBM “TCP/IP” page. In addition the option "IP configuration source: static" must be activated. Then, the IP address is stored in the EEPROM and used as static address.

You can enable the option "IP configuration source: static" in the Web-based Management System.

1. Open the WBM (see chapter: "Configuring in the Web-Based Management System (WBM)" >> "Open WBM").
2. Select the WBM page "TCP/IP".
3. Enter the assigned or desired settings for IP address, subnet mask and default gateway in the fields "IP address", "Subnet mask" and "Default gateway".
4. Enable the option "IP configuration source: static".
   At the same time, the use of the DHCP/BootP server is disabled.
5. Confirm your changes with button **[SUBMIT]**.
6. Select the “Administration” WBM page.
7. Click on the button **[Software Reset]** at the bottom of the page in order for the settings to take effect.
   Alternatively restart the fieldbus node.
   Then the fieldbus node starts with the configurations and the assigned IP address, which were previously loaded into the EEPROM. The connection to the browser is interrupted.
8. Now you must use the new IP address, if you want to access again on the WBM of this fieldbus node via browser.
8.5 Testing the Function of the Fieldbus Node

1. To ensure that the IP address is correct and to test communication with the fieldbus node, first turn off the operating voltage of the fieldbus node.

2. Create a non-serial connection between your PC and the fieldbus node.

The head station is initialized. The head station determines the I/O module configuration of the fieldbus node and creates a process image. During start-up, the I/O LED (red) flashes. If the I/O LED lights up green after a brief period, the fieldbus node is operational.

If an error occurs during start-up indicated by the I/O LED flashing red, evaluate the error code and argument and resolve the error.

Information

More information about LED signaling
The exact description for evaluating the LED signal displayed is available in the section “Diagnostics” > … > “LED Signaling”.
8.6 Preparing the Flash File System

The flash file system must be prepared in order to use the WBM of the fieldbus coupler/controller of the fieldbus node to make all configurations.

The flash file system is already prepared when delivered. However, if the flash file system has not been initialized on your fieldbus coupler/controller or it has been destroyed due to an error, you first must initialize it manually to access it.

**NOTICE**

Do not connect Communication Cable when energized!
To prevent damage to the service interface, do not connect or disconnect 750-920 respectively 750-923 Communication Cable when energized! The fieldbus coupler/controller must be de-energized!

**Note**

Resetting erases data!
Note that resetting erases all data and configurations. Only use this function when the flash file system has not been initialized yet or has been destroyed due to an error.

1. Switch off the supply voltage of the fieldbus node.
2. Connect the communication cable 750-920 or 750-923 respectively the Bluetooth® Adapter 750-921 to the service interface of the head station of the fieldbus node and to your computer.
3. Switch on the supply voltage of the fieldbus node.

The head station is initialized. The head station determines the I/O module configuration of the fieldbus node and creates a process image. During start-up, the I/O LED (red) flashes. If the I/O LED lights up green after a brief period, the fieldbus node is operational.

If an error occurs during start-up indicated by the I/O LED flashing red, evaluate the error code and argument and resolve the error.

**Information**

More information about LED signaling
The exact description for evaluating the LED signal displayed is available in the section “Diagnostics” > … > “LED Signaling”.

4. Start the “WAGO Ethernet Settings” program.
5. In the top menu bar, select [Reset File System] to format the file system and to extract the WBM pages of the flash file system.

Formatting and extracting is complete when the status window displays "Resetting the file system successfully".

---

**Note**

**Restart the Fieldbus node after resetting file system!**

Make a restart of the fieldbus node, so that the WBM pages can be displayed after resetting file system.
8.7 Synchronizing the System Time

The head station’s system time enables a date and time indication for files in the flash file system.

Note

System time will be reset when the fieldbus node is de-energized!
The head station 750-332 does not have a real-time clock. For this reason, the current system time will be reset when the fieldbus node is de-energized!
After switching on the operating voltage, the system time starts at 01/01/2000, 00:00:00 a.m.

At start-up, synchronize the system time with the computer’s current time.

There are two options to synchronize the system time:

- Synchronize the system time using “WAGO Ethernet Settings”
- Synchronize the system time using the Web Based Management System

Synchronize the system time using “WAGO Ethernet Settings”

Note

Do not set time during a WAGO I/O-CHECK communication!
Note that setting the clock during a WAGO I/O-CHECK communication may cause communication errors. Therefore set the time only if WAGO I/O-CHECK is not yet started.

1. Switch off the supply voltage of the fieldbus node.

2. Connect the communication cable 750-920 or 750-923 respectively the Bluetooth® Adapter 750-921 to the service interface of the head station of the fieldbus node and to your computer.

3. Switch on the supply voltage of the fieldbus node.

The head station is initialized. The head station determines the I/O module configuration of the fieldbus node and creates a process image.
During start-up, the I/O LED (red) flashes.
If the I/O LED lights up green after a brief period, the fieldbus node is operational.

If an error occurs during start-up indicated by the I/O LED flashing red, evaluate the error code and argument and resolve the error.
More information about LED signaling
The exact description for evaluating the LED signal displayed is available in the section “Diagnostics” > … > “LED Signaling”.

4. Start the “WAGO Ethernet Settings” program.

5. Select the Date and Time tab.

6. Click on the [Apply] button.

Synchronize the system time using the Web-based Management-System

1. Launch a Web browser (e.g., MS Internet Explorer or Mozilla) and enter in the address bar the IP address you have assigned to your fieldbus node.

2. Click [Enter] to confirm.
   The WBM start page is displayed.

3. Select “Clock” in the left navigation bar.

4. Enter your user name and password in the displayed query dialog box (default: user = "admin", password = "wago" or: user = "user", password = "user"). The WBM page "Clock" is displayed.

5. Set the current time and date values, as well as the time zone deviation in the input fields, and select the desired option for the display and Daylight Saving Time (DST).

6. Click on [SUBMIT] to apply the changes in your fieldbus node.

7. Restart the fieldbus node to apply the settings of the Web interface.
8.8 Restoring Factory Settings

To restore the factory settings, proceed as follows:

1. Switch off the supply voltage of the fieldbus node.

2. Connect the communication cable 750-920 or 750-923 respectively the Bluetooth® Adapter 750-921 to the service interface of the head station of the fieldbus node and to your computer.

3. Switch on the supply voltage of the fieldbus node.

4. Start the WAGO-ETHERNET-Settings program.

5. In the top menu bar, select [Factory Settings] and click [Yes] to confirm.

A restart of the fieldbus node is implemented automatically. The start takes place with the default settings.
9 Configuring via the Web-Based Management System (WBM)

An integrated Web server can be used for configuration and administration of the device. The HTML pages together, they are referred to as the Web-based Management System (WBM).

The WBM pages saved internally provide current information about the configuration and status of the device. The configuration of the device can be changed via the special configuration pages. Authentication is required for this. Also HTML pages created by yourself can be save via the implemented file system.

Note
After changes to the configuration, a restart may be necessary!

In order for changed configuration settings to take effect, it may be necessary for you to perform a system restart after your changes. This is then indicated in the description text on the respective WBM pages.

9.1 WBM User Groups

For authentication, 3 different password-protected user authorization groups are provided as standard:

Table 41: WBM User Groups

<table>
<thead>
<tr>
<th>User Group</th>
<th>Default Password</th>
<th>Access Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>wago</td>
<td>Read/write access to all WBM pages as well as passwords modification and CODESYS application download, if this is enabled for CODESYS (WBM page &quot;Administration&quot;&gt; &quot;Security Settings&quot;&gt; &quot;Enable CODESYS port authentication&quot;)</td>
</tr>
<tr>
<td>user</td>
<td>user</td>
<td>Read/write access to all WBM pages, but no write authorization on WBM-page &quot;Administration&quot;</td>
</tr>
<tr>
<td>guest</td>
<td>guest</td>
<td>Read only</td>
</tr>
</tbody>
</table>
9.2 Open WBM

1. To open the WBM, launch a Web browser.

2. Enter the IP address of the fieldbus coupler/controller in the address bar.

3. Click [Enter] to confirm.
   The start page of WBM loads.

4. Select the link to the desired WBM page in the left navigation bar.
   The first time a configuration page is called, a login dialog appears

5. Enter your user name and password in the query dialog (default: user = “admin”, password = “wago” or user = “user”, password = “user”).
   The corresponding WBM page is loaded.

6. Make the desired settings.

7. Click [SUBMIT] to confirm your changes or click [UNDO] to discard the changes.
   At the first confirmation via the [SUBMIT] button, a login dialog appears again. Proceed as described under point 5.

8. To apply the settings, you may have to reboot afterwards if this is indicated in the description text on the respective WBM page.
   You restart the system using WBM page “Administration”, button [SOFTWARE RESET].
9.3 WBM Pages

You can access the available WBM pages via the links given in the navigation bar on the left side. The configuration pages, listed below, are following described.

![WBM page "Information" example](image)

Figure 48: WBM page "Information" (example)
9.4 Information

The WBM page “Information” contains an overview of all important information about your fieldbus coupler.

Table 42: WBM Page “Information”

<table>
<thead>
<tr>
<th>Device details</th>
<th>Entry</th>
<th>Default</th>
<th>Value (example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product description</td>
<td>Fieldbus Coupler BACnet/IP; Generation 4</td>
<td></td>
<td></td>
<td>Produkt description</td>
</tr>
<tr>
<td>Order number</td>
<td>750-332</td>
<td></td>
<td></td>
<td>Order number</td>
</tr>
<tr>
<td>Mac address</td>
<td>0030DEXXXXXX</td>
<td>0030DE000006</td>
<td>Hardware MAC address</td>
<td></td>
</tr>
<tr>
<td>Firmware revision</td>
<td>kk.ff.bb(rr)</td>
<td>01.01.14(01)</td>
<td>Firmware revision number</td>
<td></td>
</tr>
<tr>
<td>(kk = compatibility, ff = functionality, bb = bugfix, rr = revision)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firmware loader revision</td>
<td>kk.ff.bb(rr)</td>
<td>01.03.01(03)</td>
<td>Firmware loader revision number</td>
<td></td>
</tr>
<tr>
<td>(kk = compatibility, ff = functionality, bb = bugfix, rr = revision)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial number</td>
<td>—</td>
<td>“”</td>
<td>Serial number of device</td>
<td></td>
</tr>
<tr>
<td>(manufacturer-specific identification of device)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial number (UII)</td>
<td>—</td>
<td>“”</td>
<td>“Unique Item Identifier” (world wide unique identification of device)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Active Network Settings</th>
<th>Entry</th>
<th>Default</th>
<th>Value (example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>0.0.0.0</td>
<td>172.29.233.123</td>
<td>IP address, Type of IP address assignment</td>
<td></td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
<td>255.0.0.0</td>
<td>Subnet mask</td>
<td></td>
</tr>
<tr>
<td>Default gateway</td>
<td>0.0.0.0</td>
<td>192.168.2.1</td>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>Host name</td>
<td>0030DEXXXXXX</td>
<td>0030DE000000</td>
<td>Host name</td>
<td></td>
</tr>
<tr>
<td>Domain name</td>
<td>—</td>
<td>—</td>
<td>Domain name (not assigned here)</td>
<td></td>
</tr>
<tr>
<td>Time server</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Address of Time server</td>
<td></td>
</tr>
<tr>
<td>DNS server 1</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Address of first DNS server</td>
<td></td>
</tr>
<tr>
<td>DNS server 2</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Address of second DNS server</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module Status</th>
<th>Entry</th>
<th>Default</th>
<th>Value (example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Modbus Watchdog</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Status of Modbus Watchdog</td>
<td></td>
</tr>
<tr>
<td>Error Code</td>
<td>0</td>
<td>10</td>
<td>Error code</td>
<td></td>
</tr>
<tr>
<td>Error Argument</td>
<td>0</td>
<td>5</td>
<td>Error argument</td>
<td></td>
</tr>
<tr>
<td>Error Description</td>
<td>no error</td>
<td>Missmatch in CODESYS IO-configuration</td>
<td>Error description</td>
<td></td>
</tr>
</tbody>
</table>
9.5 Administration

Use the "Administration" WBM page to set configuration options for basic administration purposes, such as boot behavior, authentication, and SSL certificate.

These configuration options are stored in non-volatile memory when the [SUBMIT] button is pressed. Changes to the configuration options take effect after the next power-on cycle or software reset.

→ Note

Changing the passwords requires administrator rights and software reset!
You can only change the passwords as an administrator with the user rights "admin" and the associated password.
Press the [Software Reset] button to restart the software for the setting changes to take effect.

→ Note

Note password restrictions!
The following restriction is applied for passwords:
• Max. 32 characters inclusive special characters.

→ Note

Renew access after software reset!
If you initiate a software reset on this page, then the fieldbus coupler/controller starts with the configurations previously loaded into the EEPROM and the connection to the browser is interrupted.
If you changed the IP address previously, you have to use the changed IP address to access the device from the browser.
You have not changed the IP address and performed other settings; you can restore the connection by refreshing the browser.

Table 43: WBM Page "Administration"
**SD Card Settings**

<table>
<thead>
<tr>
<th>Eintrag</th>
<th>Standardwert</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable firmware boot from SD card</td>
<td>□</td>
<td>Enable the firmware boot from the inserted SD card. The firmware image must be stored on the SD card in the folder “S:\firmware\boot”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Disable the firmware boot from the inserted SD card</td>
</tr>
<tr>
<td>Enable firmware update from SD card</td>
<td>✓</td>
<td>Enable the firmware update from the inserted SD card. The firmware update must be stored on the SD card in the folder “S:\firmware\update”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Disable the firmware update from the inserted SD card</td>
</tr>
</tbody>
</table>

**Security Settings**

<table>
<thead>
<tr>
<th>Entry</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable web-server authentication</td>
<td>✓</td>
<td>Enable password protection to access the Web interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Disable password protection to access the Web interface</td>
</tr>
</tbody>
</table>

**User Settings**

<table>
<thead>
<tr>
<th>Entry</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>guest</td>
<td>Select user permissions according to the default user group (see Chapter “WBM User Groups”).</td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td>Enter desired password (max. 32 characters inclusive special characters).</td>
</tr>
<tr>
<td>Confirm Password</td>
<td></td>
<td>Enter desired password again to confirm.</td>
</tr>
</tbody>
</table>

* The following default groups exist:

User: admin Password: wago
User: user Password: user
User: guest Password: guest

**SSL Certificates**

<table>
<thead>
<tr>
<th>Entry</th>
<th>Button</th>
<th>Status (Example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server certificate incl. private key</td>
<td>[Durchsuchen ...]</td>
<td>D:\xyz.crt</td>
<td>Select the file with the server certificate and user key for secure Web server communication (HTTPS protocol). The server certificate must be in *pem, *.cer or *.crt format and contain the private key of the device.</td>
</tr>
<tr>
<td></td>
<td>[UPLOAD]</td>
<td>NO FILE</td>
<td>Load the selected SSL certificate onto the device.</td>
</tr>
<tr>
<td>Root certificate (CA)</td>
<td>[Durchsuchen ...]</td>
<td>D:\abc.pem</td>
<td>Select the file with the SSL root certificate. The root certificate must be in *pem, *.cer or *.crt format.</td>
</tr>
<tr>
<td></td>
<td>[UPLOAD]</td>
<td>NO FILE</td>
<td>Load the selected SSL root certificate onto the device.</td>
</tr>
<tr>
<td>Upload and installation status</td>
<td>-</td>
<td>Ready</td>
<td>Download and install status indicator</td>
</tr>
<tr>
<td>Button</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[INSTALL]</td>
<td>Installs the SSL server and/or root certificate previously loaded on the device and replaces the existing SSL certificates.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[DOWNLOAD]</td>
<td>Downloads the SSL root certificate stored in the device to the local PC.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[SOFTWARE RESET]</td>
<td>Restart the software.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9.6 Backup & Restore

On the “Backup & Restore" WBM page, you can back up and restore device data and settings.

Please consider the following remarks when using the backup and restore service:

- Ensure that any file transfer connection (FTP or SFTP) is closed, the PLC application is stopped and all engineering tools are disconnected.

- If necessary, the restore service automatically performs a software reset in order to adopt the restored configuration.

- The upload and download service is limited to the totally available memory of the device. If the upload and download service fails, please use the FTP or SFTP protocol instead.

The size information for the backup image file is specified in units of 1 kB = 1024 Byte.

Table 44: WBM Page „Backup & Restore”

<table>
<thead>
<tr>
<th>Service Control / Status Entry</th>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup device settings to internal disk/SD card</td>
<td>[BACKUP]</td>
<td>Creates a full backup image of the fieldbus controller on the selected backup media (SD card or internal disk). The current status and progress is displayed under “Status”.</td>
</tr>
<tr>
<td>Restore all device settings from internal disk/SD card</td>
<td>[RESTORE]</td>
<td>Restores all or part of a previously created backup image. During recovery, the options selected under &quot;Backup &amp; Restore Settings&quot; are taken into account. The current status and progress is displayed under &quot;Status&quot;.</td>
</tr>
<tr>
<td></td>
<td>[DOWNLOAD]</td>
<td>Downloads a previously created backup image to the local PC. The name of the downloaded file is structured according to the following scheme: backup_&lt;ARTICLE&gt;_ &lt;VERSION&gt;_ &lt;INDEX&gt;_ &lt;MAC&gt;.img &lt;ARTICLE&gt; = article number &lt;VERSION&gt; = firmware version &lt;INDEX&gt; = release index &lt;MAC&gt; = The last 3 digits of the MAC address (00-30-DE-xx-xx-xx) Example: &quot;backup_075008xx_010103_03_123456.img&quot;</td>
</tr>
<tr>
<td>Upload a backup image file</td>
<td>[Datei auswählen...]</td>
<td>Select a backup image saved on the local PC.</td>
</tr>
<tr>
<td></td>
<td>[UPLOAD]</td>
<td>Loads the selected backup image on the device.</td>
</tr>
</tbody>
</table>
### Status

<table>
<thead>
<tr>
<th>Entry</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>READY</td>
<td>Function ready for execution.</td>
<td></td>
</tr>
<tr>
<td>CHECK</td>
<td>Function is currently being executed. Required data is collected and checked.</td>
<td></td>
</tr>
<tr>
<td>RUN (x%)</td>
<td>The function is currently being executed and is x% complete.</td>
<td></td>
</tr>
<tr>
<td>DONE (100%)</td>
<td>Function successfully completed.</td>
<td></td>
</tr>
<tr>
<td>RESET…</td>
<td>The function is completed and the system is restarted automatically.</td>
<td></td>
</tr>
<tr>
<td>INVALID STATE</td>
<td>Function cannot be executed because the application is running or an active FTP connection to the fieldbus controller exists.</td>
<td></td>
</tr>
<tr>
<td>INVALID VERSION</td>
<td>The selected backup image is incompatible.</td>
<td></td>
</tr>
<tr>
<td>NO IMAGE</td>
<td>There is no backup image on the selected backup medium.</td>
<td></td>
</tr>
<tr>
<td>IMAGE BROKEN</td>
<td>The selected backup medium is defect.</td>
<td></td>
</tr>
<tr>
<td>NO DISK</td>
<td>The selected backup medium is not available.</td>
<td></td>
</tr>
<tr>
<td>NO DISK SPACE</td>
<td>There is insufficient storage space on the selected backup medium.</td>
<td></td>
</tr>
<tr>
<td>NO DISK ACCESS</td>
<td>The selected backup medium is write-protected.</td>
<td></td>
</tr>
<tr>
<td>ERROR(x)</td>
<td>Internal error x.</td>
<td></td>
</tr>
</tbody>
</table>

### Backup & Restore Settings

<table>
<thead>
<tr>
<th>Entry</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup storage:</td>
<td></td>
<td>Selection of the storage medium</td>
</tr>
<tr>
<td>Internal disk</td>
<td>☑️</td>
<td>The backup image is created on or loaded from the internal file system.</td>
</tr>
<tr>
<td>SD card</td>
<td>☑️</td>
<td>The backup image is created on or loaded from the memory card.</td>
</tr>
<tr>
<td>Automatic restore:</td>
<td></td>
<td>Selection of the automatic restore</td>
</tr>
<tr>
<td>Enable automatic restore from SD card</td>
<td>☑️</td>
<td>When you restart (power-on reset), a backup image on the memory card is automatically restored.</td>
</tr>
<tr>
<td></td>
<td>☐</td>
<td>When restarting, a normal system startup occurs without automatic recovery.</td>
</tr>
</tbody>
</table>
### Restore contents:

| Ethernet settings (embedded switch, MAC filter, bandwidth limitation, etc.) | ✓  The settings for the network interface of the fieldbus controller are restored. |
| Network configuration (IP address, host/domain name, DNS server, etc.) | ✓  The settings for the IP-based network parameters are restored. |
| Device configuration (password settings, clock/time-zone, local bus, etc.) | ✓  The settings for the general device configuration are restored. |
| Application protocols (field bus, SNMP, SNTP, etc.) | ✓  The settings for the TCP / IP-based application protocols are restored. |
| PLC (settings, folders, boot project, web-visu, etc.) | ✓  The settings for the runtime system and the boot project are restored. |
| SSL (device and root certificate, private key, etc.) | ✓  The settings for the SSL connections (devices/root certificate and private key) are restored. |
| Non-volatile memory (merker/retain memory) | ✓  The content of the NVRAM (flag / retain variable) is restored. |
| File system (internal file system contents) | ✓  The content of the internal file system is restored. |

| Auswahl der Inhalte für die Wiederherstellung. |  |  |
| --- |  |  |
| Ethernet settings (embedded switch, MAC filter, bandwidth limitation, etc.) | ☐ | ☐  The settings for the network interface of the fieldbus controller are not restored. |
| Network configuration (IP address, host/domain name, DNS server, etc.) | ☐ | ☐  The settings for the IP-based network parameters are not restored. |
| Device configuration (password settings, clock/time-zone, local bus, etc.) | ☑ | ☐  The general device configuration settings are not restored. |
| Application protocols (field bus, SNMP, SNTP, etc.) | ☐ | ☐  The settings for the TCP / IP-based application protocols are not restored. |
| PLC (settings, folders, boot project, web-visu, etc.) | ☐ | ☐  The settings for the runtime system and the boot project are not restored. |
| SSL (device and root certificate, private key, etc.) | ☐ | ☐  The settings for the SSL connections (devices/root certificate and private key) are not restored. |
| Non-volatile memory (merker/retain memory) | ☐ | ☐  The content of the NVRAM (flag / retain variable) is not restored. |
| File system (internal file system contents) | ☐ | ☐  The content of the internal file system is not restored. |
On the WBM "Clock" page, you make settings for the internal real-time clock. Enter the current time and date here and select a time zone deviation, 12h or 24h display and automatic daylight saving time as required.

**Note**

Reset the internal clock after a longer time without power supply!
The internal clock must be reset on initial startup or after the end of days, specified in the technical Data without power supply (Powerfail RTC Buffer). If the clock is not set, the clock starts with the date 01.01.2000 around 0:00 clock with time measurement.

**Note**

Error message in WAGO I/O CHECK is possible after a power failure!
If you are using the software "WAGO-I/O-CHECK" after a loss of power has occurred, error messages may be generated. Should this occur, call up the Web-based management system and set the actual time under "Clock". Then, call up the "WAGO-I/O-CHECK" program again.

**Note**

Loss of telegrams possible when performing configuration during ongoing operation!
Telegrams may be lost if configuration is performed using WAGO-I/O-CHECK while the system is in operation.

**Note**

Use a WAGO RTC module for time synchronization!!
You can use a WAGO 750-640 RTC Module for your node to utilize the actual encoded time (Real-time – RTC) in your higher-level control system.
### Table 45: WBM Page „Clock“

<table>
<thead>
<tr>
<th>Clock Settings</th>
<th>Entry</th>
<th>Default</th>
<th>Value (example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device local time</td>
<td>(HH:MM:SS)</td>
<td>00:00:00</td>
<td>08:30:38</td>
<td>Set current time</td>
</tr>
<tr>
<td>Device local date</td>
<td>(YYYY-MM-DD)</td>
<td>2000-01-01</td>
<td>2018-07-19</td>
<td>Set current date</td>
</tr>
<tr>
<td>Device time zone</td>
<td>(+/- HH:MM)</td>
<td>0:00</td>
<td>+1:00</td>
<td>Set time zone offset from the Coordinated Universal Time (UTC)</td>
</tr>
<tr>
<td>Time display mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>24h</td>
<td></td>
<td></td>
<td>Enable 24-hour display</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Disable 24-hour display</td>
</tr>
<tr>
<td></td>
<td>12h (AM/PM)</td>
<td></td>
<td></td>
<td>Enable 12-hour display</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Disable 12-hour display</td>
</tr>
<tr>
<td>Automatic daylight</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>saving time (DST)</td>
<td>EU</td>
<td></td>
<td></td>
<td>Enable automatic Daylight Saving Time (EU)</td>
</tr>
<tr>
<td></td>
<td>(last Sunday in March, clocks are</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>advanced from 02:00 AM to 03:00 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>and last Sunday in October, clocks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>are set back from 03:00 AM to 02:00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AM)</td>
<td></td>
<td></td>
<td>Disable automatic Daylight Saving Time (EU)</td>
</tr>
<tr>
<td></td>
<td>US</td>
<td></td>
<td></td>
<td>Enable automatic Daylight Saving Time (US)</td>
</tr>
<tr>
<td></td>
<td>(second Sunday in March, clocks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>are advanced from 02:00 AM to 03:00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AM)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AU</td>
<td></td>
<td></td>
<td>Enable automatic Daylight Saving Time (AU)</td>
</tr>
<tr>
<td></td>
<td>(first Sunday in October, clocks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>are advanced from 02:00 AM to 03:00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AM)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Disable automatic Daylight Saving Time (AU)</td>
</tr>
<tr>
<td>DST current status</td>
<td>not active</td>
<td></td>
<td>not active</td>
<td>Status display for the current DST status</td>
</tr>
</tbody>
</table>
9.8 Miscellaneous

On the Miscellaneous WBM page, you can set configuration options for various features and compatibility options.

These configuration options are stored in non-volatile memory when the [SUBMIT] button is pressed. Changes to the configuration options take effect after the next power-on cycle or software reset.

Table 46: WBM Page “Miscellaneous”

<table>
<thead>
<tr>
<th>Entry</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoreset on fatal error</td>
<td></td>
<td>○ Enables an automatic software reset to be conducted when a system error occurs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Disables an automatic software reset to be conducted when a system error occurs</td>
</tr>
</tbody>
</table>
| BootP request before static IP|         | ○ Automatically set the static IP address enabled. For this configuration, the fieldbus coupler/controller uses a statically configured IP address if the request via BootP fails. This process can take a few minutes. With the setting “DHCP” this function has no effect.
|                              |         | ○ Automatically set the static IP address disabled. For this configuration, the IP address request via BootP is repeated in the event of error. |
| Non-adaptive local bus interval |         | ○ Enables a fixed sampling interval of the local bus and statically sets the pause time to 14 ms. As a result, possibly the sampling interval of the local bus is extended and more computing power is available for the PLC application. |
|                              |         | ○ Enables the dynamic sampling interval of the local bus (default). The pause time between two local bus cycles is dynamically adjusted. This shortens the sampling interval of the local bus and less computing power is available for the PLC application. |
| Local bus extension installed |         | ○ Indicates, that the bus extension (750-627/-628) is installed. |
|                              |         | ○ Indicates, that no bus extension is installed. |
9.9 SD Card

On the “SD Card” WBM page, you can find information about the memory card used, as well as delete the content of the “PLC” folder on the memory card or create and copy it on the internal memory.

Table 47: WBM Page “SD Card”

<table>
<thead>
<tr>
<th>SD Card Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry</td>
</tr>
<tr>
<td>Serial number</td>
</tr>
<tr>
<td>Volume name</td>
</tr>
<tr>
<td>Free card space</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SD Card Folders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry</td>
</tr>
<tr>
<td>Create/delete PLC root folder 'S:\plc'</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Copy PLC root folder 'S:\plc' to 'A:\plc'</td>
</tr>
</tbody>
</table>

9.10 Storage Media

Information about the available storage devices and active drives which are currently mounted within the file system of the device is given on the “Storage Media” WBM page.

This page will be refreshed every 5 s.

This size information for the storage devices listed below are specified in units of 1 kB with 1 kB = 1024 Byte.
Table 48: WBM page "Storage Media"

<table>
<thead>
<tr>
<th>Local Disks</th>
<th>Value (Example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drive Letter</td>
<td>A</td>
<td>A: internal memory</td>
</tr>
<tr>
<td></td>
<td>S</td>
<td>S: memory card</td>
</tr>
<tr>
<td>Total Size [kB]</td>
<td>1050184 kB</td>
<td>Total size of the file system</td>
</tr>
<tr>
<td>Used Size [kB]</td>
<td>295560 kB</td>
<td>Used memory capacity</td>
</tr>
<tr>
<td>Free Size [kB]</td>
<td>754624 kB</td>
<td>Free memory capacity</td>
</tr>
<tr>
<td>File System</td>
<td>FAT</td>
<td>File system (File Allocation Table)</td>
</tr>
</tbody>
</table>

9.11 Update

Use the "Update" WBM page to update the firmware of the device. To do this, the associated firmware image is first selected from the PC's local file system and downloaded to the device. Afterwards, the update will be executed and the device will be restarted automatically. After the firmware update, the WBM pages will also be updated, self-created HTML pages or settings will be remained save.

Note

Stop fieldbus application and finish FTP connections before the update! Please ensure, that the superordinate fieldbus application has been stopped and possibly existing FTP connections has been finished before starting the update process. When the software reset is being executed, the connection to the web-based management will be lost and the web-page has to be reloaded.

Table 49: WBM Page "Update"

<table>
<thead>
<tr>
<th>Firmware Selection / Upload</th>
<th>Button</th>
<th>Value (example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firmware image</td>
<td>[Durchsuchen...]</td>
<td>firmware.bin</td>
<td>Use this button to select the firmware image file on your local file system (PC).</td>
</tr>
<tr>
<td></td>
<td>[UPLOAD]</td>
<td>OK</td>
<td>This button loads the previously selected firmware image file from your local file system to the device.</td>
</tr>
<tr>
<td>Update Status</td>
<td>-</td>
<td>Verification of firmware image is done</td>
<td>Status display for the update.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[RESET]</td>
<td>Resetting the upload status (e.g. when selecting a wrong image file).</td>
</tr>
<tr>
<td>[UPDATE]</td>
<td>With this button you start the update process. The firmware image file previously loaded on the device is first checked and then installed. Afterwards an automatic restart of the device takes place.</td>
</tr>
</tbody>
</table>
9.12 Ethernet

Use the “Ethernet” WBM page to set the data transfer rate, the MAC address filter settings and bandwidth limit for each of the two switch ports for data transfer via Ethernet.

Table 50: WBM Page „Ethernet“

<table>
<thead>
<tr>
<th>PHY Settings</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable port</td>
<td>✔️</td>
<td>✔️ Enable Port X1/Port X2&lt;br&gt; □ Disable Port X1/Port X2</td>
</tr>
<tr>
<td>Enable auto-negotiation</td>
<td>☑</td>
<td>☑ Enable Autonegotiation for Port X1/Port X2. Automatically handling the best possible transmission mode and baud rate with the communication partner. □ Enable Autonegotiation for Port X1/Port X2.</td>
</tr>
<tr>
<td>10 MBit Half Duplex</td>
<td>☑</td>
<td>Use a fixed transmission mode and baud rate for Port X1/Port X2.</td>
</tr>
<tr>
<td>10 MBit Full Duplex</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>100 MBit Half Duplex</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>100 MBit Full Duplex</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Entry</td>
<td>Default value</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable filter</td>
<td></td>
<td>☑ Activate MAC address filter. Depending on the operating mode of the MAC address filter (whitelist / blacklist), the subsequently entered MAC addresses are blocked or permitted. ☐ Deactivate MAC address filter.</td>
</tr>
<tr>
<td>Filter mode</td>
<td></td>
<td>☑ Chose Whitelist. Only the following registered MAC addresses have network access to the fieldbus coupler/controller, others are blocked. ☐ Chose Blacklist. Only the following registered MAC addresses are blocked, others have network access to the fieldbus coupler/controller.</td>
</tr>
<tr>
<td>Allow WAGO devices</td>
<td></td>
<td>☑ Activate MAC address filter. The WAGO devices with the MAC address 00:30:EN:XX:XX:XX always have network access to the fieldbus coupler/controller, independent of the other settings of the MAC address filter. ☐ Deactivate MAC address filter. Only devices whose MAC address is entered in the list have network access to the fieldbus coupler / controller. The settings of the MAC address filter apply.</td>
</tr>
<tr>
<td>MAC address 1</td>
<td>00:00:00:00:00:00</td>
<td>Filter for the first MAC address (hexadecimal).</td>
</tr>
<tr>
<td>MAC address 2</td>
<td>00:00:00:00:00:00</td>
<td>Filter for the second MAC address (hexadecimal).</td>
</tr>
<tr>
<td>MAC address 3</td>
<td>00:00:00:00:00:00</td>
<td>Filter for the third MAC address (hexadecimal).</td>
</tr>
<tr>
<td>MAC address 4</td>
<td>00:00:00:00:00:00</td>
<td>Filter for the fourth MAC address (hexadecimal).</td>
</tr>
<tr>
<td>MAC address 5</td>
<td>00:00:00:00:00:00</td>
<td>Filter for the fifth MAC address (hexadecimal).</td>
</tr>
</tbody>
</table>
## Switch Settings

<table>
<thead>
<tr>
<th>Entry</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable fast aging</td>
<td></td>
<td>☑ Enable “Fast Aging”&lt;br&gt;“Fast Aging” ensures that the cache for the MAC addresses is cleared faster in the switch. This may be required if a redundancy system (e.g., using a Jet-Ring network or comparable technology) needs to be set up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>☐ Disable “Fast Aging”.&lt;br&gt;The time to discard the cache entries is five minutes.</td>
</tr>
<tr>
<td>Enable port mirroring</td>
<td></td>
<td>☑ Enable port mirroring&lt;br&gt;Port Mirroring is used for network diagnostics. Packets are mirrored from one port (mirror port) to another (sniffer port).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>☐ Disable port mirroring</td>
</tr>
<tr>
<td>Ethernet MTU</td>
<td>1500</td>
<td>Maximum packet size of a protocol, which can be transferred without fragmentation (“Maximum Transmission Unit” - MTU).</td>
</tr>
</tbody>
</table>

### Port

<table>
<thead>
<tr>
<th>Port</th>
<th>1</th>
<th>2</th>
<th>Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input data rate limit</td>
<td>No limit</td>
<td>The input limit rate limits network traffic when receiving. The rate is indicated in megabits or kilobits per second. If the limit is exceeded, packets are lost.</td>
<td></td>
</tr>
<tr>
<td>Output data rate limit</td>
<td>No limit</td>
<td>The output limit rate limits network traffic when sending. The rate is indicated in megabits or kilobits per second. If the limit is exceeded, packets are lost.</td>
<td></td>
</tr>
<tr>
<td>Enable broadcast storm protection</td>
<td>☐ ☐</td>
<td>☑ Activate broadcast storm protection. The maximum number of incoming broadcast telegrams is limited and packets affected by the limitation are discarded.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>☐ Broadcast storm protection disabled.</td>
<td></td>
</tr>
<tr>
<td>Sniffer Port</td>
<td>☐ ☒</td>
<td>Select the sniffer port the mirror port should be mirrored to.</td>
<td></td>
</tr>
<tr>
<td>Mirror Port</td>
<td>☒ ☒ ☒</td>
<td>Select the mirror port which should be mirrored to the sniffer port.</td>
<td></td>
</tr>
</tbody>
</table>

---

**Note**

Set the MTU value for fragmentation only!<br>Only set the value for MTU, i.e., the maximum packet size between client and server, if you are using a tunnel protocol (e.g., 1452 for VPN) for ETHERNET communication and the packets must be fragmented. Setting the value is independent of the transmission mode selected.

---

**Note**

Configure ETHERNET transmission mode correctly!<br>A fault configuration of the ETHERNET transmission mode may result in a lost connection, poor network performance or faulty performance of the fieldbus coupler/controller.
Note

All ETHERNET ports cannot be disabled!
Both ETHERNET ports can be switched off. If both ports are disabled and you press [SUBMIT], the selection is not applied and the previous values are restored.
9.13 Protocols

Use the "Protocols" WBM page to enable or disable ports for the services available.

**Note**

**Close any ports and services that you do not need!**

Unauthorized persons may gain access to your automation system through open ports.

To reduce the risk of cyber attacks and, thus, enhance your cyber security, close all ports and services in the control components (e.g., Port 6626 for WAGO I/O-CHECK, Port 2455 for CODESYS 2 and Port 11740 for e!COCKPIT) not required by your application.

Only open ports and services during commissioning and/or configuration.

<table>
<thead>
<tr>
<th>Table 51: WBM page „Protocols“</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol Settings</strong></td>
</tr>
<tr>
<td><strong>Entry</strong></td>
</tr>
<tr>
<td>FTP (Port 21)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>SFTP (Port 22)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>HTTP (Port __ )</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>HTTPS (Port 443)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>SNTP (Port 123)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>SNMP (Port 161, 162)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Modbus UDP (Port 502)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Modbus TCP (Port 502)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>WAGO service protocol (Port 6626)</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
9.14 SNMP

On the HTML pages „SNMP“, you can perform the settings for the Simple Network Management Protocol (SNMP v1/v2c and v3).

SNMP is a standard for device management within a TCP/IP network. The Simple Network Management Protocol (SNMP) is responsible for transporting the control data that allows the exchange of management information, the status and statistic data between individual network components and a management system.

The fieldbus coupler supports SNMP in versions 1, 2c and 3.

The SNMP of the ETHERNET TCP/IP coupler includes the general MIB according to RFC1213 (MIB II).

SNMP is processed via port 161. The port number for SNMP traps (agent messages) is 162.

---

**Note**

Enable port 161 and 162 to use SNMP!
Enable ports 161 and 162 in the WBM in menu “port”, so that the fieldbus coupler can be reached via SNMP. The port numbers cannot be modified.

---

**Note**

Modify parameter via WBM or SNMP objects!
However, parameters that can be set on the WBM pages can also be changed directly by the appropriate SNMP objects.

---

**Information**

Additional Information:
Additional information for SNMP, the Management Information Base (MIB) and traps (event messages via SNMP) may be obtained from section "Fieldbus Communication" > … > “SNMP (Simple Network Management Protocol).”

Note that the settings for SNMPV1/V2c and SNMPV3 are separate from each other. The different SNMP versions can be activated or used in parallel or individually on a fieldbus coupler.
9.14.1 SNMP v1/v2c

The SNMP version 1/2c represents a community message exchange. The community name of the network community must thereby be specified.

Table 52: WBM Page “SNMP v1/v2”

<table>
<thead>
<tr>
<th>SNMP Settings</th>
<th>Value (Default)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>FC_BACnet/IP_G4</td>
<td>Device description (sysDescription)</td>
</tr>
<tr>
<td>Physical location</td>
<td>LOCAL</td>
<td>Location of device (sysLocation)</td>
</tr>
<tr>
<td>Contact address</td>
<td><a href="mailto:support@wago.com">support@wago.com</a></td>
<td>E-mail contact address (sysContact)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SNMP v1/v2c Manager Settings</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable protocol</td>
<td>☑</td>
<td>Activating SNMP Version 1/2c</td>
</tr>
<tr>
<td>Local community name</td>
<td>public</td>
<td>used community name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SNMP v1/v2c Trap Receiver 1 Settings</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap receiver</td>
<td>0.0.0.0</td>
<td>IP address of 1. used SNMP manager</td>
</tr>
<tr>
<td>Community name</td>
<td>public</td>
<td>1. Community name of the network community used</td>
</tr>
<tr>
<td>Trap version</td>
<td>v1 v2</td>
<td>v1 v2</td>
</tr>
<tr>
<td></td>
<td>v1 v2</td>
<td>v1 v2</td>
</tr>
<tr>
<td></td>
<td>v1 v2</td>
<td>Activating Traps Version 1</td>
</tr>
<tr>
<td></td>
<td>v1 v2</td>
<td>Activating Traps Version 2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SNMP v1/v2c Trap Receiver 2 Settings</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap receiver</td>
<td>0.0.0.0</td>
<td>IP address of 2. used SNMP manager</td>
</tr>
<tr>
<td>Community name</td>
<td>public</td>
<td>2. Community name of the network community used</td>
</tr>
<tr>
<td>Trap version</td>
<td>v1 v2</td>
<td>v1 v2</td>
</tr>
<tr>
<td></td>
<td>v1 v2</td>
<td>v1 v2</td>
</tr>
<tr>
<td></td>
<td>v1 v2</td>
<td>Activating Traps Version 1</td>
</tr>
<tr>
<td></td>
<td>v1 v2</td>
<td>Activating Traps Version 2</td>
</tr>
</tbody>
</table>
### 9.14.2 SNMP V3

In SNMP version 3, exchanging messages is user-related. Each device, that knows the passwords set via WBM, may read or write values from the fieldbus coupler.

In SNMP v3, user data from SNMP messages can also be transmitted in encoded form. This is why SNMP v3 is often used in safety-related networks.

Via this WBM page "SNMP V3" two independent SNMPV3 users can be defined and activated (User 1 and User 2).

<table>
<thead>
<tr>
<th>Table 53: WBM Page &quot;SNMP V3&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNMP v3 User 1 / 2 Settings</strong></td>
</tr>
<tr>
<td><strong>Entry</strong></td>
</tr>
</tbody>
</table>
| Enable user | activate | ✓ Activating user 1 or 2
| | | □ Deactivating user 1 or 2 |
| Authentication type | None | MD5
| | | SHA1 |
| | | None
| | | | No encryption of the authentication
| | | MD5 | Encryption of the authentication with MD5
| | | SHA1 | Encryption of the authentication with SHA1
| Authentication name | Security Name | Enter the name, if the "Authentication type" MD5 or SHA1 has been selected
| Authentication key (min. 8 characters) | Authentication Key | Enter the password with at least 8 characters, if "Authentication type" MD5 or SHA1 has been selected
| Privacy enable (DES) | | ✓ Activate the DES encryption of the data
| | | □ Deactivate the DES encryption of the data
| Privacy key (min. 8 characters) | Privacy Key | Enter the password of at least 8 characters in the encryption with DES
| Enable v3 notification/trap enable | | ✓ Activate the notification traps of the SNMP version 3
| | | □ Deactivate the notification traps of the SNMP version 3
| Notification receiver (IP address) | 192.168.1.10 | IP address of the notification manager
9.15 SNTP

On the WBM page “SNTP”, you can perform the settings for the “Simple Network Time Protocol”.

The SNTP client supports configuration of static time servers. Two additional servers may be assigned by dynamic network configuration (e.g. DHCP or BootP). The selection of the active time server used to synchronize the current time is done automatically by the SNTP client. The SNTP client queries all time servers listed below and determines the most precise server to synchronize the device clock with. This takes into account whether the respective time server can be reached and how short the transmission distance between the time server and the SNTP client is.

Table 54: WBM Page “SNTP”

<table>
<thead>
<tr>
<th>SNMP Settings</th>
<th>Value (Example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol status</td>
<td>enabled</td>
<td>Display the protocol status. .enabled” SNTP protocol is activated. .disabled” SNTP protocol is deactivated.</td>
</tr>
<tr>
<td>Active time server</td>
<td>de.pool.ntp.org</td>
<td>Hostname or IP address of the active time server, which is currently used to synchronize the time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SNTP Client Settings</th>
<th>Value (Example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server update interval [s] (60 ... 65535 s)</td>
<td>3600</td>
<td>Polling interval for synchronizing the device clock with the active time server.</td>
</tr>
<tr>
<td>First time server</td>
<td>de.pool.ntp.org</td>
<td>Host name or IP address of the first user-defined time server.</td>
</tr>
<tr>
<td>Second time server</td>
<td>0.0.0.0</td>
<td>Host name or IP address of the second user-defined time server.</td>
</tr>
<tr>
<td>Additional time servers</td>
<td>-</td>
<td>List of up to 2 time servers dynamically allocated via BootP or DHCP.</td>
</tr>
</tbody>
</table>
9.16 TCP/IP

You can configure network addressing and network identification on the “TCP/IP” WBM page.

**Note**

Set the DIP switch to “0” and enable static IP configuration source!
Before you change parameters on this page, set the DIP switch to value “0” and enable the option “IP configuration source static”!
If these conditions are not met, the DIP switch settings are applied instead.

<table>
<thead>
<tr>
<th>Tabelle 55: WBM-Seite „TCP/IP“</th>
<th>Eintrag</th>
<th>Standardwert</th>
<th>Wert (Beispiel)</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>○ static</td>
<td>○</td>
<td></td>
<td>○ Use IP address from EEPROM. ○ Do not use IP address from EEPROM.</td>
</tr>
<tr>
<td></td>
<td><strong>IP address</strong></td>
<td>0.0.0.0</td>
<td>192.168.1.180</td>
<td>Enter IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>Subnet mask</strong></td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>Enter subnet mask.</td>
</tr>
<tr>
<td></td>
<td><strong>Default gateway</strong></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Enter gateway.</td>
</tr>
<tr>
<td></td>
<td><strong>Host name</strong></td>
<td>0030DEXXXX XX</td>
<td>0030DE000000</td>
<td>Enter host name.</td>
</tr>
<tr>
<td></td>
<td><strong>Domain name</strong></td>
<td></td>
<td></td>
<td>Enter domain name.</td>
</tr>
<tr>
<td></td>
<td><strong>DNS server 1</strong></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Enter IP address of the first DNS server.</td>
</tr>
<tr>
<td></td>
<td><strong>DNS server 2</strong></td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Enter optional IP address of the second DNS server.</td>
</tr>
<tr>
<td></td>
<td><strong>DIP switch base IP address</strong></td>
<td>192.168.1</td>
<td>192.168.5</td>
<td>Network address for the configuration of the IP address with DIP switch.</td>
</tr>
<tr>
<td></td>
<td><strong>IP Fragment TTL [s]</strong> (max. 255)</td>
<td>60</td>
<td>60</td>
<td>Life of a packet (Time to Live).</td>
</tr>
</tbody>
</table>
## 9.17 BACnet

On the “BACnet” page, make the BACnet-specific settings, e.g., enable/disable BACnet communication or select the respective UDP port.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Entry</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable BACnet fieldbus</td>
<td>☐</td>
<td></td>
<td>The BACnet fieldbus is disabled. BACnet communication is no longer possible. BACnet-specific blinking codes are no longer displayed.</td>
</tr>
<tr>
<td>UDP Port</td>
<td>47808</td>
<td></td>
<td>UDP port for the BACnet/IP protocol</td>
</tr>
<tr>
<td>Who-Is online interval (seconds)</td>
<td>60</td>
<td></td>
<td>Minimum time interval between two “Who-Is” queries of a fieldbus coupler for online identification of the communication partner.</td>
</tr>
<tr>
<td>Save trendlog files on removable disk</td>
<td>☐</td>
<td></td>
<td>Save trendlog file to SD card</td>
</tr>
<tr>
<td>Save trendlog file to internal flash</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default character set</td>
<td>☑ UTF-8 ☑ UCS-2</td>
<td></td>
<td>Switching the character set used for BACnet-based strings between UTF-8 encoding (default setting) and UCS-2 encoding.</td>
</tr>
</tbody>
</table>

---

**Note**

**Network number entry not necessary for WAGO BACnet Couplers!**

A BACnet network number is used to enable a BACnet router to forward messages from one BACnet network to another. The network number is not used for communication between devices in the same network. The network numbers of devices from other networks are automatically identified by the WAGO BACnet Coupler and used for communication. For this reason, the network number cannot be set on WAGO BACnet couplers. This only has to be set on the BACnet router used.

---

**Recommendation: Use UTF-8 encoding!**

It is recommended to keep the UTF-8 encoding as long as there is no known incompatibility with other devices of the control technology in the system.
9.18 BACnet Information

The WBM page "BACnet Information" provides you with statistical information about the BACnet fieldbus. It displays values of the BACnet application, such as the number of bytes and PDUs sent and received by the client and server, and statistics about the Transaction State Machine of the client and server.

Table 57: WBM page „BACnet Information“

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Refresh]</td>
<td>Update the values.</td>
</tr>
<tr>
<td>[Reset Counter]</td>
<td>Reset the values.</td>
</tr>
</tbody>
</table>

**Application Statistics**

<table>
<thead>
<tr>
<th>Entry</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client: Bytes received</td>
<td>0</td>
<td>Values of the client.</td>
</tr>
<tr>
<td>Client: Bytes sent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client: PDUs received</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client: PDUs sent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client: Number of transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client: Aborted transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client: Total retries</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Client: Timed-out transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client: Total segmented retries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client: Timed-out segmented transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client: Timed-out segmented confirmed transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: Bytes received</td>
<td>0</td>
<td>Values of the server.</td>
</tr>
<tr>
<td>Server: Bytes sent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: PDUs received</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: PDUs sent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: Number of transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: Aborted transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: Timed-out transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: Timed-out transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: Total segmented requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: Total segmented response retries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: Total segmented responses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: Timed-out segmented responses</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Transaction State Machine Statistics

<table>
<thead>
<tr>
<th>Entry</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client: Total transaction state machines</td>
<td>128</td>
<td>Values of the client.</td>
</tr>
<tr>
<td>Client: Free transaction state machines</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client: Idle transaction state machines</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client: Waiting for segment ACK</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Client: Waiting for response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client: Waiting for segment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: Total transaction state machines</td>
<td>128</td>
<td>Values of the server.</td>
</tr>
<tr>
<td>Server: Free transaction state machines</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: Idle transaction state machines</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: Waiting for segment</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Server: Waiting for response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server: Waiting for segment ACK</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9.19 MODBUS

Use the “MODBUS” WBM page to specify the settings for the Modbus protocol.

Table 58: WBM page “MODBUS”

<table>
<thead>
<tr>
<th>Modbus UDP Multicast Address Setup</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable multicast addressing</td>
<td>☐</td>
<td>☑ Enable Multicast for Modbus UDP transmission. In addition to its own IP address, the fieldbus coupler receives Modbus commands for the following registered MCAST addresses. ☐ Multicast for Modbus UDP transmission is not enabled. The fieldbus coupler receives Modbus commands only for the own IP address.</td>
</tr>
<tr>
<td>Do not reply to Modbus UDP multicast messages</td>
<td>☐</td>
<td>☑ The reply to Modbus UDP multicast messages is deactivated. ☐ The reply to Modbus UDP multicast messages is activated.</td>
</tr>
<tr>
<td>MCAST address 1 ... 5:</td>
<td>0.0.0.0</td>
<td>Multicast address 1... 5, for the multicast will be enabled. The valid address range is shown in the WBM. Multiple assigned addresses are not valid.</td>
</tr>
</tbody>
</table>

Note

Multicast function only active with a valid MCAST address!
The multicast function is only active with a valid MCAST address.
If you activate the “Enable Multicast” function, it is therefore necessary to always enter an MCAST address that is not equal to 0.0.0.0. Otherwise, clicking on the [SUBMIT] button automatically deactivates the function again.
If the “Enable Multicast” function is already enabled with valid addresses, then you can no longer describe these MCAST address fields with invalid addresses, because when clicking on the [SUBMIT] button, they are reset to the previously valid addresses. The function “Enable Multicast” remains active.

<table>
<thead>
<tr>
<th>Modbus Configuration Registers</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x1029 – 0x1037</td>
<td>Enabled</td>
<td>☑ Enable Modbus configuration register range. ☐ Disable Modbus configuration register range.</td>
</tr>
<tr>
<td>0x2040 – 0x2043</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Connection Watchdog

<table>
<thead>
<tr>
<th>Entry</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection timeout value (x 100 ms)</td>
<td>600</td>
<td>Monitoring period for TCP links. After the completion of this period without any subsequent data traffic, the TCP connection is closed.</td>
</tr>
</tbody>
</table>

## Modbus Watchdog

<table>
<thead>
<tr>
<th>Entry</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status of Modbus watchdog</td>
<td>disabled</td>
<td>“disabled” – Watchdog is disabled [running] – Watchdog is activated, Timeout monitoring is running [expired] – Watchdog is activated, Timeout occurred</td>
</tr>
<tr>
<td>Watchdog type</td>
<td>Standard</td>
<td>The watchdog can only be activated for the first time by writing to register 0x1001 or 0x1003.</td>
</tr>
<tr>
<td></td>
<td>Alternative</td>
<td>The watchdog is activated for the first time with each function code that is enabled in the coding mask (watchdog trigger mask).</td>
</tr>
<tr>
<td>Watchdog timeout value (x 100 ms)</td>
<td>100</td>
<td>Monitoring period for Modbus links. After the completion of this period without receiving a Modbus telegram, the physical outputs are set to &quot;0&quot;.</td>
</tr>
<tr>
<td>Watchdog trigger mask (FC1 to FC16)</td>
<td>0xFFFF</td>
<td>Coding mask for certain Modbus telegrams (Function Code FC1 ... FC16)</td>
</tr>
<tr>
<td>Watchdog trigger mask (FC17 to FC32)</td>
<td>0xFFFF</td>
<td>Coding mask for certain Modbus telegrams (Function Code FC17 ... FC32)</td>
</tr>
</tbody>
</table>
9.20 I/O Config

Click the link “I/O config” to view the number of modules that are connected to your hardware.

The data in the second line are not relevant for the present fieldbus coupler, because no I/O configuration will be load onto devices which have no runtime system (PLC). Therefore you always find the value “0” for the number of modules in the I/O configuration.

Table 59: WBM page „I/O Data“

<table>
<thead>
<tr>
<th>Configuration summary</th>
<th>Value (Example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of modules on terminal bus</td>
<td>6</td>
<td>Number of I/O modules (hardware)</td>
</tr>
<tr>
<td>Number of modules in I/O configuration</td>
<td>0</td>
<td>Number of I/O modules in the I/O configuration (not relevant).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[SAVE CONFIG]</td>
<td>With this button, the current status of the I/O configuration on the local bus is read in, displayed and stored on the device.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I/O Mapping</th>
<th>Entry</th>
<th>Value (Example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position</td>
<td>1</td>
<td>Position of the I/O module in the hardware</td>
<td></td>
</tr>
<tr>
<td>Module</td>
<td>750-5xx M001Ch1 M001Ch2</td>
<td>Product number of the integrated I/O module</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>8DO</td>
<td>I/O module type, e.g. 8DO (8 Channel Digital Output Module)</td>
<td></td>
</tr>
<tr>
<td>Assigned Fieldbus</td>
<td>Fieldbus 1</td>
<td>Mapping via fieldbus 1</td>
<td></td>
</tr>
</tbody>
</table>
10 Diagnostics

10.1 LED Signaling

For on-site diagnostics, the fieldbus coupler has several LEDs that indicate the operational status of the fieldbus coupler or the entire node (see following figure).

![Figure 49: Display Elements](image)

The diagnostics displays and their significance are explained in detail in the following section.

The LEDs are assigned in groups to the various diagnostics areas:

<table>
<thead>
<tr>
<th>Diagnostics area</th>
<th>LEDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fieldbus status</td>
<td>• LNK ACT 1</td>
</tr>
<tr>
<td></td>
<td>• LNK ACT 2</td>
</tr>
<tr>
<td></td>
<td>• MS/BT</td>
</tr>
<tr>
<td></td>
<td>• NS</td>
</tr>
<tr>
<td>Node status</td>
<td>• I/O</td>
</tr>
<tr>
<td>SD memory card status</td>
<td>• SD</td>
</tr>
<tr>
<td>Status Supply Voltage</td>
<td>• A (system supply)</td>
</tr>
<tr>
<td></td>
<td>• B (field supply)</td>
</tr>
</tbody>
</table>
10.1.1 Evaluating Fieldbus Status

The health of the ETHERNET Fieldbus is signaled through the top LED group (‘LNK ACT 1, 2’, ‘MS/BT’, und ‘NS’).

The two-colored LEDs ‘MS/BT’ (module status/BACnet) and ‘NS’ (network status) are used to display the status of the system and the fieldbus connections.

### Table 61: Fieldbus Diagnostics – Solution in Event of Error

<table>
<thead>
<tr>
<th>LED Status</th>
<th>Meaning</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>green</td>
<td>The fieldbus node is connected to the physical network.</td>
<td>-</td>
</tr>
<tr>
<td>green flashing</td>
<td>The fieldbus node sends and receives Ethernet telegrams</td>
<td>-</td>
</tr>
<tr>
<td>off</td>
<td>The fieldbus node is not connected to the physical network.</td>
<td>1. Check the fieldbus cable.</td>
</tr>
<tr>
<td>MS/BT</td>
<td>Network initialization completed, BACnet stack started. The fieldbus coupler is ready for BACnet data traffic.</td>
<td>-</td>
</tr>
<tr>
<td>green</td>
<td>Initialization of network and BACnet functions in progress.</td>
<td>1. Wait until initialization has been completed.</td>
</tr>
<tr>
<td>red</td>
<td>The system indicates a not remediable error</td>
<td>1. Restart the device by turning the power supply off and on again. 2. If the error still exists, please contact the I/O support.</td>
</tr>
<tr>
<td>red flashing</td>
<td>Error during initialization of the BACnet stack</td>
<td>1. Correct the BACnet configuration</td>
</tr>
<tr>
<td>off</td>
<td>No system supply voltage</td>
<td>1. Check the supply voltage.</td>
</tr>
<tr>
<td>NS</td>
<td>At least one Modbus TCP connection is developed.</td>
<td>-</td>
</tr>
<tr>
<td>grün flashing</td>
<td>No Modbus TCP connection.</td>
<td>-</td>
</tr>
<tr>
<td>red</td>
<td>The system indicates a double IP-address in the network</td>
<td>1. Use an IP address that is not used yet.</td>
</tr>
<tr>
<td>red flashing</td>
<td>At least one Modbus TCP connection announced a Timeout, where the controller functions as target.</td>
<td>1. Restart the device by turning the power supply off and on again. 2. Develop a new connection.</td>
</tr>
<tr>
<td>red/green flashing</td>
<td>Self test</td>
<td>-</td>
</tr>
<tr>
<td>off</td>
<td>No IP address is assigned to the system.</td>
<td>1. Assign to the system an IP address by BootP, DHCP or the Ethernet Settings tool.</td>
</tr>
</tbody>
</table>
10.1.2 Evaluating Node Status – I/O LED (Blink Code Table)

The communication status between fieldbus coupler/controller and the I/O modules is indicated by the I/O LED.

<table>
<thead>
<tr>
<th>LED Status I/O</th>
<th>Meaning</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>green</td>
<td>The fieldbus node is operating correctly.</td>
<td>Normal operation.</td>
</tr>
<tr>
<td>orange flashing</td>
<td>Start of the firmware. 1 ... 2 seconds of rapid flashing indicates start-up.</td>
<td>-</td>
</tr>
<tr>
<td>red</td>
<td>Fieldbus coupler/controller hardware defect</td>
<td>Replace the fieldbus coupler/controller.</td>
</tr>
<tr>
<td>red flashing</td>
<td>Flashing with approx. 10 Hz indicates the initialization of the local bus or a local bus error.</td>
<td>Note the following flashing sequence.</td>
</tr>
<tr>
<td>red cyclical flashing</td>
<td>Up to three successive flashing sequences indicate local bus errors. There are short intervals between the sequences.</td>
<td>Evaluate the flashing sequences based on the following blink code table. The blinking indicates an error message comprised of an error code and error argument.</td>
</tr>
<tr>
<td>off</td>
<td>No data cycle on the local bus.</td>
<td>The fieldbus coupler/controller supply is off.</td>
</tr>
</tbody>
</table>

Device boot-up occurs after turning on the power supply. The I/O LED flashes orange.

Then the local bus is initialized. This is indicated by flashing red at 10 Hz for 1 ... 2 seconds.

After a trouble-free initialization, the I/O LED is green.

In the event of an error, the I/O LED continues to blink red. Blink codes indicate detailed error messages. An error is indicated cyclically by up to 3 flashing sequences.

After elimination of the error, restart the node by turning the power supply of the device off and on again.
Example of a module error:

- The I/O LED starts the error display with the first flashing sequence (approx. 10 Hz).
  - After the first break, the second flashing sequence starts (approx. 1 Hz): The I/O LED blinks four times. Error code 4 indicates "data error internal data bus".
  - After the second break, the third flashing sequence starts (approx. 1 Hz): The I/O LED blinks twelve times.
Error argument 12 means that the local bus is interrupted behind the twelfth I/O module.

The thirteenth I/O module is either defective or has been pulled out of the assembly.
| Error code 1: "Hardware and configuration error" |
|---|---|---|
| **Error Argument** | **Error Description** | **Solution** |
| 1 | Overflow of the internal buffer memory for the attached I/O modules. | 1. Turn off the power supply of the node.  
2. Reduce the number of I/O modules.  
3. Turn on again the power supply of the node.  
4. If the error persists, replace the head station. |
| 2 | I/O module(s) with unknown data type | 1. Determine the faulty I/O module. First turn off the power supply of the node.  
2. Plug the end module into the middle of the node.  
3. Turn on again the power supply of the node.  
4. LED continues to flash? -  
   Turn off the power supply of the node and plug the end module into the middle of the first half of the node (toward the head station).  
   LED not flashing? -  
   Turn off the power supply of the node and plug the end module into the middle of the second half of the node (away from the head station).  
5. Turn on again the power supply of the node.  
6. Repeat the procedure described in step 4 while halving the step size until the faulty I/O module is detected.  
7. Replace the faulty I/O module.  
8. Contact I/O support and inquire about a firmware update for the head station. |
| 3 | Invalid check sum in the parameter area of the head station. | 1. Turn off the power supply of the node.  
2. Replace the head station.  
3. Turn on again the power supply of the node. |
| 4 | Fault when writing in the serial EEPROM. | 1. Turn off the power supply of the node.  
2. Replace the head station.  
3. Turn on again the power supply of the node. |
| 5 | Fault when reading the serial EEPROM | 1. Turn off the power supply of the node.  
2. Replace the head station.  
3. Turn on again the power supply of the node. |
| 6 | The I/O module configuration after AUTORESET differs from the configuration determined the last time the head station was powered up. | 1. Restart the head station by turning the power supply off and on. |
| 7 | Invalid hardware-firmware combination. | 1. Turn off the power supply of the node.  
2. Replace the head station.  
3. Turn on again the power supply of the node. |
| 8 | Timeout during serial EEPROM access. | 1. Turn off the power supply of the node.  
2. Replace the head station.  
3. Turn on again the power supply of the node. |
## Table 63: Blink code- Table for the I/O LED signaling, error code 1

<table>
<thead>
<tr>
<th>Error Argument</th>
<th>Error Description</th>
<th>Solution</th>
</tr>
</thead>
</table>
| 9              | Head station initialization error         | 1. Turn off the power supply of the node.  
|                |                                          | 2. Replace the head station.                                               
|                |                                          | 3. Turn on again the power supply of the node.                            |
| 10             | Buffer power failure real-time clock (RTC) | 1. Set the clock.  
|                |                                          | 2. Maintain the power supply of the node for at least 15 minutes in order to charge the Goldcap capacitor. |
| 11             | Fault during read access to the real-time clock (RTC) | 1. Set the clock.  
|                |                                          | 2. Maintain the power supply of the node for at least 15 minutes in order to charge the Goldcap capacitor. |
| 12             | Fault during write access to the real-time clock (RTC) | 1. Set the clock.  
|                |                                          | 2. Maintain the power supply of the node for at least 15 minutes in order to charge the Goldcap capacitor. |
| 13             | Clock interrupt fault                     | 1. Set the clock.  
|                |                                          | 2. Maintain the power supply of the node for at least 15 minutes in order to charge the Goldcap capacitor. |
| 14             | Maximum number of gateway or mailbox modules exceeded | 1. Turn off the power supply of the node.  
|                |                                          | 2. Reduce the number of corresponding modules to a valid number.  
|                |                                          | 3. Turn on again the power supply of the node.                            |
| 15             | Firmware loader was loaded from backup.  | 1. Execute the last firmware update again.                                
|                |                                          | 2. If the error persists, contact I/O support.                            |
| 16             | Firmware was loaded from backup.         | 1. Execute the last firmware update again.                                
|                |                                          | 2. If the error persists, contact I/O support.                            |

## Table 64: Blink Code Table for the I/O LED Signaling, Error Code 2

<table>
<thead>
<tr>
<th>Error Argument</th>
<th>Error Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Not used</td>
<td>-</td>
</tr>
</tbody>
</table>
| 2              | Process image is too large.     | 1. Turn off the power supply of the node.  
|                |                                  | 2. Reduce number of I/O modules.                                         
|                |                                  | 3. Turn the power supply on.                                             |
Table 65: Blink Code Table for the I/O LED Signaling, Error Code 3

<table>
<thead>
<tr>
<th>Error Code 3: “Protocol error, local bus”</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error Argument</td>
<td>Error Description</td>
</tr>
<tr>
<td>-</td>
<td>Local bus communication is faulty, defective module cannot be identified.</td>
</tr>
<tr>
<td>-</td>
<td>- Are passive power supply modules (750-613) located in the node? -</td>
</tr>
<tr>
<td></td>
<td>1. Check that these modules are supplied correctly with power.</td>
</tr>
<tr>
<td></td>
<td>2. Determine this by the state of the associated status LEDs.</td>
</tr>
<tr>
<td></td>
<td>- Are all modules connected correctly or are there any 750-613 Modules in the node? -</td>
</tr>
<tr>
<td></td>
<td>1. Determine the faulty I/O module. First turn off the power supply for the node.</td>
</tr>
<tr>
<td></td>
<td>2. Plug the end module into the middle of the node.</td>
</tr>
<tr>
<td></td>
<td>3. Turn the power supply on again.</td>
</tr>
<tr>
<td></td>
<td>4. - LED continues to flash? -</td>
</tr>
<tr>
<td></td>
<td>Turn off the power supply and plug the end module into the middle of the first half of the node (toward the fieldbus controller).</td>
</tr>
<tr>
<td></td>
<td>- LED not flashing? -</td>
</tr>
<tr>
<td></td>
<td>Turn off the power and plug the end module into the middle of the second half of the node (away from the fieldbus controller).</td>
</tr>
<tr>
<td></td>
<td>5. Turn the power supply on again.</td>
</tr>
<tr>
<td></td>
<td>6. Repeat the procedure described in step 4 while halving the step size until the faulty I/O module is detected.</td>
</tr>
<tr>
<td></td>
<td>7. Replace the faulty I/O module.</td>
</tr>
<tr>
<td></td>
<td>8. If there is only one I/O module on the fieldbus controller and the LED is flashing, either the I/O module or fieldbus controller is defective.</td>
</tr>
<tr>
<td></td>
<td>9. Replace the defective component.</td>
</tr>
</tbody>
</table>
### Table 66: Blink Code Table for the I/O LED Signaling, Error Code 4

<table>
<thead>
<tr>
<th>Error Code 4: “Physical error, local bus”</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Error Argument</strong></td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>-</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

* The number of light pulses (n) indicates the position of the I/O module.
I/O modules without data are not counted (e.g., supply modules without diagnostics)

### Table 67: Blink Code Table for the I/O LED Signaling, Error Code 5

<table>
<thead>
<tr>
<th>Error Code 5: “Initialization error, local bus”</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Error Argument</strong></td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>n*</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

* The number of light pulses (n) indicates the position of the I/O module.
I/O modules without data are not counted (e.g., supply modules without diagnostics)
**Table 68: Blink Code Table for the I/O LED Signaling, Error Code 6**

<table>
<thead>
<tr>
<th>Error code 6: &quot;Fieldbus specific errors&quot;</th>
<th>Error Argument</th>
<th>Error Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Invalid MACID</td>
<td>1. Turn off the power supply of the node. 2. Exchange fieldbus coupler. 3. Turn the power supply on again.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Ethernet Hardware initialization error</td>
<td>1. Restart the fieldbus coupler by turning the power supply off and on again. 2. If the error still exists, exchange the fieldbus coupler.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>TCP/IP initialization error</td>
<td>1. Restart the fieldbus coupler by turning the power supply off and on again. 2. If the error still exists, exchange the fieldbus coupler.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Network configuration error (no IP Address)</td>
<td>1. Check the settings of BootP server.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Application protocol initialization error</td>
<td>1. Restart the fieldbus coupler by turning the power supply off and on again. 2. If the error still exists, exchange the fieldbus coupler.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Process image is too large</td>
<td>1. Turn off the power supply of the node. 2. Reduce number of I/O modules</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Double IP address in network</td>
<td>1. Change configuration. Use another IP address, which is not yet present in network. 2. Restart the fieldbus coupler by turning the power supply off and on again.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Error when building the process image</td>
<td>1. Turn off the power supply of the node. 2. Reduce number of I/O modules 3. Restart the fieldbus coupler by turning the power supply off and on again. 4. If the error still exists, exchange the fieldbus coupler.</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Error with mapping between bus modules and fieldbus</td>
<td>1. Check io-config.xml file on the fieldbus coupler</td>
<td></td>
</tr>
</tbody>
</table>

**Table 69: Blink Code Table for the I/O LED Signaling, Error Code 7**

<table>
<thead>
<tr>
<th>Error code 7: &quot;Not supported I/O module&quot;</th>
<th>Error Argument</th>
<th>Error Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>First unsupported I/O module in place of n.</td>
<td>1. Turn off the power supply to the node. 2. Replace the nth I/O module containing process data or reduce the number of modules to the number of n-1. 3. Turn the power supply on.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 70: Blink Code Table for the I/O LED Signaling, Error Code 8 ... 10**

<table>
<thead>
<tr>
<th>Error code 8 ... 10 --not used--</th>
<th>Error Argument</th>
<th>Error Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>not used</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Table 71: Blink Code Table for the I/O LED Signaling, Error Code 11

<table>
<thead>
<tr>
<th>Error Argument</th>
<th>Error Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Maximum number of Gateway modules exceeded</td>
<td>1. Turn off the power supply of the node.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Reduce number of Gateway modules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Turn the power supply on again.</td>
</tr>
<tr>
<td>2</td>
<td>Maximum size of Mailbox exceeded</td>
<td>1. Turn off the power supply of the node.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Reduce the Mailbox size.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Turn the power supply on again.</td>
</tr>
<tr>
<td>3</td>
<td>Maximum size of process image exceeded due to the put</td>
<td>1. Turn off the power supply of the node.</td>
</tr>
<tr>
<td></td>
<td>Gateway modules</td>
<td>2. Reduce the data width of the Gateway modules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Turn the power supply on again.</td>
</tr>
</tbody>
</table>

* The number of blink pulses (n) indicates the position of the I/O module.
I/O modules without data are not counted (e.g. supply module without diagnosis)

Table 72: Blink code table for I/O LED signaling, error code 12

<table>
<thead>
<tr>
<th>Error Argument</th>
<th>Error Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>General error of the operating system</td>
<td>1. Restart the fieldbus node by turning the power supply off and on again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. If the error still exists, please contact the I/O Support.</td>
</tr>
<tr>
<td>2</td>
<td>General error of the file system</td>
<td>1. Reset the file system using &quot;WAGO Ethernet Settings&quot;, button [Reset File System] in the menu above.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Restart the fieldbus node by turning the power supply off and on again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. If the error still exists, please contact the I/O Support.</td>
</tr>
<tr>
<td>3</td>
<td>Insufficient RAM memory</td>
<td>1. Reduce number of BACnet objects.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Restart the access function.</td>
</tr>
</tbody>
</table>

Table 73: Blink code table for I/O LED signaling, error code 13

<table>
<thead>
<tr>
<th>Error Argument</th>
<th>Error description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not used</td>
<td>-</td>
</tr>
<tr>
<td>Error Argument</td>
<td>Error Description</td>
<td>Solution</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>The inserted memory card is unusable (defect or format/file system is not supported).</td>
<td>1. Check the function of the memory card on a PC. If necessary, replace the memory card. 2. Check if the memory card is formatted with the FAT. If not, format the memory card with the FAT file system.</td>
</tr>
<tr>
<td>2</td>
<td>The memory card was removed during an ongoing read/write access.</td>
<td>1. Insert the memory card back into the card slot. 2. Restart the canceled function.</td>
</tr>
<tr>
<td>3</td>
<td>The space on the internal drive A is exhausted.</td>
<td>1. Remove unnecessary files on the internal drive A. 2. Restart the canceled function.</td>
</tr>
<tr>
<td>4</td>
<td>The space on the memory card (drive S) is exhausted.</td>
<td>1. Remove unnecessary files on the drive S. 2. Use a larger capacity memory card. 3. Restart the canceled function.</td>
</tr>
<tr>
<td>5</td>
<td>Saving parameters in non-volatile memory failed.</td>
<td>1. Restart the device. 2. Restart the canceled function. 3. If the problem persists, contact support.</td>
</tr>
<tr>
<td>6</td>
<td>The backup function failed due to an internal error.</td>
<td>1. Restart the device. 2. Restart the canceled function. 3. If the problem persists, contact support.</td>
</tr>
<tr>
<td>7</td>
<td>The restore function failed due to an internal error.</td>
<td>1. Restart the device. 2. Restart the canceled function. 3. If the problem persists, contact support.</td>
</tr>
<tr>
<td>8</td>
<td>The memory card is not inserted.</td>
<td>1. Insert a memory card into the card slot. 2. Repeat the last action.</td>
</tr>
<tr>
<td>9</td>
<td>The memory card is write-protected.</td>
<td>1. Remove the write-protection of the inserted SD card. 2. Repeat the last action. 3. If the problem persists, contact support.</td>
</tr>
<tr>
<td>10</td>
<td>The version of the selected backup image is not compatible.</td>
<td>1. Use backup image files created by a compatible fieldbus coupler (part number, firmware version). 2. Repeat the last action. 3. If the problem persists, contact support.</td>
</tr>
<tr>
<td>11</td>
<td>The selected backup image is defective / cannot be interpreted.</td>
<td>1. Create a new backup image. 2. Repeat the last action. 3. If the problem persists, contact support.</td>
</tr>
<tr>
<td>12</td>
<td>There is no backup image file on the selected backup media.</td>
<td>1. Copy a backup image file to the selected backup medium: A: \ backup or S: \ backup. 2. Repeat the last action. 3. If the problem persists, contact support.</td>
</tr>
<tr>
<td>13</td>
<td>The executed action cannot currently be executed.</td>
<td>1. Disconnect all active FTP / SFTP and fieldbus connections. 2. Repeat the last action. 3. If the problem persists, contact support.</td>
</tr>
</tbody>
</table>
10.1.3 Evaluating Memory Card Status

The access to the memory card is indicated by the SD-LED. The SD-LED is directly above the memory card slot behind the transparent cover flap.

10.1.4 Evaluating Power Supply Status

The power supply unit of the device has two green LEDs that indicate the status of the power supplies.
LED 'A' indicates the 24 V supply of the coupler.
LED 'B' reports the power available on the power jumper contacts for field side power.

<table>
<thead>
<tr>
<th>LED Status</th>
<th>Meaning</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Green</td>
<td>Operating voltage for the system is available.</td>
<td>-</td>
</tr>
<tr>
<td>Off</td>
<td>No power is available for the system</td>
<td>Check the power supply for the system (24 V and 0 V).</td>
</tr>
<tr>
<td>B Green</td>
<td>The operating voltage for power jumper contacts is available.</td>
<td>-</td>
</tr>
<tr>
<td>Off</td>
<td>No operating voltage is available for the power jumper contacts.</td>
<td>Check the power supply for the power jumper contacts (24 V and 0 V).</td>
</tr>
</tbody>
</table>
10.2 Fault Behavior

10.2.1 Fieldbus Failure

A fieldbus and thus a connection failure occurs if the set time-out time of the watchdog has elapsed without being triggered by the higher-level controller. This can happen, for example, when the master is switched off or the fieldbus cable is interrupted. A fault in the master can also lead to a fieldbus failure. Then there is no connection via ETHERNET given.

The Modbus Watchdog monitors the Modbus communication running via the Modbus protocol. If the Modbus watchdog has been configured and activated, a fieldbus failure is indicated by the red I/O LED lighting up. All subsequent Modbus TCP/IP requests are answered with the exception code 0x0004 (Slave Device Failure).

Further Information

For detailed information on the Watchdog see Chapter "Modbus Functions" >...> "Modbus Watchdog".

10.2.2 Local Bus Failure

I/O LED indicates a local bus failure.

When a local bus failure occurs, the head station generates an error message (error code and error argument) via the red-flashing I/O LED (see chapter "Diagnostics" => "Evaluating Node Status - I/O LED (Blink Code Table)").

If the local bus completely fails, output modules switch to defined states, e.g. "Off" or "0 V".

Example:

A fieldbus node consists of head station, five I/O modules with process data and the end module.
The output of one digital output module is activated.

If the end module is removed of the fieldbus node during operation, the local bus is interrupted. The output of the digital output module is automatically deactivated and the I/O LED flashes red and indicates with it error message 4/5.

The flashing code table provides for error code 4: "Physical error, local bus" with error argument 5: "Interruption of the local bus behind the nth I/O module with process data".
If the end module is re-inserted into the fieldbus node, the local bus will restart after a few seconds. After the initialization blink code is completely, the I/O LED lights up again in a steady green and the transmission of the process data is resumed. Also the output of the digital output module is re-activated.

If the local bus error is caused by a defective module, it must be replaced, as described in the blink code table for error code 4 under "Solution".
11 Fieldbus Communication

Fieldbus communication between master application and a WAGO fieldbus coupler/controller based on the ETHERNET standard normally occurs via a fieldbus-specific application protocol.

Depending on the application, this can be e.g., MODBUS TCP/UDP, EtherNet/IP, BACnet/IP, KNXnet/IP, PROFINET, sercos or other.

In addition to the ETHERNET standard and the fieldbus-specific application protocol, there are also other communications protocols important for reliable communication and data transmission and other related protocols for configuring and diagnosing the system implemented in the WAGO fieldbus coupler/controller based on ETHERNET.

These protocols are explained in more detail in the other sections.

11.1 Implemented Protocols

11.1.1 Communication Protocols

11.1.1.1 IP (Internet Protocol)

The Internet protocol divides datagrams into segments and is responsible for their transmission from one network subscriber to another. The stations involved may be connected to the same network or to different physical networks which are linked together by routers.

Routers are able to select various paths (network transmission paths) through connected networks, and bypass congestion and individual network failures. However, as individual paths may be selected which are shorter than other paths, datagrams may overtake each other, causing the sequence of the data packets to be incorrect.

Therefore, it is necessary to use a higher-level protocol, for example, TCP to guarantee correct transmission.

**IP Packet**

In addition to the data units to be transported, the IP data packets contain a range of address information and additional information in the packet header.

<table>
<thead>
<tr>
<th>Table 76: IP Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Header</td>
</tr>
<tr>
<td>IP Data</td>
</tr>
</tbody>
</table>

The most important information in the IP header is the IP address of the transmitter and the receiver and the transport protocol used.
**IP Addresses**

To allow communication over the network each fieldbus node requires a 32 bit Internet address (IP address).

---

**Note**

**IP Address must be unique!**

For error free operation, the IP address must be unique within the network. The same IP address may not be assigned twice.

As shown below there are various address classes with net identification (net ID) and subscriber identification (subscriber ID) of varying lengths. The net ID defines the network in which the subscriber is located. The subscriber ID identifies a particular subscriber within this network.

Networks are divided into various network classes for addressing purposes:

- **Class A:** (Net ID: Byte 1, Host ID: Byte 2… Byte 4)

  Table 77: Network Class A  
  e. g. 101 . 16 . 232 . 22  
  | 01100101 | 00010000 | 11101000 | 00010110 |
  | 0       | Net ID   | Host ID   |

  The highest bit in Class A networks is always '0'. This means the highest byte can be in a range of '0 0000000' to '0 1111111'. Therefore, the address range of a Class A network in the first byte is always between 0 and 127.

- **Class B:** (Net ID: Byte 1 … Byte 2, Host ID: Byte 3… Byte 4)

  Table 78: Network Class B  
  e. g. 181 . 16 . 232 . 22  
  | 10110101 | 00010000 | 11101000 | 00010110 |
  | 10      | Net ID   | Host ID   |

  The highest bits in Class B networks are always '10'. This means the highest byte can be in a range of '10 000000' to '10 111111'. Therefore, the address range of Class B networks in the first byte is always between 128 and 191.

- **Class C:** (Net ID: Byte 1 … Byte 3, Host ID: Byte 4)

  Table 79: Network Class C  
  e. g. 201 . 16 . 232 . 22  
  | 11000101 | 00010000 | 11101000 | 00010110 |
  | 110     | Net ID   | Host ID   |

  The highest bits in Class C networks are always '110'. This means the highest byte can be in a range of '110 00000' to '110 11111'.
Therefore, the address range of Class C networks in the first byte is always between 192 and 223.

- **Additional network classes (D, E):** are only used for special tasks.

**Key Data**

Table 80: Key Data Class A, B and C

<table>
<thead>
<tr>
<th>Network Class</th>
<th>Address range of the subnetwork</th>
<th>Possible number of Networks</th>
<th>Hosts per Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A</td>
<td>0.XXX.XXX.XXX ... 127.XXX.XXX.XXX</td>
<td>128 ( (2^7) )</td>
<td>Approx. 16 Million ( (2^{24}) )</td>
</tr>
<tr>
<td>Class B</td>
<td>128.000.XXX.XXX ... 191.255.XXX.XXX</td>
<td>Approx. 16 Thousand ( (2^{14}) )</td>
<td>Ca. 65 Thousand ( (2^{16}) )</td>
</tr>
<tr>
<td>Class C</td>
<td>192.000.000.XXX ... 223.255.255.XXX</td>
<td>Approx. 2 Million ( (2^{21}) )</td>
<td>254 ( (2^8) )</td>
</tr>
</tbody>
</table>

Each WAGO ETHERNET fieldbus coupler or controller can be easily assigned an IP address via the implemented BootP protocol. For small internal networks we recommend selecting a network address from Class C.

**Note**

**Do not set IP addresses to 0.0.0.0 or 255.255.255.255!**

Never set all bits to equal 0 or 1 in one byte (byte = 0 or 255). These are reserved for special functions and may not be allocated. Therefore, the address 10.0.10.10 may not be used due to the 0 in the second byte.

If a network is to be directly connected to the Internet, only registered, internationally unique IP addresses allocated by a central registration service may be used. These are available from InterNIC (International Network Information Center).

**Note**

**Internet access only by the authorized network administrator!**

Direct connection to the Internet should only be performed by an authorized network administrator and is therefore not described in this manual.

**Subnets**

To allow routing within large networks a convention was introduced in the specification RFC 950. Part of the Internet address, the subscriber ID is divided up again into a subnetwork number and the station number of the node. With the aid of the network number it is possible to branch into internal subnetworks within the partial network, but the entire network is physically connected together. The size and position of the subnetwork ID are not defined; however, the size is dependent upon the number of subnets to be addressed and the number of subscribers per subnet.
Table 81: Example: Class B Address with Field for Subnet IDs

<table>
<thead>
<tr>
<th>1</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>32</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>...</td>
<td>Network ID</td>
<td>Subnet ID</td>
</tr>
</tbody>
</table>

**Subnet Mask**

A subnet mask was introduced to encode the subnets in the Internet. This involves a bit mask, which is used to mask out or select specific bits of the IP address. The mask defines the subscriber ID bits used for subnet coding, which denote the ID of the subscriber. The entire IP address range theoretically lies between 0.0.0.0 and 255.255.255.255. Each 0 and 255 from the IP address range are reserved for the subnet mask.

The standard masks depending upon the respective network class are as follows:

- **Class A Subnet mask:**
  
  
  Table 82: Subnet Mask for Class A Network
  
  | 255 | .0 | .0 | .0 |

- **Class B Subnet mask:**
  
  
  Table 83: Subnet Mask for Class B Network
  
  | 255 | .255 | .0 | .0 |

- **Class C Subnet mask:**
  
  
  Table 84: Subnet Mask for Class C Network
  
  | 255 | .255 | .255 | .0 |

Depending on the subnet division the subnet masks may, however, contain other values beyond 0 and 255, such as 255.255.255.128 or 255.255.255.248.

Your network administrator allocates the subnet mask number to you.

Together with the IP address, this number determines which network your PC and your node belongs to.

The recipient node, which is located on a subnet, initially calculates the correct network number from its own IP address and subnet mask. Only then the node checks the node number and, if it corresponds, delivers the entire packet frame.

Table 85: Example for an IP Address from a Class B Network

| IP address | 172.16.233.200 | 10101100 00010000 11101001 11001000’ |
| Subnet mask | 255.255.255.128 | 11111111 11111111 11111111 10000000’ |
| Net ID | 172.16.0.0 | 10101100 00010000 00000000 00000000’ |
| Subnet ID | 0.0.233.128 | 00000000 00000000 11101001 10000000’ |
| Host ID | 0.0.0.72 | 00000000 00000000 00000000 01001000’ |
**Note**

**Specification of the network mask necessary!**
Specify the network mask defined by the administrator in the same way as the IP address when installing the network protocol.

**Gateway**

The subnets of the Internet are normally connected via gateways. The function of these gateways is to forward packets to other networks or subnets.

This means that in addition to the IP address and network mask for each network card, it is necessary to specify the correct IP address of the standard gateway for a PC or fieldbus node connected to the Internet. You should also be able to obtain this IP address from your network administrator.

The IP function is limited to the local subnet if this address is not specified.

To communicate directly with each other, host and gateway must be on the same subnet, that means the network ID must be the same.

**RAW IP**

Raw IP manages without protocols such as PPP (point-to-point protocol). With RAW IP, the TCP/IP packets are directly exchanged without handshaking, thus enabling the connection to be established more quickly.

However, the connection must beforehand have been configured with a fixed IP address. The advantages of RAW IP are high data transfer rate and good stability.

**IP Multicast**

Multicast refers to a method of transmission from a point to a group, which is a point-to-multipoint transfer or multipoint connection. The advantage of multicast is that messages are simultaneously transferred to several users or closed user groups via one address.

IP multicasting at the Internet level is realized with the help of the Internet Group Message Protocol IGMP; neighboring routers use this protocol to inform each other on membership to the group.

For distribution of multicast packets in the sub-network, IP assumes that the datalink layer supports multicasting. In the case of Ethernet, you can provide a packet with a multicast address in order to send the packet to several recipients with a single send operation. Here, the common medium enables packets to be sent simultaneously to several recipients. The stations do not have to inform each other on who belongs to a specific multicast address – every station
physically receives every packet. The resolution of IP address to Ethernet address is solved by the use of algorithms, IP multicast addresses are embedded in Ethernet multicast addresses.

11.1.1.2 TCP (Transmission Control Protocol)

As the layer above the Internet protocol, TCP (Transmission Control Protocol) guarantees the secure transport of data through the network.

TCP enables two subscribers to establish a connection for the duration of the data transmission. Communication takes place in full-duplex mode (i.e., transmission between two subscribers in both directions simultaneously).

TCP provides the transmitted message with a 16-bit checksum and each data packet with a sequence number.

The receiver checks that the packet has been correctly received on the basis of the checksum and then sets off the sequence number. The result is known as the acknowledgement number and is returned with the next self-sent packet as an acknowledgement.

This ensures that the lost TCP packets are detected and resent, if necessary, in the correct sequence.

TCP Data Packet

The packet header of a TCP data packet is comprised of at least 20 bytes and contains, among others, the application port number of the transmitter and the receiver, the sequence number and the acknowledgement number.

The resulting TCP packet is used in the data unit area of an IP packet to create a TCP/IP packet.

TCP Port Numbers

TCP can, in addition to the IP address (network and subscriber address), respond to a specific application (service) on the addressed subscriber. For this the applications located on a subscriber, such as a web server, FTP server and others are addressed via different port numbers. Well-known applications are assigned fixed ports to which each application can refer when a connection is built up (Examples: Telnet Port number: 23, http Port number: 80).

A complete list of “standardized services” is contained in the RFC 1700 (1994) specifications.

11.1.1.3 UDP (User Datagram Protocol)

The UDP protocol, like the TCP protocol, is responsible for the transport of data. Unlike the TCP protocol, UDP is not connection-orientated; meaning that there are no control mechanisms for the data exchange between transmitter and receiver. The advantage of this protocol is the efficiency of the transmitted data and the resulting higher processing speed.
11.1.2 Configuration and Diagnostics Protocols

11.1.2.1 BootP (Bootstrap Protocol)

The “Bootstrap Protocol” (BootP) can be used to assign an IP address and other parameters to the fieldbus coupler/controller in a TCP/IP network. Subnet masks and gateways can also be transferred using this protocol. Protocol communication is comprised of a client request from the fieldbus coupler or controller and a server response from the PC.

A broadcast request is transmitted to Port 67 (BootP server) via the protocol that contains the hardware address (MAC ID) for the fieldbus coupler or controller.

The BootP server then receives this message. The server contains a database in which the MAC ID and IP addresses are assigned to one another. When a MAC address is found a broadcast reply is transmitted via the network.

The fieldbus coupler/controller “listens” at the specified Port 68 for a response from the BootP server. Incoming packets contain information such as the IP address and the MAC address for the fieldbus coupler/controller. A fieldbus coupler/controller recognizes by the MAC address that the message is intended for that particular fieldbus coupler/controller and accepts the transmitted IP address into its network.

**Note**

**IP addresses can be assigned via BootP under Windows and Linux!**
You can use WAGO-BootP-Server to assign an IP address under the Windows and Linux operating systems. You can also use any other BootP server besides WAGO-BootP-Server. You can also use any other BootP server besides the WAGO-BootP-Server.

**Information**

**More information about WAGO-BootP-Server**
The process for assigning addresses using WAGO-BootP-Server is described in detail in the section “Commissioning”.

The fieldbus coupler/controller supports the following options in addition to the default “IP address” option:
The “Features” WBM page can also be used to select the “BootP Request before static IP” option. After the restart, 5 BootP queries are sent. If there is no response to any of these queries, the fieldbus coupler/controller tries to configure itself with the IP parameters saved in the EEPROM.

If you want the IP address and subnet mask are stored in the EEPROM when using the Bootstrap protocol, then the option “use IP from EEPROM” has to be switched (via the WBM, HTML page “Port”) following the configuration via BootP. When booting next the fieldbus coupler/controller uses the parameters saved in the EEPROM.

By default, BootP is activated in the fieldbus coupler/controller.

When BootP is activated, the fieldbus coupler/controller expects the BootP server to be permanently available.

DHCP (Dynamic Host Configuration Protocol)

The fieldbus coupler/controller internal HTML page opened via the “Port” link provides the option to configure the network using the data saved in the EEPROM or via DHCP instead of via the BootP protocol.

DHCP (Dynamic Host Configuration Protocol) is a further development of BootP and is backwards compatible with BootP.

Both BOOTP and DHCP assign an IP address to the fieldbus node (Client) when starting; the sequence is the same as for BootP.

For configuration of the network parameters via DHCP, the fieldbus coupler/controller sends a client request to the DHCP server e.g., on the connected PC.

A broadcast request is transmitted to Port 67 (DHCP server) via the protocol that contains the hardware address (MAC ID) for the fieldbus coupler/controller.
The DHCP server then receives this message. The server contains a database in which the MAC ID and IP addresses are assigned to one another. When a MAC address is found a broadcast reply is transmitted via the network.

The fieldbus coupler/controller “listens” at the specified Port 68 for a response from the DHCP server. Incoming packets contain information such as the IP address and the MAC address for the fieldbus coupler/controller. A fieldbus coupler/controller recognizes by the MAC address that the message is intended for that particular fieldbus coupler/controller and accepts the transmitted IP address into its network.

If there is no reply, the inquiry is sent again after 4 seconds, 8 seconds and 16 seconds.
If all inquiries receive no reply, a blink code is reported via the I/O LED.

If you want the IP address and subnet mask are stored in the EEPROM when using DHCP, then the option “use IP from EEPROM” has to be switched (via the WBM, HTML page “Port”) following the configuration via DHCP.
When booting next the fieldbus coupler/controller uses the parameters saved in the EEPROM.

The difference between BOOTP and DHCP is that both use different assignment methods and that configuration with DHCP is time limited. The DHCP client always has to update the configuration after the time has elapsed. Normally, the same parameters are continuously confirmed by the server.

BOOTP can be used to assign a fixed IP address for each client where the addresses and their reservation are permanently saved in the BOOTP server database.

Because of this time dependency, DHCP is also used to dynamically assign available IP addresses through client leases (lease time after which the client requests a new address) where each DHCP client address is saved temporarily in the server database.

In addition, DHCP clients do not require a system restart to rebind or renew configuration with the DHCP server. Instead, clients automatically enter a rebinding state at set timed intervals to renew their leased address allocation with the DHCP server. This process occurs in the background and is transparent to the user.

There are three different operating modes for a DHCP server:

- **Manual assignment**
  In this mode, the IP addresses are permanently assigned on the DHCP server to specific MAC addresses. The addresses are assigned to the MAC address for an indefinite period.
  Manual assignments are used primarily to ensure that the DHCP client can be reached under a fixed IP address.

- **Automatic assignment**
  For automatic assignment, a range of IP addresses is assigned on the
DHCP server.
If the address was assigned from this range once to a DHCP client, then it belongs to the client for an indefinite period as the assigned IP address is also bound to the MAC address.

- **Dynamic assignment**
  This process is similar to automatic assignment, but the DHCP server has a statement in its configuration file that specifies how long a certain IP address may be “leased” to a client before the client must log into the server again and request an “extension”.
  If the client does not log in, the address is released and can be reassigned to another (or the same) client. The time defined by the administrator is called Lease Time.
  Some DHCP servers also assign IP addresses based on the MAC address, i.e., a client receives the same IP address as before after longer network absence and elapse of the Lease Time (unless the IP address has been assigned otherwise in the mean time).

DHCP is used to dynamically configure the network parameters.
The ETHERNET TCP/IP fieldbus coupler/controller has a DHCP client that supports the following options in addition to the default “IP address” option:

<table>
<thead>
<tr>
<th>Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>[OPT1] Subnet mask</td>
<td>32-bit address mask that displays which bits of the IP address identify the network and which identify the network stations.</td>
</tr>
<tr>
<td>[OPT2] Time zone</td>
<td>Time difference between the local time and the UTC (Universal Time Coordinated).</td>
</tr>
<tr>
<td>[OPT3] Gateway</td>
<td>IP address of the router that permits access to other networks.</td>
</tr>
<tr>
<td>[OPT6] DNS server</td>
<td>IP address of the name servers that converts a name into an IP address. Up to 2 DNS servers can be configured.</td>
</tr>
<tr>
<td>[OPT15] Domain name</td>
<td>The name of the domain is the unique name of a network. The domain name can contain up to 32 characters.</td>
</tr>
<tr>
<td>[OPT42] NTP server</td>
<td>IP address of the Network Time Server. This address is only accepted if the protocol “SNTP” is activated via the WBM.</td>
</tr>
<tr>
<td>[OPT51] Lease time</td>
<td>The maximum duration in seconds (i.e., how long the fieldbus coupler/controller maintains the assigned IP address) can be defined here. The maximum lease time for the fieldbus controller is 48 days. This is due to the internal timer resolution. The minimum lease time is 16 minutes.</td>
</tr>
<tr>
<td>[OPT58] Renewing time</td>
<td>The renewing time indicates when the fieldbus coupler/controller must renew the lease time. The renewing time should be approximately half of the lease time.</td>
</tr>
<tr>
<td>[OPT59] Rebinding time</td>
<td>The rebinding time indicates after what amount of time the fieldbus coupler/controller must have received its new address. The rebinding time should be approximately 7/8 of the lease time.</td>
</tr>
</tbody>
</table>

*) In contrast to BootP, the DHCP client does not support assignment of the host name.
11.1.2.3  **HTTP (Hypertext Transfer Protocol)**

HTTP is a protocol used by WWW (World Wide Web) servers for the forwarding of hypermedia, texts, images, audiodata, etc.

Today, HTTP forms the basis of the Internet and is also based on requests and responses in the same way as the BootP protocol.

The HTTP server implemented in the (programmable) fieldbus coupler or controller is used for viewing the HTML pages saved in the coupler/controller. The HTML pages provide information about the coupler/controller (state, configuration), the network and the process image.

On some HTML pages, (programmable) fieldbus coupler or controller settings can also be defined and altered via the web-based management system (e.g. whether IP configuration of the coupler/controller is to be performed via the DHCP protocol, the BootP protocol or from the data stored in the EEPROM).

The HTTP server uses port number 80.

11.1.2.4  **DNS (Domain Name Systems)**

The DNS client enables conversion of logical Internet names such as www.wago.com into the appropriate decimal IP address represented with separator stops, via a DNS server. Reverse conversion is also possible.

The addresses of the DNS server are configured via DHCP, BootP or web-based management. Up to 2 DNS servers can be specified. The host identification can be achieved with two functions; an internal host table is not supported.

11.1.2.5  **FTP-Server (File Transfer Protocol)**

The file transfer protocol (FTP) enables files to be exchanged between different network stations regardless of operating system.

In the case of the ETHERNET coupler/controller, FTP is used to store and read the HTML pages created by the user, the IEC61131 program and the IEC61131 source code in the (programmable) fieldbus coupler or controller.

A total memory of 1 GB is available for the internal file system.

---

**Note**

Cycles for flash limited to 1 million!
Up to 1 million write cycles per sector are allowed when writing the flash for the file system. The file system supports "Wear-Leveling", so that the same sectors are not always written to.
More Information about the implemented Protocols

You can find a list of the exact available implemented protocols in the section “Technical Data” to the fieldbus coupler and/or controller.

11.1.2.6 SNMP (Simple Network Management Protocol)

The Simple Network Management Protocol (SNMP) is responsible for transporting the control data that allows the exchange of management information as well as status and statistic data between individual network components and a management system.

An SNMP management workstation polls the SNMP agents to obtain information on the relevant devices.

SNMP is supported in versions 1/2c and some fieldbus couplers/controllers in version 3.

This represents a community message exchange in SNMP versions 1 and 2c. The community name of the network community must thereby be specified.

In SNMP version 3, exchanging messages is user-related. Each device, that knows the passwords set via WBM, may read or write values from the controller. In SNMPv3, user data from SNMP messages can also be transmitted in encoded form. This way, both requested values and values to be written cannot be easily decoded by others via ETHERNET. This is why SNMPv3 is often used in safety-related networks.

The device data, that can be accessed or modified by an SNMP agent, is called SNMP object. The sets of SNMP objects are stored in a logical database called Management Information Base (MIB); this is why these objects are typically known as “MIB objects”.

The SNMP of the ETHERNET controller includes both the general MIB acc. to RFC1213 (MIB II) and a special WAGO MIB.

SNMP is processed via port 161. The port number for SNMP traps (agent messages) is 161. Both ports must be enabled to use SNMP.
11.1.2.6.1 MIB II Description

MIB II acc. to RFC1213 is divided into the following groups:

Table 88: MIB II groups

<table>
<thead>
<tr>
<th>Group</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Group</td>
<td>1.3.6.1.2.1.1</td>
</tr>
<tr>
<td>Interface Group</td>
<td>1.3.6.1.2.1.2</td>
</tr>
<tr>
<td>IP Group</td>
<td>1.3.6.1.2.1.4</td>
</tr>
<tr>
<td>IpRoute Table Group</td>
<td>1.3.6.1.2.1.4.21</td>
</tr>
<tr>
<td>ICMP Group</td>
<td>1.3.6.1.2.1.5</td>
</tr>
<tr>
<td>TCP Group</td>
<td>1.3.6.1.2.1.6</td>
</tr>
<tr>
<td>UDP Group</td>
<td>1.3.6.1.2.1.7</td>
</tr>
<tr>
<td>SNMP Group</td>
<td>1.3.6.1.2.1.11</td>
</tr>
</tbody>
</table>
11.1.2.6.2 Traps

**Standard Traps**

For specific events, the SNMP agent will independently send one of the following messages without polling the manager.

---

**Note**

Enable event messages (traps) in the WBM!
Initially enable the event messages in the WBM in menu “SNMP” under “Trap Enable”. Traps in version 1, 2c and 3 may be activated separately.

---

The following messages are triggered automatically as traps (SNMPv1) by the fieldbus coupler/controller:

### Table 89: Standard Traps

<table>
<thead>
<tr>
<th>TrapType/TrapNumber/OID of the provided value</th>
<th>Name</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrapType = 0</td>
<td>ColdStart</td>
<td>Restart the coupler/controller</td>
</tr>
<tr>
<td>TrapType = 1</td>
<td>WarmStart</td>
<td>Reset via mode selector switch (only for controller)</td>
</tr>
<tr>
<td>TrapType = 3</td>
<td>EthernetUp</td>
<td>Network connection detected</td>
</tr>
<tr>
<td>TrapType = 4</td>
<td>AuthenticationFailure</td>
<td>Unauthorized (abortive) MIB access</td>
</tr>
<tr>
<td>TrapType = 6/ab Trap-Nummer 25 benutzerspezifisch</td>
<td>enterpriseSpecific</td>
<td>Enterprise-specific messages and function poll in the PFC program starting with enterprise trap number 25</td>
</tr>
</tbody>
</table>
11.1.3 Application Protocols

If fieldbus specific application protocols are implemented, then the appropriate fieldbus specific communication is possible with the respective coupler/controller. Thus the user is able to have a simple access from the respective fieldbus on the fieldbus node.

The fieldbus specific application protocols implemented in the fieldbus coupler/controller are listed in the following chapters and some special details are described.
11.2 BACnet/IP

The "Building Automation and Control Network", BACnet for short, is a standardized and company-neutral network protocol for building automation, and is originally geared towards the area of heating, ventilation and air conditioning (HVAC).

This protocol has been an ASHRAE standard since 1995, was accepted as a standard by ANSI (ANSI/ASHRAE 135-2004) and has become anchored in the DIN EN ISO standard 16484-5 (Building Automation Systems, Data Communication Protocols). The following chapter refers to the content of the BACnet standard ANSI/ASHRAE 135-2010, DIN EN ISO 16484-5.

For general and further information on the fieldbus and network with BACnet, please refer to the relevant technical literature in the “Literature List”.

All supported features and objects of the "FC BACnet/IP; G4" (750-332) are specified in the document of the corresponding BACnet Protocol Implementation Conformance Statement (PICS).

Additional Information
You can find the corresponding PICS document as a download for your WAGO BACnet product at: www.wago.com.
11.3 Modbus Functions

11.3.1 General

Modbus is a manufacturer-independent, open fieldbus standard for diverse applications in manufacturing and process automation.

The Modbus protocol is implemented according to the current Internet Draft of the IETF (Internet Engineering Task Force) and performs the following functions:

- Transmission of the process image
- Transmission of the fieldbus variables
- Transmission of different settings and information on the coupler/controller

The data transmission in the fieldside takes place via TCP and via UDP.

The Modbus TCP protocol is a variation of the Modbus protocol, which was optimized for communication via TCP/IP connections.

This protocol was designed for data exchange in the field level (i.e. for the exchange of I/O data in the process image).

All data packets are sent via a TCP connection with the port number 502.

Modbus TCP segment

The general Modbus TCP header is as follows:

Table 90: Modbus TCP Header

<table>
<thead>
<tr>
<th>Byte</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8 ... n</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Identifier (entered by receiver)</td>
<td>Protocol-identifier (is always 0)</td>
<td>Length field (High byte, low byte)</td>
<td>Unit identifier (Slave address)</td>
<td>Modbus function code</td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Information

Additional Information
The structure of a datagram is specific for the individual function. Refer to the descriptions of the Modbus Function codes.

For the MODBUS protocol 15 connections are made available over TCP. Thus it allows digital and analog output data to be directly read out at a fieldbus node and special functions to be executed by way of simple MODBUS function codes from 15 stations simultaneously.

For this purpose a set of MODBUS functions from the Open MODBUS/TCP specification is realized.
More information
More information on the “Open MODBUS/TCP specification” you can find in the Internet: [www.modbus.org](http://www.modbus.org).

Therefore the MODBUS protocol based essentially on the following basic data types:

<table>
<thead>
<tr>
<th>Data type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discrete inputs</td>
<td>1 bit</td>
<td>Digital inputs</td>
</tr>
<tr>
<td>Coils</td>
<td>1 bit</td>
<td>Digital outputs</td>
</tr>
<tr>
<td>Input register</td>
<td>16 bits</td>
<td>Analog input data</td>
</tr>
<tr>
<td>Holding register</td>
<td>16 bits</td>
<td>Analog output data</td>
</tr>
</tbody>
</table>

For each basic data type one or more function codes are defined.

These functions allow digital or analog input and output data, and internal variables to be set or directly read out of the fieldbus node.

<table>
<thead>
<tr>
<th>Function code</th>
<th>Designation</th>
<th>Value (hex)</th>
<th>Function</th>
<th>Access method and description</th>
<th>Access to resources (R=read/W=write)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC1</td>
<td>0x01</td>
<td></td>
<td>Read Coils</td>
<td>Reading of several single input bits</td>
<td>R: Process image</td>
</tr>
<tr>
<td>FC2</td>
<td>0x02</td>
<td></td>
<td>Read Discrete Inputs</td>
<td>Reading of several input bits</td>
<td>R: Process image</td>
</tr>
<tr>
<td>FC3</td>
<td>0x03</td>
<td></td>
<td>Read Holding Registers</td>
<td>Reading of several input registers</td>
<td>R: Process image, internal variables</td>
</tr>
<tr>
<td>FC4</td>
<td>0x04</td>
<td></td>
<td>Read Input Registers</td>
<td>Reading of several input registers</td>
<td>R: Process image, internal variables</td>
</tr>
<tr>
<td>FC5</td>
<td>0x05</td>
<td></td>
<td>Write Single Coil</td>
<td>Writing of an individual output bit</td>
<td>W: Process image</td>
</tr>
<tr>
<td>FC6</td>
<td>0x06</td>
<td></td>
<td>Write Single Register</td>
<td>Writing of an individual output register</td>
<td>W: Process image, internal variables</td>
</tr>
<tr>
<td>FC11</td>
<td>0x0B</td>
<td></td>
<td>Get Comm Event Counters</td>
<td>Communication event counter</td>
<td>R: None</td>
</tr>
<tr>
<td>FC15</td>
<td>0x0F</td>
<td></td>
<td>Write Multiple Coils</td>
<td>Writing of several output bits</td>
<td>W: Process image</td>
</tr>
<tr>
<td>FC16</td>
<td>0x10</td>
<td></td>
<td>Write Multiple Registers</td>
<td>Writing of several output registers</td>
<td>W: Process image, internal variables</td>
</tr>
<tr>
<td>FC22</td>
<td>0x16</td>
<td></td>
<td>Mask Write Register</td>
<td>Writing of several bits of an individual output register by mask</td>
<td>W: Process image</td>
</tr>
<tr>
<td>FC23</td>
<td>0x17</td>
<td></td>
<td>Read/Write Multiple Registers</td>
<td>Reading and writing of several output registers</td>
<td>R/W: Process image</td>
</tr>
</tbody>
</table>
To execute a desired function, specify the respective function code and the address of the selected input or output channel or of the register.

---

**Note**

Note the number system when addressing!
The examples listed use the hexadecimal system (i.e.: 0x000) as their numerical format. Addressing begins with 0. The format and beginning of the addressing may vary according to the software and the control system. All addresses then need to be converted accordingly.
11.3.2 Use of the MODBUS Functions

The example below uses a graphical view of a fieldbus node to show which MODBUS functions can be used to access data of the process image.

Figure 52: Use of the MODBUS Functions
Use register functions to access analog signals and coil functions to access binary signals!

It is recommended that analog data be accessed with register functions \( \mathbb{1} \) and digital data with coil functions \( \mathbb{2} \). If reading or writing access to binary signals is performed via register functions \( \mathbb{3} \), an address shift may occur as soon as further analog modules are operated on the coupler/controller.

### 11.3.3 Description of the MODBUS Functions

All MODBUS functions are executed as follows:

1. A MODBUS TCP master (e.g., a PC) makes a request to the WAGO fieldbus node using a specific function code based on the desired operation.

2. The WAGO fieldbus node receives the datagram and then responds to the master with the proper data, which is based on the master’s request.

If the WAGO fieldbus node receives an incorrect request, it sends an error datagram (Exception) to the master. The exception code contained in the exception has the following meaning:

<table>
<thead>
<tr>
<th>Exception code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01</td>
<td>Illegal function</td>
</tr>
<tr>
<td>0x02</td>
<td>Illegal data address</td>
</tr>
<tr>
<td>0x03</td>
<td>Illegal data value</td>
</tr>
<tr>
<td>0x04</td>
<td>Slave device failure</td>
</tr>
<tr>
<td>0x05</td>
<td>Acknowledge</td>
</tr>
<tr>
<td>0x06</td>
<td>Server busy</td>
</tr>
<tr>
<td>0x08</td>
<td>Memory parity error</td>
</tr>
<tr>
<td>0x0A</td>
<td>Gateway path unavailable</td>
</tr>
<tr>
<td>0x0B</td>
<td>Gateway target device failed to respond</td>
</tr>
</tbody>
</table>

The following chapters describe the datagram architecture of request, response and exception with examples for each function code.
**Note**

Reading and writing of outputs via FC1 to FC4 is also possible by adding an offset!

In the case of the read functions (FC1 ... FC4) the outputs can be additionally written and read back by adding an offset of 200hex (0x0200) to the MODBUS addresses in the range of \([0_{\text{hex}} ... \text{FF}_{\text{hex}}]\) and an offset of 1000hex (0x01000) to the MODBUS addresses in the range of \([6000_{\text{hex}} ... 62FC_{\text{hex}}]\).

### 11.3.3.1 Function Code FC1 (Read Coils)

This function reads the status of the input and output bits (coils) in a slave device.

**Request**

The request specifies the reference number (starting address) and the bit count to read.

Example: Read output bits 0 to 7.

Table 94: Request of Function Code FC1

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 0, 1</td>
<td>Transaction identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 2, 3</td>
<td>Protocol identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 4, 5</td>
<td>Length field</td>
<td>0x0006</td>
</tr>
<tr>
<td>Byte 6</td>
<td>Unit identifier</td>
<td>0x01 not used</td>
</tr>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x01</td>
</tr>
<tr>
<td>Byte 8, 9</td>
<td>Reference number</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 10, 11</td>
<td>Bit count</td>
<td>0x0008</td>
</tr>
</tbody>
</table>

**Response**

The current values of the response bits are packed in the data field. A binary 1 corresponds to the ON status and a 0 to the OFF status. The lowest value bit of the first data byte contains the first bit of the request. The others follow in ascending order. If the number of inputs is not a multiple of 8, the remaining bits of the last data byte are filled with zeroes (truncated).

Table 95: Response of Function Code FC1

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x01</td>
</tr>
<tr>
<td>Byte 8</td>
<td>Byte count</td>
<td>0x01</td>
</tr>
<tr>
<td>Byte 9</td>
<td>Bit values</td>
<td>0x12</td>
</tr>
</tbody>
</table>

The status of the inputs 7 to 0 is shown as byte value 0x12 or binary 0001 0010. Input 7 is the bit having the highest significance of this byte and input 0 the
lowest value.
The assignment is thus made from 7 to 0 as follows:

Table 96: Assignment of Inputs

<table>
<thead>
<tr>
<th>Bit</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coil</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bit</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coil</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Exception

Table 97: Exception of Function Code FC1

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>MODBUS function code</td>
<td>0x81</td>
</tr>
<tr>
<td>Byte 7</td>
<td>Exception code</td>
<td>0x01 or 0x02</td>
</tr>
</tbody>
</table>
11.3.3.2 Function Code FC2 (Read Discrete Inputs)

This function reads the input bits from a slave device.

Request

The request specifies the reference number (starting address) and the bit count to be read.

Example: Read input bits 0 to 7

Table 98: Request of Function Code FC2

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 0, 1</td>
<td>Transaction identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 2, 3</td>
<td>Protocol identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 4, 5</td>
<td>Length field</td>
<td>0x0006</td>
</tr>
<tr>
<td>Byte 6</td>
<td>Unit identifier</td>
<td>0x01 not used</td>
</tr>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x02</td>
</tr>
<tr>
<td>Byte 8, 9</td>
<td>Reference number</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 10, 11</td>
<td>Bit count</td>
<td>0x0008</td>
</tr>
</tbody>
</table>

Response

The current value of the requested bits are packed into the data field. A binary 1 corresponds to the ON status and a 0 the OFF status. The lowest value bit of the first data byte contains the first bit of the inquiry. The others follow in an ascending order. If the number of inputs is not a multiple of 8, the remaining bits of the last data byte are filled with zeroes (truncated).

Table 99: Response of Function Code FC2

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x02</td>
</tr>
<tr>
<td>Byte 8</td>
<td>Byte count</td>
<td>0x01</td>
</tr>
<tr>
<td>Byte 9</td>
<td>Bit values</td>
<td>0x12</td>
</tr>
</tbody>
</table>

The status of the inputs 7 to 0 is shown as a byte value 0x12 or binary 0001 0010. Input 7 is the bit having the highest significance of this byte and input 0 the lowest value. The assignment is thus made from 7 to 0 as follows:

Table 100: Assignment of Inputs

<table>
<thead>
<tr>
<th>Bit</th>
<th>OFF</th>
<th>OFF</th>
<th>OFF</th>
<th>ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coil</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
### Exception

Table 101: Exception of Function Code FC2

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x82</td>
</tr>
<tr>
<td>Byte 8</td>
<td>Exception code</td>
<td>0x01 or 0x02</td>
</tr>
</tbody>
</table>
11.3.3.3  Function Code FC3 (Read Multiple Registers)

This function reads the contents of holding registers from a slave device in word format.

Request

The request specifies the reference number (start register) and the word count (register quantity) of the registers to be read. The reference number of the request is zero based, therefore, the first register starts at address 0.

Example: Read registers 0 and 1.

Table 102: Request of Function Code FC3

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 0, 1</td>
<td>Transaction identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 2, 3</td>
<td>Protocol identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 4, 5</td>
<td>Length field</td>
<td>0x0006</td>
</tr>
<tr>
<td>Byte 6</td>
<td>Unit identifier</td>
<td>0x01 not used</td>
</tr>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x03</td>
</tr>
<tr>
<td>Byte 8, 9</td>
<td>Reference number</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 10, 11</td>
<td>Word count</td>
<td>0x0002</td>
</tr>
</tbody>
</table>

Response

The reply register data is packed as 2 bytes per register. The first byte contains the higher value bits, the second the lower values.

Table 103: Response of Function Code FC3

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x03</td>
</tr>
<tr>
<td>Byte 8</td>
<td>Byte count</td>
<td>0x04</td>
</tr>
<tr>
<td>Byte 9, 10</td>
<td>Value register 0</td>
<td>0x1234</td>
</tr>
<tr>
<td>Byte 11, 12</td>
<td>Value register 1</td>
<td>0x2345</td>
</tr>
</tbody>
</table>

The contents of register 0 are displayed by the value 0x1234 and the contents of register 1 is 0x2345.

Exception

Table 104: Exception of Function Code FC3

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x83</td>
</tr>
<tr>
<td>Byte 8</td>
<td>Exception code</td>
<td>0x01 or 0x02</td>
</tr>
</tbody>
</table>
11.3.3.4 Function Code FC4 (Read Input Registers)

This function reads contents of input registers from the slave device in word format.

**Request**

The request specifies a reference number (start register) and the word count (register quantity) of the registers to be read. The reference number of the request is zero based, therefore, the first register starts at address 0.

Example: Read registers 0 and 1

**Table 105: Request of Function Code FC4**

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 0, 1</td>
<td>Transaction identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 2, 3</td>
<td>Protocol identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 4, 5</td>
<td>Length field</td>
<td>0x0006</td>
</tr>
<tr>
<td>Byte 6</td>
<td>Unit identifier</td>
<td>0x01 not used</td>
</tr>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x04</td>
</tr>
<tr>
<td>Byte 8, 9</td>
<td>Reference number</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 10, 11</td>
<td>Word count</td>
<td>0x0002</td>
</tr>
</tbody>
</table>

**Response**

The register data of the response is packed as 2 bytes per register. The first byte has the higher value bits, the second the lower values.

**Table 106: Response of Function Code FC4**

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x04</td>
</tr>
<tr>
<td>Byte 8</td>
<td>Byte count</td>
<td>0x04</td>
</tr>
<tr>
<td>Byte 9, 10</td>
<td>Value register 0</td>
<td>0x1234</td>
</tr>
<tr>
<td>Byte 11, 12</td>
<td>Value register 1</td>
<td>0x2345</td>
</tr>
</tbody>
</table>

The contents of register 0 are shown by the value 0x1234 and the contents of register 1 is 0x2345.

**Exception**

**Table 107: Exception of Function Code FC4**

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x84</td>
</tr>
<tr>
<td>Byte 8</td>
<td>Exception code</td>
<td>0x01 or 0x02</td>
</tr>
</tbody>
</table>
11.3.3.5 Function Code FC5 (Write Coil)

This function writes a single output bit to the slave device.

**Request**

The request specifies the reference number (output address) of output bit to be written. The reference number of the request is zero based; therefore, the first coil starts at address 0.

Example: Turn ON the second output bit (address 1)

<table>
<thead>
<tr>
<th>Table 108: Request of Function Code FC5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Byte</strong></td>
</tr>
<tr>
<td>Byte 0, 1</td>
</tr>
<tr>
<td>Byte 2, 3</td>
</tr>
<tr>
<td>Byte 4, 5</td>
</tr>
<tr>
<td>Byte 6</td>
</tr>
<tr>
<td>Byte 7</td>
</tr>
<tr>
<td>Byte 8, 9</td>
</tr>
<tr>
<td>Byte 10</td>
</tr>
<tr>
<td>Byte 11</td>
</tr>
</tbody>
</table>

**Response**

<table>
<thead>
<tr>
<th>Table 109: Response of Function Code FC5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Byte</strong></td>
</tr>
<tr>
<td>Byte 7</td>
</tr>
<tr>
<td>Byte 8, 9</td>
</tr>
<tr>
<td>Byte 10</td>
</tr>
<tr>
<td>Byte 11</td>
</tr>
</tbody>
</table>

**Exception**

<table>
<thead>
<tr>
<th>Table 110: Exception of Function Code FC5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Byte</strong></td>
</tr>
<tr>
<td>Byte 7</td>
</tr>
<tr>
<td>Byte 8</td>
</tr>
</tbody>
</table>
11.3.3.6 Function Code FC6 (Write Single Register)

This function writes the value of one single output register to a slave device in word format.

Request

The request specifies the reference number (register address) of the first output word to be written. The value to be written is specified in the “Register Value” field. The reference number of the request is zero based; therefore, the first register starts at address 0.

Example: Write a value of 0x1234 to the second output register

Table 111: Request of Function Code FC6

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 0, 1</td>
<td>Transaction identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 2, 3</td>
<td>Protocol identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 4, 5</td>
<td>Length field</td>
<td>0x0006</td>
</tr>
<tr>
<td>Byte 6</td>
<td>Unit identifier</td>
<td>0x01 not used</td>
</tr>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x06</td>
</tr>
<tr>
<td>Byte 8, 9</td>
<td>Reference number</td>
<td>0x0001</td>
</tr>
<tr>
<td>Byte 10, 11</td>
<td>Register value</td>
<td>0x1234</td>
</tr>
</tbody>
</table>

Response

The reply is an echo of the inquiry.

Table 112: Response of Function Code FC6

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x06</td>
</tr>
<tr>
<td>Byte 8, 9</td>
<td>Reference number</td>
<td>0x0001</td>
</tr>
<tr>
<td>Byte 10, 11</td>
<td>Register value</td>
<td>0x1234</td>
</tr>
</tbody>
</table>

Exception

Table 113: Exception of Function Code FC6

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x85</td>
</tr>
<tr>
<td>Byte 8</td>
<td>Exception code</td>
<td>0x01 or 0x02</td>
</tr>
</tbody>
</table>
11.3.3.7 Function Code FC11 (Get Comm Event Counter)

This function returns a status word and an event counter from the slave device's communication event counter. By reading the current count before and after a series of messages, a master can determine whether the messages were handled normally by the slave.

Following each successful new processing, the counter counts up. This counting process is not performed in the case of exception replies, poll commands or counter inquiries.

**Request**

Table 114: Request of Function code FC11

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 0, 1</td>
<td>Transaction identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 2, 3</td>
<td>Protocol identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 4, 5</td>
<td>Length field</td>
<td>0x0002</td>
</tr>
<tr>
<td>Byte 6</td>
<td>Unit identifier</td>
<td>0x01 not used</td>
</tr>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x0B</td>
</tr>
</tbody>
</table>

**Response**

The reply contains a 2-byte status word and a 2-byte event counter. The status word only contains zeroes.

Table 115: Response of Function Code FC11

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x0B</td>
</tr>
<tr>
<td>Byte 8, 9</td>
<td>Status</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 10, 11</td>
<td>Event count</td>
<td>0x0003</td>
</tr>
</tbody>
</table>

The event counter shows that 3 (0x0003) events were counted.

**Exception**

Table 116: Exception of Function Code FC11

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x85</td>
</tr>
<tr>
<td>Byte 8</td>
<td>Exception code</td>
<td>0x01 or 0x02</td>
</tr>
</tbody>
</table>
11.3.3.8 Function Code FC15 (Write Multiple Coils)

This function sets a sequence of output bits to 1 or 0 in a slave device. The maximum number is 256 bits.

Request

The request message specifies the reference number (first coil in the sequence), the bit count (number of bits to be written), and the output data. The output coils are zero-based; therefore, the first output point is 0.

In this example 16 bits are set, starting with the address 0. The request contains 2 bytes with the value 0xA5F0, or 1010 0101 1111 0000 in binary format.

The first data byte transmits the value of 0xA5 to the addresses 7 to 0, whereby 0 is the lowest value bit. The next byte transmits 0xF0 to the addresses 15 to 8, whereby the lowest value bit is 8.

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 0, 1</td>
<td>Transaction identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 2, 3</td>
<td>Protocol identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 4, 5</td>
<td>Length field</td>
<td>0x0009</td>
</tr>
<tr>
<td>Byte 6</td>
<td>Unit identifier</td>
<td>0x01 not used</td>
</tr>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x0F</td>
</tr>
<tr>
<td>Byte 8, 9</td>
<td>Reference number</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 10, 11</td>
<td>Bit count</td>
<td>0x0010</td>
</tr>
<tr>
<td>Byte 12</td>
<td>Byte count</td>
<td>0x02</td>
</tr>
<tr>
<td>Byte 13</td>
<td>Data byte1</td>
<td>0xA5</td>
</tr>
<tr>
<td>Byte 14</td>
<td>Data byte2</td>
<td>0xF0</td>
</tr>
</tbody>
</table>

Response

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x0F</td>
</tr>
<tr>
<td>Byte 8, 9</td>
<td>Reference number</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 10, 11</td>
<td>Bit count</td>
<td>0x0010</td>
</tr>
</tbody>
</table>
## Exception

Table 119: Exception of Function Code FC15

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x8F</td>
</tr>
<tr>
<td>Byte 8</td>
<td>Exception code</td>
<td>0x01 or 0x02</td>
</tr>
</tbody>
</table>
11.3.3.9 **Function Code FC16 (Write Multiple Registers)**

This function writes a sequence of registers in a slave device in word format.

**Request**

The Request specifies the reference number (starting register), the word count (number of registers to write), and the register data. The data is sent as 2 bytes per register. The registers are zero-based; therefore, the first output is at address 0.

Example: Set data in registers 0 and 1

Table 120: Request of Function Code FC16

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 0, 1</td>
<td>Transaction identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 2, 3</td>
<td>Protocol identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 4, 5</td>
<td>Length field</td>
<td>0x000B</td>
</tr>
<tr>
<td>Byte 6</td>
<td>Unit identifier</td>
<td>0x01 not used</td>
</tr>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x10</td>
</tr>
<tr>
<td>Byte 8, 9</td>
<td>Reference number</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 10, 11</td>
<td>Word count</td>
<td>0x0002</td>
</tr>
<tr>
<td>Byte 12</td>
<td>Byte count</td>
<td>0x04</td>
</tr>
<tr>
<td>Byte 13, 14</td>
<td>Register value 1</td>
<td>0x1234</td>
</tr>
<tr>
<td>Byte 15, 16</td>
<td>Register value 2</td>
<td>0x2345</td>
</tr>
</tbody>
</table>

**Response**

Table 121: Response of Function Code FC16

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x10</td>
</tr>
<tr>
<td>Byte 8, 9</td>
<td>Reference number</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 10, 11</td>
<td>Word count</td>
<td>0x0002</td>
</tr>
</tbody>
</table>

**Exception**

Table 122: Exception of Function Code FC16

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x85</td>
</tr>
<tr>
<td>Byte 8</td>
<td>Exception code</td>
<td>0x01 or 0x02</td>
</tr>
</tbody>
</table>
11.3.3.10 Function Code FC22 (Mask Write Register)

This function manipulates individual bits within a register using a combination of an AND mask, an OR mask, and the register's current content.

Request

Table 123: Request of Function Code FC22

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 0, 1</td>
<td>Transaction identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 2, 3</td>
<td>Protocol identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 4, 5</td>
<td>Length field</td>
<td>0x0002</td>
</tr>
<tr>
<td>Byte 6</td>
<td>Unit identifier</td>
<td>0x01 not used</td>
</tr>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x16</td>
</tr>
<tr>
<td>Byte 8, 9</td>
<td>Reference number</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 10, 11</td>
<td>AND mask</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 12, 13</td>
<td>OR mask</td>
<td>0xAAAA</td>
</tr>
</tbody>
</table>

Response

Table 124: Response of Function Code FC22

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x10</td>
</tr>
<tr>
<td>Byte 8, 9</td>
<td>Reference number</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 10, 11</td>
<td>AND mask</td>
<td>0x0000</td>
</tr>
<tr>
<td>Byte 12, 13</td>
<td>OR mask</td>
<td>0xAAAA</td>
</tr>
</tbody>
</table>

Exception

Table 125: Exception of Function Code FC22

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 7</td>
<td>MODBUS function code</td>
<td>0x85</td>
</tr>
<tr>
<td>Byte 8</td>
<td>Exception code</td>
<td>0x01 or 0x02</td>
</tr>
</tbody>
</table>
11.3.3.11 Function Code FC23 (Read/Write Multiple Registers)

This function performs a combination of a read and write operation in a single request. The function can write the new data to a group registers, and then return the data of a different group. The write operation is performed before the read.

Request

The reference numbers (addresses) are zero-based in the request message; therefore, the first register is at address 0. The request message specifies the registers to read and write. The data is sent as 2 bytes per register.

Example: The data in register 3 is set to value 0x0123, and values 0x0004 and 0x5678 are read out of the two registers 0 and 1.

Table 126: Request of Function Code FC23

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>0, 1</td>
<td>Transaction identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>2, 3</td>
<td>Protocol identifier</td>
<td>0x0000</td>
</tr>
<tr>
<td>4, 5</td>
<td>Length field</td>
<td>0x000D</td>
</tr>
<tr>
<td>6</td>
<td>Unit identifier</td>
<td>0x01 not used</td>
</tr>
<tr>
<td>7</td>
<td>MODBUS function code</td>
<td>0x17</td>
</tr>
<tr>
<td>8, 9</td>
<td>Reference number for read</td>
<td>0x0000</td>
</tr>
<tr>
<td>10, 11</td>
<td>Word count for read (1…125)</td>
<td>0x0002</td>
</tr>
<tr>
<td>12, 13</td>
<td>Reference number for write</td>
<td>0x0003</td>
</tr>
<tr>
<td>14, 15</td>
<td>Word count for write (1…100)</td>
<td>0x0001</td>
</tr>
<tr>
<td>16</td>
<td>Byte count (2 x word count for write)</td>
<td>0x02</td>
</tr>
<tr>
<td>17...(B+16)</td>
<td>Register values (B = Byte count)</td>
<td>0x0123</td>
</tr>
</tbody>
</table>

Response

Table 127: Response of Function Code FC23

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>MODBUS function code</td>
<td>0x17</td>
</tr>
<tr>
<td>8</td>
<td>Byte count (2 x word count for read)</td>
<td>0x04</td>
</tr>
<tr>
<td>9...(B+1)</td>
<td>Register values (B = Byte count)</td>
<td>0x0004 or 0x5678</td>
</tr>
</tbody>
</table>

Exception

Table 128: Exception of Function Code FC23

<table>
<thead>
<tr>
<th>Byte</th>
<th>Field name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>MODBUS function code</td>
<td>0x97</td>
</tr>
<tr>
<td>8</td>
<td>Exception code</td>
<td>0x01 or 0x02</td>
</tr>
</tbody>
</table>
Note

Note that if the register ranges overlap, the results are undefined!
If register areas for read and write overlap, the results are undefined.
11.3.4 MODBUS Register Mapping

The following tables display the MODBUS addressing and the internal variables.

Via the register services the states of the complex and digital I/O modules can be determined or changed.

Register Access Reading (with FC3 and FC4)

Table 129: Register Access Reading (with FC3 and FC4)

<table>
<thead>
<tr>
<th>MODBUS address [dec]</th>
<th>MODBUS address [hex]</th>
<th>IEC 61131 address</th>
<th>Memory range</th>
</tr>
</thead>
<tbody>
<tr>
<td>0...255</td>
<td>0x0000...0x00FF</td>
<td>%IW0...%IW255</td>
<td>Physical input area (1) First 256 Words of physical input data</td>
</tr>
<tr>
<td>256...511</td>
<td>0x0100...0x01FF</td>
<td></td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>512...767</td>
<td>0x0200...0x02FF</td>
<td>%QW0...%QW255</td>
<td>Physical output area (1) First 256 Words of physical output data</td>
</tr>
<tr>
<td>768...4095</td>
<td>0x0300...0x0FFF</td>
<td></td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>4096...12287</td>
<td>0x0400...0x0FFF</td>
<td></td>
<td>Configuration register (see Section &quot;Configuration Register&quot;)</td>
</tr>
<tr>
<td>12288...24575</td>
<td>0x0500...0x5FFF</td>
<td></td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>24576...25339</td>
<td>0x0600...0x62FF</td>
<td>%IW256...%IW1020</td>
<td>Physical input area (2) Additional 764 Words physical input data</td>
</tr>
<tr>
<td>25340...28671</td>
<td>0x062F...0x6FFF</td>
<td></td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>28672...29435</td>
<td>0x0700...0x72FF</td>
<td>%QW256...%QW1020</td>
<td>Physical output area (2) Additional 764 Words physical output data</td>
</tr>
<tr>
<td>29436...65535</td>
<td>0x072F...0xFFFF</td>
<td></td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
</tbody>
</table>
### Register Access Writing (with FC6 and FC16)

The digital MODBUS services (coil services) are bit accesses, with which only the states of digital I/O modules can be determined or changed. Complex I/O modules are not attainable with these services and so they are ignored. Because of this the addressing of the digital channels begins again with 0, so that the MODBUS address is always identical to the channel number, (i.e. the digital input no. 47 has the MODBUS address "46").

<table>
<thead>
<tr>
<th>MODBUS address [dec]</th>
<th>MODBUS address [hex]</th>
<th>IEC 61131 address</th>
<th>Memory range</th>
</tr>
</thead>
<tbody>
<tr>
<td>0...255</td>
<td>0x0000...0x00FF</td>
<td>%QW0...%QW255</td>
<td>Physical output area (1) First 256 Words of physical output data</td>
</tr>
<tr>
<td>256...511</td>
<td>0x0100...0x01FF</td>
<td>-</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>512...767</td>
<td>0x0200...0x02FF</td>
<td>%QW0...%QW255</td>
<td>Physical output area (1) First 256 Words of physical output data</td>
</tr>
<tr>
<td>768...4095</td>
<td>0x0300...0x0FFF</td>
<td>-</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>4096...12287</td>
<td>0x1000...0x1FFF</td>
<td>-</td>
<td>Configuration register (see Section &quot;Configuration Register&quot;)</td>
</tr>
<tr>
<td>12288...24575</td>
<td>0x2000...0x2FFF</td>
<td>-</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>24576...25339</td>
<td>0x6000...0x62FF</td>
<td>%QW256...%QW1020</td>
<td>Physical output area (2) Additional 764 Words physical output data</td>
</tr>
<tr>
<td>25340...28671</td>
<td>0x62FC...0x6FFF</td>
<td>-</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>28672...29435</td>
<td>0x7000...0x72FB</td>
<td>%QW256...%QW1020</td>
<td>Physical output area (2) Additional 764 Words physical output data</td>
</tr>
<tr>
<td>29436...65535</td>
<td>0x72FC...0xFFFF</td>
<td>-</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
</tbody>
</table>
### Bit Access Reading (with FC1 and FC2)

Table 131: Bit Access Reading (with FC1 and FC2)

<table>
<thead>
<tr>
<th>MODBUS address [dec]</th>
<th>Memory range [hex]</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0...511</td>
<td>0x0000...0x01FF</td>
<td>Physical input area (1) First 512 digital inputs</td>
</tr>
<tr>
<td>512...1023</td>
<td>0x0200...0x03FF</td>
<td>Physical output area (1) First 512 digital outputs</td>
</tr>
<tr>
<td>1024...12287</td>
<td>0x0400...0x2FFFF</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>12288...13815</td>
<td>0x0300...0x35F7</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>13816...16383</td>
<td>0x035F8...0x3FFFF</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>16384...17911</td>
<td>0x04000...0x45F7</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>17912...32767</td>
<td>0x045F8...0x7FFFF</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>0x8000...0x85F7</td>
<td></td>
<td>Physical input area (2) Starts with the 513th and ends with the 2039th digital input</td>
</tr>
<tr>
<td>0x85F8...0x8FFFF</td>
<td></td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>0x9000...0x95F7</td>
<td></td>
<td>Physical output area (2) Starts with the 513th and ends with the 2039th digital output</td>
</tr>
<tr>
<td>0x95F8...0xFFFF</td>
<td></td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
</tbody>
</table>

### Bit Access Writing (with FC5 and FC15)

Table 132: Bit Access Writing (with FC5 and FC15)

<table>
<thead>
<tr>
<th>MODBUS address [dec]</th>
<th>Memory range [hex]</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0...511</td>
<td>0x0000...0x01FF</td>
<td>Physical output area (1) First 512 digital outputs</td>
</tr>
<tr>
<td>512...1023</td>
<td>0x0200...0x03FF</td>
<td>Physical output area (1) First 512 digital outputs</td>
</tr>
<tr>
<td>1024...12287</td>
<td>0x04000...0x2FFFF</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>12288...13815</td>
<td>0x03000...0x35F7</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>13816...16383</td>
<td>0x035F8...0x3FFFF</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>16384...17911</td>
<td>0x04000...0x45F7</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>17912...32767</td>
<td>0x045F8...0x7FFFF</td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>0x8000...0x85F7</td>
<td></td>
<td>Physical input area (2) Starts with the 513th and ends with the 2039th digital output</td>
</tr>
<tr>
<td>0x85F8...0x8FFFF</td>
<td></td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
<tr>
<td>0x9000...0x95F7</td>
<td></td>
<td>Physical output area (2) Starts with the 513th and ends with the 2039th digital output</td>
</tr>
<tr>
<td>0x95F8...0xFFFF</td>
<td></td>
<td>MODBUS exception: &quot;Illegal data address&quot;</td>
</tr>
</tbody>
</table>
### 11.3.5 Modbus Registers

Table 133: Modbus Registers

<table>
<thead>
<tr>
<th>Register address</th>
<th>Access</th>
<th>Length (Word)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x1000</td>
<td>R/W</td>
<td>1</td>
<td>Watchdog time read/write</td>
</tr>
<tr>
<td>0x1001</td>
<td>R/W</td>
<td>1…2</td>
<td>Watchdog coding mask 1…16</td>
</tr>
<tr>
<td>0x1002</td>
<td>R/W</td>
<td>1</td>
<td>Watchdog coding mask 17…32</td>
</tr>
<tr>
<td>0x1003</td>
<td>R/W</td>
<td>1</td>
<td>Watchdog trigger</td>
</tr>
<tr>
<td>0x1004</td>
<td>R</td>
<td>1</td>
<td>Minimum trigger time</td>
</tr>
<tr>
<td>0x1005</td>
<td>R/W</td>
<td>1</td>
<td>Watchdog stop (Write sequence 0xAAAA, 0x5555)</td>
</tr>
<tr>
<td>0x1006</td>
<td>R</td>
<td>1</td>
<td>Watchdog status</td>
</tr>
<tr>
<td>0x1007</td>
<td>R/W</td>
<td>1</td>
<td>Restart watchdog (Write sequence 0x1)</td>
</tr>
<tr>
<td>0x1008</td>
<td>R/W</td>
<td>1</td>
<td>Stop watchdog (Write sequence 0x55AA or 0xAA55)</td>
</tr>
<tr>
<td>0x1009</td>
<td>R/W</td>
<td>1</td>
<td>Modbus and HTTP close at watchdog time-out</td>
</tr>
<tr>
<td>0x100A</td>
<td>R/W</td>
<td>1</td>
<td>Watchdog configuration</td>
</tr>
<tr>
<td>0x100B</td>
<td>W</td>
<td>1</td>
<td>Save watchdog parameter (Write sequence 0x55AA or 0xAA55)</td>
</tr>
<tr>
<td>0x1020</td>
<td>R</td>
<td>1…2</td>
<td>LED error code</td>
</tr>
<tr>
<td>0x1021</td>
<td>R</td>
<td>1</td>
<td>LED error argument</td>
</tr>
<tr>
<td>0x1022</td>
<td>R</td>
<td>1…4</td>
<td>Number of analog output data in the process image (in bits)</td>
</tr>
<tr>
<td>0x1023</td>
<td>R</td>
<td>1…3</td>
<td>Number of analog input data in the process image (in bits)</td>
</tr>
<tr>
<td>0x1024</td>
<td>R</td>
<td>1…2</td>
<td>Number of digital output data in the process image (in bits)</td>
</tr>
<tr>
<td>0x1025</td>
<td>R</td>
<td>1</td>
<td>Number of digital input data in the process image (in bits)</td>
</tr>
<tr>
<td>0x1029</td>
<td>R/W</td>
<td>1…9</td>
<td>Modbus TCP statistics (Write sequence 0x55AA or 0xAA55)</td>
</tr>
<tr>
<td>0x102A</td>
<td>R</td>
<td>1</td>
<td>Number of TCP connections</td>
</tr>
<tr>
<td>0x102B</td>
<td>W</td>
<td>1</td>
<td>KBUS Reset</td>
</tr>
<tr>
<td>0x1030</td>
<td>R/W</td>
<td>1</td>
<td>Configuration MODBUS/TCP time-out</td>
</tr>
<tr>
<td>0x1031</td>
<td>R</td>
<td>1…3</td>
<td>Read out the MAC-ID of the coupler/controller</td>
</tr>
<tr>
<td>0x1037</td>
<td>R/W</td>
<td>1</td>
<td>Modbus Response Delay (ms)</td>
</tr>
<tr>
<td>0x1038</td>
<td>R</td>
<td>1</td>
<td>Modbus TOS</td>
</tr>
<tr>
<td>0x1050</td>
<td>R</td>
<td>3</td>
<td>Diagnosis of the connected I/O modules</td>
</tr>
<tr>
<td>0x2000</td>
<td>R</td>
<td>1…9</td>
<td>Constant 0x0000</td>
</tr>
<tr>
<td>0x2001</td>
<td>R</td>
<td>1…8</td>
<td>Constant 0xFFFF</td>
</tr>
<tr>
<td>0x2002</td>
<td>R</td>
<td>1…7</td>
<td>Constant 0x1234</td>
</tr>
<tr>
<td>0x2003</td>
<td>R</td>
<td>1…6</td>
<td>Constant 0xAAAA</td>
</tr>
<tr>
<td>0x2004</td>
<td>R</td>
<td>1…5</td>
<td>Constant 0x5555</td>
</tr>
<tr>
<td>0x2005</td>
<td>R</td>
<td>1…4</td>
<td>Constant 0x7FFF</td>
</tr>
<tr>
<td>0x2006</td>
<td>R</td>
<td>1…3</td>
<td>Constant 0x8000</td>
</tr>
<tr>
<td>0x2007</td>
<td>R</td>
<td>1…2</td>
<td>Constant 0x3FFF</td>
</tr>
<tr>
<td>0x2008</td>
<td>R</td>
<td>1</td>
<td>Constant 0x4000</td>
</tr>
<tr>
<td>0x2010</td>
<td>R</td>
<td>1</td>
<td>Firmware version</td>
</tr>
<tr>
<td>0x2011</td>
<td>R</td>
<td>1</td>
<td>Series code</td>
</tr>
<tr>
<td>0x2012</td>
<td>R</td>
<td>1</td>
<td>Coupler/controller code</td>
</tr>
<tr>
<td>0x2013</td>
<td>R</td>
<td>1</td>
<td>Firmware version major revision</td>
</tr>
<tr>
<td>0x2014</td>
<td>R</td>
<td>1</td>
<td>Firmware version minor revision</td>
</tr>
</tbody>
</table>
Table 134: MODBUS registers (Continuation)

<table>
<thead>
<tr>
<th>Register address</th>
<th>Access</th>
<th>Length (Word)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x2020</td>
<td>R</td>
<td>1...16</td>
<td>Short description controller</td>
</tr>
<tr>
<td>0x2021</td>
<td>R</td>
<td>1...8</td>
<td>Compile time of the firmware</td>
</tr>
<tr>
<td>0x2022</td>
<td>R</td>
<td>1...8</td>
<td>Compile date of the firmware</td>
</tr>
<tr>
<td>0x2023</td>
<td>R</td>
<td>1...32</td>
<td>Indication of the firmware loader</td>
</tr>
<tr>
<td>0x2030</td>
<td>R</td>
<td>1...65</td>
<td>Description of the connected I/O modules (module 0…64)</td>
</tr>
<tr>
<td>0x2031</td>
<td>R</td>
<td>1...64</td>
<td>Description of the connected I/O modules (module 65…128)</td>
</tr>
<tr>
<td>0x2032</td>
<td>R</td>
<td>1...64</td>
<td>Description of the connected I/O modules (module 129…192)</td>
</tr>
<tr>
<td>0x2033</td>
<td>R</td>
<td>1...63</td>
<td>Description of the connected I/O modules (module 193…255)</td>
</tr>
<tr>
<td>0x2035</td>
<td>R/W</td>
<td>1</td>
<td>Process image settings table 0 register 3</td>
</tr>
<tr>
<td>0x2036</td>
<td>R</td>
<td></td>
<td>Fieldbus coupler/controller diagnostics</td>
</tr>
<tr>
<td>0x2040</td>
<td>W</td>
<td>1</td>
<td>Software reset (Write sequence 0x55AA or 0xAA55)</td>
</tr>
<tr>
<td>0x2043</td>
<td>W</td>
<td>1</td>
<td>Factory settings</td>
</tr>
</tbody>
</table>
11.3.5.1 Accessing Register Values

You can use any den Modbus application to access (read from or write to) register values. Both commercial (e.g., “Modscan”) and free programs (from http://www.modbus.org/tech.php) are available.

The following sections describe the Modbus watchdog and how to access both the registers and their values.

11.3.5.2 Modbus-Watchdog

With the aid of the Modbus watchdog, it is possible to monitor whether communication takes place with Modbus function codes with a specific regularity. If the communication lapses for a given time, it is called a "time-out", which is considered fieldbus failure. In general, the Modbus watchdog ensures that all analog output modules in the fieldbus node are set to "0" and all digital output modules are set to logical "Off". At the same time, the user is informed about the time-out via the WBM as well as via a status register (0x1006).

An internal timer is used to monitor the time-out. This timer is set to a certain maximum time (register 0x1000) and started at the beginning of the monitoring. If communication with a Modbus function code to be monitored occurs before reaching the maximum time, the timer starts again at "0". However, only the function codes selected in the coding mask (0x1001) are monitored (respective bit = '1'). All other function codes keep the timer running or, unlike the selected function codes, do not restart the watchdog after a time-out.

The head station’s behavior after a time-out is defined by the initial choice of two possible operating modes (“Standard”/“Alternative”) and by an additional parameter for the TCP interface (register 0x1009, "MODBUS and HTTP close for Modbus Watchdog time-out").

- **Behavior 1 (lowest restriction):**
  After a Modbus watchdog time-out, all analog and digital output modules are set to "0" or "Off", however, the Modbus watchdog is immediately restarted the next time a function code is sent (provided the function code in the coding mask (0x1001) is selected).

  => Select the operating mode "Alternative",
  => Set register 0x1009 to the value '0'.

  When reading the status register (0x1006), the correct value is read first: "2" = "Watchdog expired". Because this restarts the Modbus watchdog, the next read would result in "1" = "watchdog active".

- **Behavior 2 (medium restriction):**
  Further communication in relation to process data should be prevented.
Any attempt to access process data via Modbus function codes should be answered with an error.

=> Select the operating mode "Standard" for this.

However, the Modbus TCP connection will still work to access the Modbus configuration and status registers.

=> Set the register 0x1009 to the value '0'.

Access to the Modbus watchdog registers is still possible after a Modbus watchdog time-out, although Modbus function codes are also sent in this case.

For all other Modbus TCP/IP requests, the head station responds with the exception code 0x0004 ("Slave Device Failure").

- **Behavior 3 (highest restriction):**
  Further communication in relation to process data should be prevented. Any attempt to access process data via Modbus function codes should be answered with an error.

  => Select the operating mode "Standard" for this.

  In addition, the TCP connection should also be closed to prevent access to the Modbus watchdog registers. For example thereby a restart of the Modbus watchdog is not possible without a previous TCP reconnection.

  => Set the register 0x1009 to the value '1'.

  After renewed TCP connection, in the "Standard" operating mode the Modbus watchdog is still in the "expired" status and must be restarted (register 0x1003 or 0x1007).

### 11.3.5.3 Modbus Watchdog Register

The watchdog registers can be addressed analogously with the described Modbus function codes (read and write). Instead of the address of an I/O module channel, the respective register address is therefore specified.

<table>
<thead>
<tr>
<th>Table 135: Register Address 0x1000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Register address 0x1000 (4096 dec)</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
Table 136: Register Address 0x1001

<table>
<thead>
<tr>
<th>Register address 0x1001 (4097&lt;sub&gt;dec&lt;/sub&gt;)</th>
<th>Value</th>
<th>Access</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Watchdog function coding mask, function code 1...16, WDFCM_1_16</td>
<td>Read/write</td>
<td>0xFFFF</td>
<td>Using this mask, the function codes can be set to trigger the watchdog function. The function code can be selected via a &quot;1&quot;</td>
</tr>
<tr>
<td>FC 1 Bit 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 2 Bit 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 3 Bit 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 4 Bit 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 5 Bit 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 16 Bit 15</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Changes to the register value can only be made if the watchdog is deactivated. The bit pattern stored in the register defines the function codes that trigger the watchdog. Some function codes are not supported. For those the watchdog will not be triggered even if another Modbus device transmits one of them. When switching the watchdog type from "Standard" to "Alternative", the coding mask is reset to default value 0xFFFF.

Table 137: Register Address 0x1002

<table>
<thead>
<tr>
<th>Register address 0x1002 (4098&lt;sub&gt;dec&lt;/sub&gt;)</th>
<th>Value</th>
<th>Access</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Watchdog function coding mask, function code 17...32, WD_FCM_17_32</td>
<td>Read/write</td>
<td>0xFFFF</td>
<td>Same function as above, however, with the function codes 17 to 32.</td>
</tr>
<tr>
<td>FC 17 Bit 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 18 Bit 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 32 Bit 15</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

These codes are currently not supported, for this reason the default value should not be changed. Changes to the register value can only be made if the watchdog is deactivated. It is not possible to modify this value while the watchdog is running.

Table 138: Register Address 0x1003

<table>
<thead>
<tr>
<th>Register address 0x1003 (4099&lt;sub&gt;dec&lt;/sub&gt;)</th>
<th>Value</th>
<th>Access</th>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Watchdog trigger, WD_TRIGGER</td>
<td>Read/write</td>
<td>0x0000</td>
<td>This register is used for an alternative trigger method. The watchdog is triggered by writing different values in this register. Values following each other must differ in size. Writing of a value not equal to zero starts the watchdog after a Power-on. For a restart the written value must necessarily be unequal the before written value! A watchdog fault is reset and writing process data is possible again.</td>
</tr>
</tbody>
</table>
Table 139: Register Address 0x1004

<table>
<thead>
<tr>
<th>Register address 0x1004 (4100dez)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Standard</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

Table 140: Register Address 0x1005

<table>
<thead>
<tr>
<th>Register address 0x1005 (4101dez)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Standard</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

Table 141: Register Address 0x1006

<table>
<thead>
<tr>
<th>Register address 0x1006 (4102dez)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Standard</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

Table 142: Register Address 0x1007

<table>
<thead>
<tr>
<th>Register address 0x1007 (4103dez)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Standard</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

Table 143: Register Address 0x1008

<table>
<thead>
<tr>
<th>Register address 0x1008 (4104dez)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Standard</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
Table 144: Register Address 0x1009

<table>
<thead>
<tr>
<th>Register address 0x1009 (4105&lt;sub&gt;dec&lt;/sub&gt;)</th>
<th>Value</th>
<th>Access</th>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Close Modbus socket after watchdog timeout</td>
<td>Read/write</td>
<td>0x0000</td>
<td>0: Modbus socket is not closed</td>
</tr>
</tbody>
</table>

Table 145: Register Address 0x100A

<table>
<thead>
<tr>
<th>Register address 0x100A (4106&lt;sub&gt;dec&lt;/sub&gt;)</th>
<th>Value</th>
<th>Access</th>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Watchdog type Standard/Alternative</td>
<td>Read/write</td>
<td>0x0000</td>
<td>0: Modbus watchdog type &quot;Standard&quot;</td>
</tr>
</tbody>
</table>

The length of each register is 1 word; i.e., with each access only one word can be written or read. Following are two examples of how to set the value for a time overrun:

**Setting the watchdog for a timeout of more than 1 second:**

1. Write 0x000A in the register for time overrun (0x1000).
   - Register 0x1000 works with a multiple of 100 ms;
   - 1 s = 1000 ms; 1000 ms / 100 ms = 10<sub>dec</sub> = A<sub>hex</sub>

2. Use the function code 5 to write 0x0010 (=2<sup>(5-1)</sup>) in the coding mask (register 0x1001).

Table 146: Starting Watchdog

<table>
<thead>
<tr>
<th>FC Bit</th>
<th>FC16</th>
<th>FC15</th>
<th>FC14</th>
<th>FC13</th>
<th>FC12</th>
<th>FC11</th>
<th>FC10</th>
<th>FC9</th>
<th>FC8</th>
<th>FC7</th>
<th>FC6</th>
<th>FC5</th>
<th>FC4</th>
<th>FC3</th>
<th>FC2</th>
<th>FC1</th>
</tr>
</thead>
<tbody>
<tr>
<td>bin</td>
<td>15</td>
<td>14</td>
<td>13</td>
<td>12</td>
<td>11</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>hex</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Function code 5 (writing a digital output bit) continuously triggers the watchdog to restart the watchdog timer again and again within the specified time. If time between requests exceeds 1 second, a watchdog timeout error occurs.

3. To stop the watchdog, write the value 0xAA55 or 0x55AA into 0x1008
   (Simply Stop Watchdog register, WD_AC_STOP_SIMPLE).
Setting the watchdog for a timeout of 10 minutes or more:

1. Write 0x1770 (= 10*60*1000 ms / 100 ms) in the register for time overrun (0x1000).
   (Register 0x1000 works with a multiple of 100 ms; 10 min = 600,000 ms; 600,000 ms / 100 ms = 6000dec = 1770hex)

2. Write 0x0001 in the watchdog trigger register (0x1003) to start the watchdog.

3. Write different values (e.g., counter values 0x0000, 0x0001) in the watchdog to trigger register (0x1003).

   Values following each other must differ in size. Writing of a value not equal to zero starts the watchdog. Watchdog faults are reset and writing process data is possible again.

4. To stop the watchdog, write the value 0xAA55 or 0x55AA into 0x1008 (Simply Stop Watchdog register, WD_AC_STOP_SIMPLE).

<table>
<thead>
<tr>
<th>Table 147: Register Address 0x100B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Register address 0x100B (4107_{dez})</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Standard</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
11.3.5.4  Diagnostic Registers

The following registers can be read to determine errors in the node:

Table 148: Register Address 0x1020

<table>
<thead>
<tr>
<th>Value</th>
<th>LedErrCode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Read</td>
</tr>
<tr>
<td>Description</td>
<td>Declaration of the error code</td>
</tr>
</tbody>
</table>

Table 149: Register Address 0x1021

<table>
<thead>
<tr>
<th>Value</th>
<th>LedErrArg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Read</td>
</tr>
<tr>
<td>Description</td>
<td>Declaration of the error argument</td>
</tr>
</tbody>
</table>
11.3.5.5 Configuration Registers

The following registers contain configuration information of the connected modules:

Table 150: Register Address 0x1022

<table>
<thead>
<tr>
<th>Register address 0x1022 (4130 dec)</th>
<th>Value</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CnfLen.AnalogOut</td>
<td>Read</td>
<td>Number of word-based outputs registers in the process image in bits (divide by 16 to get the total number of analog words)</td>
</tr>
</tbody>
</table>

Table 151: Register Address 0x1023

<table>
<thead>
<tr>
<th>Register address 0x1023 (4131 dec)</th>
<th>Value</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CnfLen.AnalogInp</td>
<td>Read</td>
<td>Number of word-based inputs registers in the process image in bits (divide by 16 to get the total number of analog words)</td>
</tr>
</tbody>
</table>

Table 152: Register Address 0x1024

<table>
<thead>
<tr>
<th>Register address 0x1024 (4132 dec)</th>
<th>Value</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CnfLen.DigitalOut</td>
<td>Read</td>
<td>Number of digital output bits in the process image</td>
</tr>
</tbody>
</table>

Table 153: Register Address 0x1025

<table>
<thead>
<tr>
<th>Register address 0x1025 (4133 dec)</th>
<th>Value</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CnfLen.DigitalInp</td>
<td>Read</td>
<td>Number of digital input bits in the process image</td>
</tr>
</tbody>
</table>

Table 154: Register Address 0x1029

<table>
<thead>
<tr>
<th>Register Address 0x1029 (4137 dec) with 9 Words</th>
<th>Value</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MODBUS TCP statistics</td>
<td>Read/write</td>
<td>1 word SlaveDeviceFailure → local bus error, fieldbus error by activated watchdog</td>
</tr>
<tr>
<td></td>
<td>1 word BadProtocol → error in the MODBUS TCP header</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 word BadLength → Wrong telegram length</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 word BadFunction → Invalid function code</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 word BadAddress → Invalid register address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 word BadData → Invalid value</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 word TooManyRegisters → Number of the registers which can be worked on is too large, Read/Write 125/100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 word TooManyBits → Number of the coils which can be worked on is too large, Read/Write 2000/800</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 word ModTcpMessageCounter → Number of received MODBUS/TCP requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>By writing 0xAA55 or 0x55AA the register is reset.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 155: Register Address 0x102A

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MODBUS/TCP connections</td>
<td>Number of TCP connections</td>
</tr>
</tbody>
</table>

Table 156: Register Address 0x102B

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local bus reset</td>
<td>Writing of this register restarts the local bus</td>
</tr>
</tbody>
</table>

Table 157: Register Address 0x1030

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration MODBUS/TCP time-out</td>
<td>This is the maximum number of milliseconds the fieldbus coupler will allow a MODBUS/TCP connection to stay open without receiving a MODBUS request. Upon time-out, idle connection will be closed. Outputs remain in last state. Default value is 600 ms (60 seconds), the time base is 100 ms, the minimal value is 100 ms. If the value is set to '0', the timeout is disabled. On this connection, the watchdog is triggered with a request.</td>
</tr>
</tbody>
</table>

Table 158: Register Address 0x1031

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read the MAC-ID of the controller</td>
<td>This register gives the MAC-ID, with a length of 3 words</td>
</tr>
</tbody>
</table>

Table 159: Register Address 0x1037

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration of Modbus Response Delay Time</td>
<td>This register saves the value for the Modbus Response Delay Time for a Modbus connection. The time base is 1 ms. On the Modbus TCP connection, the response will be delayed by the inscribed time.</td>
</tr>
</tbody>
</table>

Table 160: Register Address 0x1038

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration of Modbus TOS</td>
<td>This register saves the value for the Modbus Response Delay Time for a Modbus TCP connection. The time base is 1 ms. On the Modbus TCP connection, the response will be delayed by the inscribed time. Range 0 … 63</td>
</tr>
</tbody>
</table>
### 11.3.5.6 Constant Registers

The following registers contain constants, which can be used to test communication with the master:

#### Table 161: Register Address 0x1050

<table>
<thead>
<tr>
<th>Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x1050 (4176dec)</td>
<td>Diagnosis of the connected I/O modules, length 3 words</td>
</tr>
<tr>
<td>Word 1:</td>
<td>Number of the module</td>
</tr>
<tr>
<td>Word 2:</td>
<td>Number of the channel</td>
</tr>
<tr>
<td>Word 3:</td>
<td>Diagnosis</td>
</tr>
</tbody>
</table>

#### Table 162: Register Address 0x2000

<table>
<thead>
<tr>
<th>Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x2000 (8192dec)</td>
<td>Zero, GP_ZERO</td>
</tr>
<tr>
<td>Access</td>
<td>Read</td>
</tr>
</tbody>
</table>

#### Table 163: Register Address 0x2001

<table>
<thead>
<tr>
<th>Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x2001 (8193dec)</td>
<td>Ones, GP_ONES</td>
</tr>
<tr>
<td>Access</td>
<td>Read</td>
</tr>
</tbody>
</table>

- –1 if this is declared as "signed int"
- MAXVALUE if it is declared as "unsigned int"

#### Table 164: Register Address 0x2002

<table>
<thead>
<tr>
<th>Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x2002 (8194dec)</td>
<td>1,2,3,4, GP_1234</td>
</tr>
<tr>
<td>Access</td>
<td>Read</td>
</tr>
</tbody>
</table>

This constant value is used to test the Intel/Motorola format specifier. If the master reads a value of 0x1234, then with Intel format is selected – this is the correct format. If 0x3412 appears, Motorola format is selected.

#### Table 165: Register Address 0x2003

<table>
<thead>
<tr>
<th>Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x2003 (8195dec)</td>
<td>Mask 1, GP_AAAA</td>
</tr>
<tr>
<td>Access</td>
<td>Read</td>
</tr>
</tbody>
</table>

This constant is used to verify that all bits are accessible to the fieldbus master. This will be used together with register 0x2004.
Table 166: Register Address 0x2004

<table>
<thead>
<tr>
<th>Value</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mask 1, GP_5555</td>
<td>Read</td>
<td>This constant is used to verify that all bits are accessible to the fieldbus master. This will be used together with register 0x2003.</td>
</tr>
</tbody>
</table>

Table 167: Register Address 0x2005

<table>
<thead>
<tr>
<th>Value</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum positive number, GP_MAX_POS</td>
<td>Read</td>
<td>Constant in order to control arithmetic.</td>
</tr>
</tbody>
</table>

Table 168: Register Address 0x2006

<table>
<thead>
<tr>
<th>Value</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum negative number, GP_MAX_NEG</td>
<td>Read</td>
<td>Constant in order to control arithmetic</td>
</tr>
</tbody>
</table>

Table 169: Register Address 0x2007

<table>
<thead>
<tr>
<th>Value</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum half positive number, GP_HALF_POS</td>
<td>Read</td>
<td>Constant in order to control arithmetic</td>
</tr>
</tbody>
</table>

Table 170: Register Address 0x2008

<table>
<thead>
<tr>
<th>Value</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum half negative number, GP_HALF_NEG</td>
<td>Read</td>
<td>Constant in order to control arithmetic</td>
</tr>
</tbody>
</table>
## 11.3.5.7 Firmware Information Registers

The following registers contain information on the firmware of the controller:

<table>
<thead>
<tr>
<th>Table</th>
<th>Register Address</th>
<th>Value</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>171</td>
<td>0x2010</td>
<td>Revision, INFO_REVISION</td>
<td>Read</td>
<td>Firmware index, e.g. 0x0005 for version 5</td>
</tr>
<tr>
<td>172</td>
<td>0x2011</td>
<td>Series code, INFO_SERIES</td>
<td>Read</td>
<td>WAGO serial number, e.g. 0x02EE (750 dec.) for WAGO-I/O-SYSTEM 750</td>
</tr>
<tr>
<td>173</td>
<td>0x2012</td>
<td>Order number, INFO_ITEM</td>
<td>Read</td>
<td>First part of WAGO order number, e.g. 0x0349 (841 dec.) for the controller 750-841 or 0x0155 (341 dec.) for the coupler 750-341 etc.</td>
</tr>
<tr>
<td>174</td>
<td>0x2013</td>
<td>Major sub item code, INFO_MAJOR</td>
<td>Read</td>
<td>Firmware version major revision</td>
</tr>
<tr>
<td>175</td>
<td>0x2014</td>
<td>Minor sub item code, INFO_MINOR</td>
<td>Read</td>
<td>Firmware version minor revision</td>
</tr>
<tr>
<td>176</td>
<td>0x2020</td>
<td>Description, INFO_DESCRIPTION</td>
<td>Read</td>
<td>Information on the controller, 16 words</td>
</tr>
<tr>
<td>Table 177: Register Address 0x2021</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Register address 0x2021 (8225\text{dec}) with a word count of up to 8</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>Description, INFO_DESCRIPTION</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td>Read</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Time of the firmware version, 8 words</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 178: Register Address 0x2022</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Register address 0x2022 (8226\text{dec}) with a word count of up to 8</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 179: Register Address 0x2023</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Register address 0x2023 (8227\text{dec}) with a word count of up to 32</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
Table 180: Register Address 0x2030

<table>
<thead>
<tr>
<th>Value</th>
<th>Description of the connected I/O modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Read module 0...64</td>
</tr>
<tr>
<td>Description</td>
<td>Length 1...65 words</td>
</tr>
<tr>
<td></td>
<td>The node configuration can be specified in the 0x2030 register. The item number of the I/O modules or fieldbus coupler/controller (without leading 750) is listed in order. Each module is represented in a word. Because order numbers cannot be read out of digital modules, a code is displayed for them, as defined below:</td>
</tr>
<tr>
<td>Bit position 0</td>
<td>Input module</td>
</tr>
<tr>
<td>Bit position 1</td>
<td>Output module</td>
</tr>
<tr>
<td>Bit position 2...7</td>
<td>Not used</td>
</tr>
<tr>
<td>Bit position 8...14</td>
<td>Module size in bits</td>
</tr>
<tr>
<td>Bit position 15</td>
<td>Designation digital module</td>
</tr>
</tbody>
</table>

Examples:

**4 Channel Digital Input Module = 0x8401**

<table>
<thead>
<tr>
<th>Bit</th>
<th>15</th>
<th>14</th>
<th>13</th>
<th>12</th>
<th>11</th>
<th>10</th>
<th>9</th>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Hex</td>
<td>8</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**2 Channel Digital Output Module = 0x8202**

<table>
<thead>
<tr>
<th>Bit</th>
<th>15</th>
<th>14</th>
<th>13</th>
<th>12</th>
<th>11</th>
<th>10</th>
<th>9</th>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Hex</td>
<td>8</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 181: Register Address 0x2031

<table>
<thead>
<tr>
<th>Value</th>
<th>Description of the connected I/O modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Read modules 65...128</td>
</tr>
<tr>
<td>Description</td>
<td>Length 1...64 words</td>
</tr>
<tr>
<td></td>
<td>The node configuration can be specified in the 0x2031 register. The item number of the I/O modules or fieldbus coupler/controller (without leading 750) is listed in order. Because order numbers cannot be read out of digital modules, a code is displayed for them, as defined below:</td>
</tr>
<tr>
<td>Bit position 0</td>
<td>Input module</td>
</tr>
<tr>
<td>Bit position 1</td>
<td>Output module</td>
</tr>
<tr>
<td>Bit position 2...7</td>
<td>Not used</td>
</tr>
<tr>
<td>Bit position 8...14</td>
<td>Module size in bits</td>
</tr>
<tr>
<td>Bit position 15</td>
<td>Designation digital module</td>
</tr>
</tbody>
</table>

Table 182: Register Address 0x2032

<table>
<thead>
<tr>
<th>Value</th>
<th>Description of the connected I/O modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Read modules 129...192</td>
</tr>
<tr>
<td>Description</td>
<td>Length 1...64 words</td>
</tr>
<tr>
<td></td>
<td>The node configuration can be specified in the 0x2032 register. The item number of the I/O modules or fieldbus coupler/controller (without leading 750) is listed in order. Because order numbers cannot be read out of digital modules, a code is displayed for them, as defined below:</td>
</tr>
<tr>
<td>Bit position 0</td>
<td>Input module</td>
</tr>
<tr>
<td>Bit position 1</td>
<td>Output module</td>
</tr>
<tr>
<td>Bit position 2...7</td>
<td>Not used</td>
</tr>
<tr>
<td>Bit position 8...14</td>
<td>Module size in bits</td>
</tr>
<tr>
<td>Bit position 15</td>
<td>Designation digital module</td>
</tr>
</tbody>
</table>
Table 183: Register Address 0x2033

<table>
<thead>
<tr>
<th>Register address 0x2033 (8243&lt;sub&gt;dec&lt;/sub&gt;) with a word count of up to 65</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Table 184: Register Address 0x2035

<table>
<thead>
<tr>
<th>Register address 0x2035 (8245&lt;sub&gt;dec&lt;/sub&gt;) with a word count of up to 65</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Table 185: Register Address 0x2036

<table>
<thead>
<tr>
<th>Register address 0x2036 (8246&lt;sub&gt;dec&lt;/sub&gt;) with a word count of up to 65</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Table 186: Register Address 0x2040

<table>
<thead>
<tr>
<th>Register address 0x2040 (8256&lt;sub&gt;dec&lt;/sub&gt;)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
Table 187: Register Address 0x2043

<table>
<thead>
<tr>
<th>Register address 0x2043 (8259dez)</th>
<th>Value</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0x55AA</td>
<td>Write</td>
<td>Factory settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The default settings are applied after the next reset, e.g., software reset via Modbus register address 0x2040.</td>
</tr>
</tbody>
</table>
12 I/O Modules

12.1 Overview

For modular applications with the WAGO I/O SYSTEM 750, different types of I/O modules are available

- Digital Input Modules
- Digital Output Modules
- Analog Input Modules
- Analog Output Modules
- Communication Modules, Supply and Segment Modules
- Function and Technology Modules

For detailed information on the I/O modules and the module variations, refer to the manuals for the I/O modules.

You will find these manuals on the WAGO web pages under www.wago.com.

---

**Information**

More Information about the WAGO I/O SYSTEM
Current information on the modular WAGO I/O SYSTEM is available in the Internet under: www.wago.com.

---

12.2 Process Data Architecture for Modbus TCP

**NOTICE**

Equipment damage due to incorrect address!
Depending on the specific position of an I/O module in the fieldbus node, the process data of all previous byte or bit-oriented modules must be taken into account to determine its location in the process data map.

With some I/O modules, the structure of the process data is fieldbus specific.

Modbus TCP process image uses a word structure (with word alignment). The internal mapping method for data greater than one byte conforms to the Intel format.

The fieldbus-specific representation in the process image as well as the structure of the process values for Modbus TCP for all I/O modules of the
WAGO I/O-SYSTEM 750 and 753 are listed in detail in the manuals for the Modbus products from WAGO.

---

**Information**

Further information about the process data for Modbus TCP!
You can read the fieldbus-specific process images for all I/O modules in the corresponding manuals for the WAGO Modbus products. These manuals are available for free download at: [www.wago.com](http://www.wago.com).
See the chapter: "I/O Modules" >> "Structure of the Process Data for Modbus TCP" e.g. in the manual for the product "Controller Modbus TCP, 750-891".
13 **Application Examples**

13.1 **Test of Modbus protocol and fieldbus nodes**

You require a Modbus master to test the function of your fieldbus node. For this purpose, various manufacturers offer a range of PC applications that you can, in part, download from the Internet as free of charge demo versions.

One of the programs which is particularly suitable to test your ETHERNET TCP/IP fieldbus node, is for instance **ModScan** from Win-Tech.

---

**Information**

**Additional Information**

A free of charge demo version from ModScan32 and further utilities from Win-Tech can be found in the Internet under:


ModScan32 is a Windows application that works as a Modbus master.

This program allows you to access the data points of your connected ETHERNET TCP/IP fieldbus node and to proceed with the desired changes.

---

**Information**

**Additional Information**

For a description example relating to the software operation, refer to:


---

13.2 **Visualization and Control using SCADA Software**

This chapter is intended to give insight into how the WAGO ETHERNET fieldbus coupler/controller can be used for process visualization and control using standard user software.

There is a wide range of process visualization programs, called SCADA Software, from various manufacturers.

SCADA is the abbreviation for Supervisory Control and Data Acquisition.

It is a user-orientated tool used as a production information system in the areas of automation technology, process control and production monitoring.

The use of SCADA systems includes the areas of visualization and monitoring, data access, trend recording, event and alarm processing, process analysis and targeted intervention in a process (control).

The WAGO ETHERNET fieldbus node provides the required process input and output values.
**Note**

SCADA software has to provide a Modbus device driver and support Modbus TCP functions!
When choosing suitable SCADA software, ensure that it provides a Modbus device driver and supports the Modbus TCP functions in the coupler.

Visualization programs with Modbus device drivers are available from i.e. Wonderware, National Instruments, Think&Do or KEPware Inc., some of which are available on the Internet as demo versions.

The operation of these programs is very specific. However, a few essential steps are described to illustrate the way an application can be developed using a WAGO ETHERNET fieldbus node and SCADA software in principle:

1. Load the Modbus ETHERNET driver and select Modbus ETHERNET
2. Enter the IP address for addressing the fieldbus node

   At this point, some programs allow the user to give the node an alias name, i.e. to call the node “Measuring data”. The node can then be addressed with this name.

3. Create a graphic object, such as a switch (digital) or a potentiometer (analog)

   This object is displayed on the work area.

4. Link the object to the desired data point on the node by entering the following data:
   - Node address (IP address or alias name)
   - The desired Modbus function codes (register/bit read/write)
   - The Modbus address of the selected channel

Entry is program specific.

Depending on the user software the Modbus addressing of a bus module can be represented with up to 5 digits.
Example of the Modbus Addressing

In the case of SCADA Software Lookout from National Instruments the Modbus function codes are used with a 6 digit coding, whereby the first digit represents the Modbus table (0, 1, 3 or 4) and implicit the function code (see following table):

<table>
<thead>
<tr>
<th>Modbus table</th>
<th>Modbus function code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>FC1 or FC15</td>
<td>Reading of input bits or writing of several output bits</td>
</tr>
<tr>
<td>1</td>
<td>FC2</td>
<td>Reading of several input bits</td>
</tr>
<tr>
<td>3</td>
<td>FC4 or FC16</td>
<td>Reading of several input registers or writing of several output registers</td>
</tr>
<tr>
<td>4</td>
<td>FC3</td>
<td>Reading of several input registers</td>
</tr>
</tbody>
</table>

The following five digits specify the channel number (beginning with 1) of the consecutively numbered digital or analog input and/or output channels.

Examples:

- Reading/writing the first digital input: i.e. 0 0000 1
- Reading/writing the second analog input: i.e. 3 0000 2

Application Example:

Thus, the digital input channel 2 of the above node “Measuring data” can be read out with the input: “Measuring data. 0 0000 2”.

Additional Information

Please refer to the respective SCADA product manual for a detailed description of the particular software operation.
14 Use in Hazardous Environments

The WAGO I/O SYSTEM 750 (electrical equipment) is designed for use in Zone 2 hazardous areas and shall be used in accordance with the marking and installation regulations.

The following sections include both the general identification of components (devices) and the installation regulations to be observed. The individual subsections of the “Installation Regulations” section must be taken into account if the I/O module has the required approval or is subject to the range of application of the ATEX directive.
14.1 Marking Configuration Examples

14.1.1 Marking for Europe According to ATEX and IECEx

Figure 54: Marking Example According to ATEX and IECEx

TUEV 07 ATEX 554036 X
II 3 D Ex tC IIC T185 °C Dc
I M2 Ex d I Mb
II 3 G Ex nA IIC T4 Gc
IECEx TUN 090001 X

Figure 55: Text Detail – Marking Example According to ATEX and IECEx
Table 189: Description of Marking Example According to ATEX and IECEx

<table>
<thead>
<tr>
<th>Marking</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUEV 07 ATEX 554086 X</td>
<td>Approving authority resp. certificate numbers</td>
</tr>
<tr>
<td>IECEx TUN 09.0001 X</td>
<td></td>
</tr>
</tbody>
</table>

**Dust**

<table>
<thead>
<tr>
<th>Marking</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>II</td>
<td>Equipment group: All except mining</td>
</tr>
<tr>
<td>3 D</td>
<td>Category 3 (Zone 22)</td>
</tr>
<tr>
<td>Ex</td>
<td>Explosion protection mark</td>
</tr>
<tr>
<td>tc</td>
<td>Type of protection: Protection by enclosure</td>
</tr>
<tr>
<td>IIIC</td>
<td>Explosion group of dust</td>
</tr>
<tr>
<td>T135°C</td>
<td>Max. surface temperature of the enclosure (without a dust layer)</td>
</tr>
<tr>
<td>Dc</td>
<td>Equipment protection level (EPL)</td>
</tr>
</tbody>
</table>

**Mining**

<table>
<thead>
<tr>
<th>Marking</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Equipment group: Mining</td>
</tr>
<tr>
<td>M2</td>
<td>Category: High level of protection</td>
</tr>
<tr>
<td>Ex</td>
<td>Explosion protection mark</td>
</tr>
<tr>
<td>d</td>
<td>Type of protection: Flameproof enclosure</td>
</tr>
<tr>
<td>I</td>
<td>Explosion group for electrical equipment for mines susceptible to firedamp</td>
</tr>
<tr>
<td>Mb</td>
<td>Equipment protection level (EPL)</td>
</tr>
</tbody>
</table>

**Gases**

<table>
<thead>
<tr>
<th>Marking</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>II</td>
<td>Equipment group: All except mining</td>
</tr>
<tr>
<td>3 G</td>
<td>Category 3 (Zone 2)</td>
</tr>
<tr>
<td>Ex</td>
<td>Explosion protection mark</td>
</tr>
<tr>
<td>nA</td>
<td>Type of protection: Non-sparking equipment</td>
</tr>
<tr>
<td>IIIC</td>
<td>Explosion group of gas and vapours</td>
</tr>
<tr>
<td>T4</td>
<td>Temperature class: Max. surface temperature 135 °C</td>
</tr>
<tr>
<td>Gc</td>
<td>Equipment protection level (EPL)</td>
</tr>
</tbody>
</table>
Figure 56: Marking Example for Approved Ex i I/O Module According to ATEX and IECEx

TUEV 12 ATEX 106032 X
II 3 [I] D Ex tc [ia Da] IIC T135°C Dc
I M2 (IM) Ex d [ia Ma] I Mb
II 3 [I] G Ex ec [ia Ga] IIC T4 Gc
IECEx TUN 120039 X

Figure 57: Text Detail – Marking Example for Approved Ex i I/O Module According to ATEX and IECEx
Table 190: Description of Marking Example for Approved Ex i I/O Module According to ATEX and IECEx

<table>
<thead>
<tr>
<th>Marking</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUEV 12 ATEX 106032 X IECEx TUN 12 0039 X</td>
<td>Approving authority resp. certificate numbers</td>
</tr>
</tbody>
</table>

### Dust

<table>
<thead>
<tr>
<th>Equipment group: All except mining</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category 3 (Zone 22) equipment containing a safety device for a category 1 (Zone 20) equipment</td>
</tr>
</tbody>
</table>

**Ex**

<table>
<thead>
<tr>
<th>Type of protection: Protection by enclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ia Da] Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 20</td>
</tr>
</tbody>
</table>

**IIIC**

<table>
<thead>
<tr>
<th>Explosion group of dust</th>
</tr>
</thead>
<tbody>
<tr>
<td>T135°C Max. surface temperature of the enclosure (without a dust layer)</td>
</tr>
</tbody>
</table>

**Dc**

<table>
<thead>
<tr>
<th>Equipment protection level (EPL)</th>
</tr>
</thead>
</table>

### Mining

<table>
<thead>
<tr>
<th>Equipment Group: Mining</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category: High level of protection with electrical circuits which present a very high level of protection</td>
</tr>
</tbody>
</table>

**Ex**

<table>
<thead>
<tr>
<th>Type of protection: Flameproof enclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ia Ma] Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety electrical circuits</td>
</tr>
</tbody>
</table>

**I**

| Explosion group for electrical equipment for mines susceptible to firedamp |

**Mb**

| Equipment protection level (EPL) |

### Gases

<table>
<thead>
<tr>
<th>Equipment group: All except mining</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category 3 (Zone 2) equipment containing a safety device for a category 1 (Zone 0) equipment</td>
</tr>
</tbody>
</table>

**Ex**

<table>
<thead>
<tr>
<th>Equipment protection by increased safety “e”</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ia Ga] Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 0</td>
</tr>
</tbody>
</table>

**IIIC**

<table>
<thead>
<tr>
<th>Explosion group of gas and vapours</th>
</tr>
</thead>
<tbody>
<tr>
<td>T4 Temperature class: Max. surface temperature 135 °C</td>
</tr>
</tbody>
</table>

**Gc**

| Equipment protection level (EPL) |
14.1.2 **Marking for the United States of America (NEC) and Canada (CEC)**

![Image of marking example](image)

**Figure 58: Marking Example According to NEC**

- **CL 1**
- **DIV 2**
- **Grp. A B C D**
- **op temp code T4**

**Figure 59: Text Detail – Marking Example According to NEC 500**

<table>
<thead>
<tr>
<th>Marking</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CL I</td>
<td>Explosion protection (gas group)</td>
</tr>
<tr>
<td>DIV 2</td>
<td>Area of application</td>
</tr>
<tr>
<td>Grp. A B C D</td>
<td>Explosion group (gas group)</td>
</tr>
<tr>
<td>op temp code T4</td>
<td>Temperature class</td>
</tr>
</tbody>
</table>
Table 192: Description of Marking Example for Approved Ex i I/O Module According to NEC 505

<table>
<thead>
<tr>
<th>Marking</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI I,</td>
<td>Explosion protection group</td>
</tr>
<tr>
<td>Zn 2</td>
<td>Area of application</td>
</tr>
<tr>
<td>AEx</td>
<td>Explosion protection mark</td>
</tr>
<tr>
<td>nA</td>
<td>Type of protection</td>
</tr>
<tr>
<td>[ia Ga]</td>
<td>Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 20</td>
</tr>
<tr>
<td>IIC</td>
<td>Group</td>
</tr>
<tr>
<td>T4</td>
<td>Temperature class</td>
</tr>
<tr>
<td>Gc</td>
<td>Equipment protection level (EPL)</td>
</tr>
</tbody>
</table>

Table 193: Description of Marking Example for Approved Ex i I/O Modules According to NEC 506

<table>
<thead>
<tr>
<th>Marking</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI I,</td>
<td>Explosion protection group</td>
</tr>
<tr>
<td>Zn 2</td>
<td>Area of application</td>
</tr>
<tr>
<td>AEx</td>
<td>Explosion protection mark</td>
</tr>
<tr>
<td>nA</td>
<td>Type of protection</td>
</tr>
<tr>
<td>[ia IIIC]</td>
<td>Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 20</td>
</tr>
<tr>
<td>IIC</td>
<td>Group</td>
</tr>
<tr>
<td>T4</td>
<td>Temperature class</td>
</tr>
<tr>
<td>Gc</td>
<td>Equipment protection level (EPL)</td>
</tr>
</tbody>
</table>
Figure 62: Text Detail – Marking Example for Approved Ex i I/O Modules According to CEC 18 attachment J

Table 194: Description of Marking Example for Approved Ex i I/O Modules According to CEC 18 attachment J

<table>
<thead>
<tr>
<th>Marking</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dust</td>
<td></td>
</tr>
<tr>
<td>Ex</td>
<td>Explosion protection mark</td>
</tr>
<tr>
<td>nA</td>
<td>Type of protection</td>
</tr>
<tr>
<td>[ia IIIC]</td>
<td>Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 20</td>
</tr>
<tr>
<td>IIC</td>
<td>Group</td>
</tr>
<tr>
<td>T4</td>
<td>Temperature class</td>
</tr>
<tr>
<td>Gc</td>
<td>Equipment protection level (EPL)</td>
</tr>
<tr>
<td>X</td>
<td>Symbol used to denote specific conditions of use</td>
</tr>
<tr>
<td>Gases</td>
<td></td>
</tr>
<tr>
<td>Ex</td>
<td>Explosion protection mark</td>
</tr>
<tr>
<td>nA</td>
<td>Type of protection</td>
</tr>
<tr>
<td>[ia Ga]</td>
<td>Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 0</td>
</tr>
<tr>
<td>IIC</td>
<td>Group</td>
</tr>
<tr>
<td>T4</td>
<td>Temperature class</td>
</tr>
<tr>
<td>Gc</td>
<td>Equipment protection level (EPL)</td>
</tr>
<tr>
<td>X</td>
<td>Symbol used to denote specific conditions of use</td>
</tr>
</tbody>
</table>
14.2 Installation Regulations

For the installation and operation of electrical equipment in hazardous areas, the valid national and international rules and regulations which are applicable at the installation location must be carefully followed.

14.2.1 Special Notes including Explosion Protection

The following warning notices are to be posted in the immediately proximity of the WAGO I/O SYSTEM 750 (hereinafter “product”):

**WARNING – DO NOT REMOVE OR REPLACE FUSED WHILE ENERGIZED!**

**WARNING – DO NOT DISCONNECT WHILE ENERGIZED!**

**WARNING – ONLY DISCONNECT IN A NON-HAZARDOUS AREA!**

Before using the components, check whether the intended application is permitted in accordance with the respective printing. Pay attention to any changes to the printing when replacing components.

The product is an open system. As such, the product must only be installed in appropriate enclosures or electrical operation rooms to which the following applies:

- Can only be opened using a tool or key
- Inside pollution degree 1 or 2
- In operation, internal air temperature within the range of $0 \, ^\circ C \leq T_a \leq +55 \, ^\circ C$ or $-20 \, ^\circ C \leq T_a \leq +60 \, ^\circ C$ for components with extension number …/025-xxx or $-40 \, ^\circ C \leq T_a \leq +70 \, ^\circ C$ for components with extension number …/040-xxx
- Minimum degree of protection: min. IP54 (acc. to EN/IEC 60529)
- For use in Zone 2 (Gc), compliance with the applicable requirements of the standards EN/IEC/ABNT NBR IEC 60079-0, -7, -11, -15
- For use in Zone 22 (Dc), compliance with the applicable requirements of the standards EN/IEC/ABNT NBR IEC 60079-0, -7, -11, -15 and -31
- For use in mining (Mb), minimum degree of protection IP64 (acc. EN/IEC 60529) and adequate protection acc. EN/IEC/ABNT NBR IEC 60079-0 and -1
- Depending on zoning and device category, correct installation and compliance with requirements must be assessed and certified by a “Notified Body” (ExNB) if necessary!
Explosive atmosphere occurring simultaneously with assembly, installation or repair work must be ruled out. Among other things, these include the following activities:

- Insertion and removal of components
- Connecting or disconnecting from fieldbus, antenna, D-Sub, ETHERNET or USB connections, DVI ports, memory cards, configuration and programming interfaces in general and service interface in particular:
  - Operating DIP switches, coding switches or potentiometers
  - Replacing fuses

Wiring (connecting or disconnecting) of non-intrinsically safe circuits is only permitted in the following cases:

- The circuit is disconnected from the power supply.
- The area is known to be non-hazardous.

Outside the device, suitable measures must be taken so that the rated voltage is not exceeded by more than 40 % due to transient faults (e.g., when powering the field supply).

Product components intended for intrinsically safe applications may only be powered by 750-606 or 750-625/000-001 bus supply modules.

Only field devices whose power supply corresponds to overvoltage category I or II may be connected to these components.
14.2.2 Special Notes Regarding ANSI/ISA Ex

For ANSI/ISA Ex acc. to UL File E198726, the following additional requirements apply:

- Use in Class I, Division 2, Group A, B, C, D or non-hazardous areas only
- ETHERNET connections are used exclusively for connecting to computer networks (LANs) and may not be connected to telephone networks or telecommunication cables
- **WARNING** – The radio receiver module 750-642 may only be used to connect to external antenna 758-910!
- **WARNING** – Product components with fuses must not be fitted into circuits subject to overloads! These include, e.g., motor circuits.
- **WARNING** – When installing I/O module 750-538, “Control Drawing No. 750538” in the manual must be strictly observed!

---

**Information**

**Additional Information**
Proof of certification is available on request. Also take note of the information given on the operating and assembly instructions. The manual, containing these special conditions for safe use, must be readily available to the user.
15 Appendix

15.1 MIB II Groups

15.1.1 System Group

The system group contains general information about the coupler/controller.

Table 195: MIB II – System Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.1.1</td>
<td>sysDescr</td>
<td>R</td>
<td>This entry contains the device identification. The object has a fixed code (e.g., &quot;WAGO 750-841&quot;)</td>
</tr>
<tr>
<td>1.3.6.1.2.1.1.2</td>
<td>sysObjectID</td>
<td>R</td>
<td>This entry contains the manufacturer's authorization identification.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.1.3</td>
<td>sysUpTime</td>
<td>R</td>
<td>This entry contains the time (in hundredths of a second) since the management unit has been last reset.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.1.4</td>
<td>sysContact</td>
<td>R/W</td>
<td>This entry contains the identification and contact information for the system contact person.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.1.5</td>
<td>sysName</td>
<td>R/W</td>
<td>This entry contains the administration-assigned device name.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.1.6</td>
<td>sysLocation</td>
<td>R/W</td>
<td>This entry contains the node's physical location.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.1.7</td>
<td>sysServices</td>
<td>R</td>
<td>This entry designates the quantity of services that this coupler/controller contains.</td>
</tr>
</tbody>
</table>
## 15.1.2 Interface Group

The interface group contains information and statistics about the device interface.

A device interface describes the Ethernet interface of a coupler/controller and provides status information on the physical Ethernet ports as well as on the internal loopback interface.

Table 196: MIB II – Interface Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.2.1.2.1</td>
<td>ifNumber</td>
<td>R</td>
<td>Number of network interfaces in this system</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.1.2.2</td>
<td>ifTable</td>
<td>-</td>
<td>List of network interfaces</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.1</td>
<td>ifEntry</td>
<td>-</td>
<td>Network interface entry</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.1.1</td>
<td>ifIndex</td>
<td>R</td>
<td>This entry contains a unique value for each interface</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.2</td>
<td>ifDescr</td>
<td>R</td>
<td>This entry contains the name of the manufacturer, the product name, and the version of the hardware interface: e.g., &quot;WAGO Kontakttechnik GmbH 750-841: Rev 1.0&quot;</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.3</td>
<td>ifType</td>
<td>R</td>
<td>This entry describes the type of interface. ETHERNET CSMA/CD = 6 Software Loopback = 24</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.4</td>
<td>ifMtu</td>
<td>R</td>
<td>This entry specifies the largest transfer unit; i.e., the maximum telegram length that can be transferred via this interface.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.5</td>
<td>ifSpeed</td>
<td>R</td>
<td>This entry indicates the interface speed in bits per second.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.6</td>
<td>ifPhysAddress</td>
<td>R</td>
<td>This entry indicates the physical address of the interface. For example, for Ethernet, this entry contains a MAC ID.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.7</td>
<td>ifAdmin-Status</td>
<td>R/W</td>
<td>This entry specifies the desired state of the interfaces. Possible values are: up(1): Ready for operation for transmission and reception down(2): Interface is switched off testing(3): Interface is in test mode</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.8</td>
<td>ifOperStatus</td>
<td>R</td>
<td>This entry indicates the current operational state of the interface.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.9</td>
<td>ifLastChange</td>
<td>R</td>
<td>This entry indicates the value of the sysUpTime when the state was last changed.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.10</td>
<td>ifInOctets</td>
<td>R</td>
<td>This entry gives the total number of bytes received via interface.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.11</td>
<td>ifInUcastPkts</td>
<td>R</td>
<td>This entry indicates the number of received unicast packets delivered to a higher layer.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.12</td>
<td>ifInNUcastPkts</td>
<td>R</td>
<td>This entry indicates the number of received broad and multicast packets delivered to a higher layer.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.13</td>
<td>ifInDiscards</td>
<td>R</td>
<td>This entry indicates the number of packets that were discarded even though no errors had been detected.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.14</td>
<td>ifInErrors</td>
<td>R</td>
<td>This entry indicates the number of received packets that contained errors preventing them from being deliverable to a higher layer.</td>
</tr>
</tbody>
</table>
### Table 196: MIB II – Interface Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.2.2.1.15</td>
<td>IfInUnknown-Protos</td>
<td>R</td>
<td>This entry indicates the number of received packets sent to an unknown or unsupported port number.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.16</td>
<td>IfOutOctets</td>
<td>R</td>
<td>This entry gives the total number of bytes sent via interface.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.17</td>
<td>IfOutUcastPkts</td>
<td>R</td>
<td>This entry contains the number of outgoing unicast packets delivered to a higher layer.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.18</td>
<td>IfOutNUcastPkts</td>
<td>R</td>
<td>This entry indicates the number of outgoing broadcast and multicast packets delivered to a higher layer.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.19</td>
<td>IfOutDiscards</td>
<td>R</td>
<td>This entry indicates the number of packets that were discarded even though no errors had been detected.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.2.2.1.20</td>
<td>IfOutErrors</td>
<td>R</td>
<td>This entry indicates the number of packets that could not be transmitted because of errors.</td>
</tr>
</tbody>
</table>
## 15.1.3 IP Group

The IP group contains information about IP communication.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.4.1</td>
<td>ipForwarding</td>
<td>R/W</td>
<td>1: Host is a router; 2: Host is not a router</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.2</td>
<td>ipDefaultTTL</td>
<td>R/W</td>
<td>Default value for the Time-To-Live field of each IP frame.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.3</td>
<td>ipInReceives</td>
<td>R</td>
<td>Number of received IP frames, including those received in error.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.4</td>
<td>ipInHdrErrors</td>
<td>R</td>
<td>Number of received IP frames with header errors.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.5</td>
<td>ipInAddrErrors</td>
<td>R</td>
<td>Number of received IP frames with a misdirected IP address.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.6</td>
<td>ipForwDatagrams</td>
<td>R</td>
<td>Number of received IP frames passed on (routed)</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.7</td>
<td>ipUnknownProtos</td>
<td>R</td>
<td>Number of received IP frames with an unknown protocol type.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.8</td>
<td>ipInDiscards</td>
<td>R</td>
<td>Number of received IP frames rejected although no disturbance was present.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.9</td>
<td>ipInDelivers</td>
<td>R</td>
<td>Number of received IP frames passed on a higher protocol layer.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.10</td>
<td>ipOutRequests</td>
<td>R</td>
<td>Number of sent IP frames</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.11</td>
<td>ipOutDiscards</td>
<td>R</td>
<td>Number of rejected IP Frames that should have been sent.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.12</td>
<td>ipOutNoRoutes</td>
<td>R</td>
<td>Number of sent IP frames rejected because of incorrect routing information.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.13</td>
<td>ipReasmTimeout</td>
<td>R</td>
<td>Minimum time duration until an IP frame is re-assembled.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.14</td>
<td>ipReasmReqds</td>
<td>R</td>
<td>Minimum number of the IP fragments for building up and passing on.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.15</td>
<td>ipReasmOKs</td>
<td>R</td>
<td>Number of IP frames re-assembled successfully.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.16</td>
<td>ipReasmFails</td>
<td>R</td>
<td>Number of IP frames not re-assembled successfully.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.17</td>
<td>ipFragOKs</td>
<td>R</td>
<td>Number of IP frames fragmented and passed on.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.18</td>
<td>ipFragFails</td>
<td>R</td>
<td>Number of IP frames that should have been fragmented but could not be, because their don't fragment bit was set in the header.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.19</td>
<td>ipFragCreates</td>
<td>R</td>
<td>Number of generated IP fragment frames</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.20</td>
<td>ipAddrTable</td>
<td>-</td>
<td>Table of all local IP addresses of the coupler/controller.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.20.1</td>
<td>ipAddrEntry</td>
<td>-</td>
<td>Address information for an entry</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.20.1.1</td>
<td>ipAdEntAddr</td>
<td>R</td>
<td>The IP address corresponding to the entry's address information</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.20.1.2</td>
<td>ipAdEntIfIndex</td>
<td>R</td>
<td>Index of the interface</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.20.1.3</td>
<td>ipAdEntNetMask</td>
<td>R</td>
<td>The entry's associated subnet mask</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.20.1.4</td>
<td>ipAdEntBcastAddr</td>
<td>R</td>
<td>Value of the last significant bit in the IP broadcast address</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.20.1.5</td>
<td>ipAdEntReasm-MaxSize</td>
<td>R</td>
<td>The size of the longest IP telegram that can be defragmented (reassembled) again.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.23</td>
<td>ipRoutingDiscards</td>
<td>R</td>
<td>Number of deleted routing entries</td>
</tr>
</tbody>
</table>
### 15.1.4 IpRoute Table Group

The IP route table contains information about the routing table in the coupler/controller.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.4.21.1</td>
<td>ipRouteTable</td>
<td>-</td>
<td>IP routing table</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.1</td>
<td>ipRouteEntry</td>
<td>-</td>
<td>A routing entry for a particular destination</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.1.1</td>
<td>ipRouteDest</td>
<td>R/W</td>
<td>This entry indicates the destination address of the routing entry</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.2</td>
<td>ipRouteIfIndex</td>
<td>R/W</td>
<td>This entry indicates the index of the interface, which is the next route destination</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.3</td>
<td>ipRouteMetric1</td>
<td>R/W</td>
<td>The primary route to the target system</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.4</td>
<td>ipRouteMetric2</td>
<td>R/W</td>
<td>An alternative route to the target system</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.5</td>
<td>ipRouteMetric3</td>
<td>R/W</td>
<td>An alternative route to the target system</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.6</td>
<td>ipRouteMetric4</td>
<td>R/W</td>
<td>An alternative route to the target system</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.7</td>
<td>ipRouteNextHop</td>
<td>R/W</td>
<td>The IP address of the next route section</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.8</td>
<td>ipRouteType</td>
<td>R/W</td>
<td>The route type</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.9</td>
<td>ipRouteProto</td>
<td>R</td>
<td>Routing mechanism via which the route is developed</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.10</td>
<td>ipRouteAge</td>
<td>R/W</td>
<td>Number of seconds since then the route was last renewed/examined</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.11</td>
<td>ipRouteMask</td>
<td>R/W</td>
<td>This entry contains the subnet mask for this entry</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.12</td>
<td>ipRouteMetric5</td>
<td>R/W</td>
<td>An alternative route to the target system</td>
</tr>
<tr>
<td>1.3.6.1.2.1.4.21.1.13</td>
<td>ipRouteInfo</td>
<td>R/W</td>
<td>A reference to a special MIB</td>
</tr>
</tbody>
</table>
### 15.1.5 ICMP Group

Table 199: MIB II – ICMP Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.5.1</td>
<td>icmpInMsgs</td>
<td>R</td>
<td>Number of received ICMP messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.2</td>
<td>icmpInErrors</td>
<td>R</td>
<td>Number of received ICMP errors containing ICMP-specific errors</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.3</td>
<td>icmpInDestUnreachs</td>
<td>R</td>
<td>Number of received ICMP destination unreachable messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.4</td>
<td>icmpInTimeExcds</td>
<td>R</td>
<td>Number of received ICMP time exceeded messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.5</td>
<td>icmpInParmProbs</td>
<td>R</td>
<td>Number of received ICMP parameter problem messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.6</td>
<td>icmpInSrcQuenchs</td>
<td>R</td>
<td>Number of received ICMP source quench messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.7</td>
<td>icmpInRedirects</td>
<td>R</td>
<td>Number of received ICMP redirect messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.8</td>
<td>icmpInEchos</td>
<td>R</td>
<td>Number of received ICMP echo request messages (Ping)</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.9</td>
<td>icmpInEchoReps</td>
<td>R</td>
<td>Number of received ICMP echo reply messages (Ping)</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.10</td>
<td>icmpInTimestamps</td>
<td>R</td>
<td>Number of received ICMP timestamp request messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.11</td>
<td>icmpInTimestampReps</td>
<td>R</td>
<td>Number of received ICMP timestamp reply messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.12</td>
<td>icmpInAddrMasks</td>
<td>R</td>
<td>Number of received ICMP address mask request messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.13</td>
<td>icmpInAddrMaskReps</td>
<td>R</td>
<td>Number of received ICMP address mask reply messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.14</td>
<td>icmpOutMsgs</td>
<td>R</td>
<td>Number of sent ICMP messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.15</td>
<td>icmpOutErrors</td>
<td>R</td>
<td>Number of sent ICMP messages that could not be sent due to errors</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.16</td>
<td>icmpOutDestUnreachs</td>
<td>R</td>
<td>Number of sent ICMP destination unreachable messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.17</td>
<td>icmpOutTimeExcds</td>
<td>R</td>
<td>Number of sent ICMP time exceeded messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.18</td>
<td>icmpOutParmProbs</td>
<td>R</td>
<td>Number of sent ICMP parameter problem messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.19</td>
<td>icmpOutSrcQuenchs</td>
<td>R</td>
<td>Number of sent ICMP source quench messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.20</td>
<td>icmpOutRedirects</td>
<td>R</td>
<td>Number of sent ICMP redirection messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.21</td>
<td>icmpOutEchos</td>
<td>R</td>
<td>Number of sent ICMP echo request messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.22</td>
<td>icmpOutEchoReps</td>
<td>R</td>
<td>Number of sent ICMP echo reply messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.23</td>
<td>icmpOutTimestamps</td>
<td>R</td>
<td>Number of sent ICMP timestamp request messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.24</td>
<td>icmpOutTimestampReps</td>
<td>R</td>
<td>Number of sent ICMP timestamp reply messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.25</td>
<td>icmpOutAddrMasks</td>
<td>R</td>
<td>Number of sent ICMP address mask request messages</td>
</tr>
<tr>
<td>1.3.6.1.2.1.5.26</td>
<td>icmpOutAddrMaskReps</td>
<td>R</td>
<td>Number of sent ICMP address mask reply messages</td>
</tr>
</tbody>
</table>
## 15.1.6 TCP Group

Table 200: MIB II – TCP Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.6.1</td>
<td>tcpRtoAlgorithm</td>
<td>R</td>
<td>Retransmission time: 1 = other, 2 = constant, 3 = RSRE, 4 = VANJ</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.2</td>
<td>tcpRtoMin</td>
<td>R</td>
<td>Minimum value for the retransmission timer</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.3</td>
<td>tcpRtoMax</td>
<td>R</td>
<td>Maximum value for the retransmission timer</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.4</td>
<td>tcpMaxConn</td>
<td>R</td>
<td>Number of maximum TCP connections that can exist simultaneously</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.5</td>
<td>tcpActiveOpens</td>
<td>R</td>
<td>Number of existing active TCP connections</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.6</td>
<td>tcpPassiveOpens</td>
<td>R</td>
<td>Number of existing passive TCP connections</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.7</td>
<td>tcpAttemptFails</td>
<td>R</td>
<td>Number of failed connection attempts</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.8</td>
<td>tcpEstabResets</td>
<td>R</td>
<td>Number of connection resets</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.9</td>
<td>tcpCurrEstab</td>
<td>R</td>
<td>The number of TCP connections for which the current state is either Established or Close-Wait</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.10</td>
<td>tcpInSegs</td>
<td>R</td>
<td>Number of received TCP frames including the error frames</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.11</td>
<td>tcpOutSegs</td>
<td>R</td>
<td>Number of correctly sent TCP frames with data</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.12</td>
<td>tcpRetransSegs</td>
<td>R</td>
<td>Number of sent TCP frames retransmitted because of errors</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.13</td>
<td>tcpConnTable</td>
<td>-</td>
<td>For each existing connection, a table entry is created</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.13.1</td>
<td>tcpConnEntry</td>
<td>-</td>
<td>Table entry for connection</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.13.1.1</td>
<td>tcpConnState</td>
<td>R</td>
<td>This entry indicates the status of the TCP connection</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.13.1.2</td>
<td>tcpConnLocalAddress</td>
<td>R</td>
<td>The entry contains the IP address for the connection. For a server, this entry is constant 0.0.0.0</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.13.1.3</td>
<td>tcpConnLocalPort</td>
<td>R</td>
<td>The entry indicates the port number of the TCP connection.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.13.1.4</td>
<td>tcpConnRemAddress</td>
<td>R</td>
<td>The entry contains the remote IP address of the TCP connection.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.13.1.5</td>
<td>tcpConnRemPort</td>
<td>R</td>
<td>The entry contains the remote port of the TCP connection.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.14</td>
<td>tcpInErrs</td>
<td>R</td>
<td>Number of received incorrect TCP frames</td>
</tr>
<tr>
<td>1.3.6.1.2.1.6.15</td>
<td>tcpOutRsts</td>
<td>R</td>
<td>Number of sent TCP frames with set RST flag</td>
</tr>
</tbody>
</table>
## 15.1.7 UDP Group

Table 201: MIB II – UDP Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.7.1.1</td>
<td>udpInDatagrams</td>
<td>R</td>
<td>Number of received UDP frames that could be passed on to the appropriate applications</td>
</tr>
<tr>
<td>1.3.6.1.2.1.7.1.2</td>
<td>udpNoPorts</td>
<td>R</td>
<td>Number of received UDP frames that could not be passed on to the appropriate applications (port unreachable)</td>
</tr>
<tr>
<td>1.3.6.1.2.1.7.1.3</td>
<td>udpInErrors</td>
<td>R</td>
<td>Number of received UDP frames that could not be passed on to the appropriate applications for other reasons.</td>
</tr>
<tr>
<td>1.3.6.1.2.1.7.1.4</td>
<td>udpOutDatagrams</td>
<td>R</td>
<td>Number of sent UDP frames</td>
</tr>
<tr>
<td>1.3.6.1.2.1.7.1.5</td>
<td>udpTable</td>
<td>-</td>
<td>A table entry is created for each application that received UDP frames</td>
</tr>
<tr>
<td>1.3.6.1.2.1.7.5.1.1</td>
<td>udpEntry</td>
<td>-</td>
<td>Table entry for an application that received an UDP frame</td>
</tr>
<tr>
<td>1.3.6.1.2.1.7.5.1.2</td>
<td>udpLocalAddress</td>
<td>R</td>
<td>IP address of the local UDP server</td>
</tr>
<tr>
<td>1.3.6.1.2.1.7.5.1.3</td>
<td>udpLocalPort</td>
<td>R</td>
<td>Port number of the local UDP server</td>
</tr>
</tbody>
</table>
## 15.1.8 SNMP Group

Table 202: MIB II – SNMP Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.11.1</td>
<td>snmpInPkts</td>
<td>R</td>
<td>Number of received SNMP frames</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.2</td>
<td>snmpOutPkts</td>
<td>R</td>
<td>Number of sent SNMP frames</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.3</td>
<td>snmpInBadVersions</td>
<td>R</td>
<td>Number of received SNMP frames with an invalid version number</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.4</td>
<td>snmpInBadCommunity-Names</td>
<td>R</td>
<td>Number of received SNMP frames with an invalid community</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.5</td>
<td>snmpInBadCommunity-Uses</td>
<td>R</td>
<td>Number of received SNMP frames whose community did not have sufficient authorization for the actions that it tried to execute</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.6</td>
<td>snmpInASNParseErrs</td>
<td>R</td>
<td>Number of received SNMP frames with an incorrect structure</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.8</td>
<td>snmpInTooBigs</td>
<td>R</td>
<td>Number of received SNMP frames that acknowledged the result too Big</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.9</td>
<td>snmpInNoSuchNames</td>
<td>R</td>
<td>Number of received SNMP frames that acknowledged the result noSuchName</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.10</td>
<td>snmpInBadValues</td>
<td>R</td>
<td>Number of received SNMP frames that acknowledged the result bad value</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.11</td>
<td>snmpInReadOnlys</td>
<td>R</td>
<td>Number of received SNMP frames that acknowledged the result readOnly</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.12</td>
<td>snmpInGenErrs</td>
<td>R</td>
<td>Number of received SNMP frames that acknowledged the result genError</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.13</td>
<td>snmpInTotalReqVars</td>
<td>R</td>
<td>Number of received SNMP frames with valid GET or GET-NEXT requests</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.14</td>
<td>snmpInTotalSetVars</td>
<td>R</td>
<td>Number of received SNMP frames with valid SET requests</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.15</td>
<td>snmpInGetRequests</td>
<td>R</td>
<td>Number of GET requests received and processed</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.16</td>
<td>snmpInGetNexts</td>
<td>R</td>
<td>Number of GET-NEXT requests received and processed</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.17</td>
<td>snmpInSetRequests</td>
<td>R</td>
<td>Number of SET requests received and processed</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.18</td>
<td>snmpInResponses</td>
<td>R</td>
<td>Number of received GET responses</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.19</td>
<td>snmpInTraps</td>
<td>R</td>
<td>Number of received traps</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.20</td>
<td>snmpOutTooBigs</td>
<td>R</td>
<td>Number of sent SNMP frames that contained the result too Big</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.21</td>
<td>snmpOutNoSuchNames</td>
<td>R</td>
<td>Number of sent SNMP frames that contained the result noSuchName</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.22</td>
<td>snmpOutBadValues</td>
<td>R</td>
<td>Number of sent SNMP frames that contained the result bad value</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.24</td>
<td>SnmpOutGenErrs</td>
<td>R</td>
<td>Number of sent SNMP frames that contained the result genErrs</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.25</td>
<td>snmpOutGetRequests</td>
<td>R</td>
<td>Number of GET requests sent</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.26</td>
<td>snmpOutGetNexts</td>
<td>R</td>
<td>Number of GET NEXT requests sent</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.27</td>
<td>snmpOutSetRequests</td>
<td>R</td>
<td>Number of SET requests sent</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.28</td>
<td>snmpOutGetResponses</td>
<td>R</td>
<td>Number of GET responses sent</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.29</td>
<td>snmpOutTraps</td>
<td>R</td>
<td>Number of traps sent</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.30</td>
<td>snmpEnableAuthenTraps</td>
<td>R/W</td>
<td>Authentication failure traps(1 = on, 2 = off )</td>
</tr>
</tbody>
</table>
15.2 WAGO MIB Groups

15.2.1 Company Group

The company group contains general information about the company WAGO Kontakttechnik GmbH & Co. KG.

Table 203: WAGO MIB – Company Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.1.1</td>
<td>wagoName</td>
<td>R</td>
<td>Company’s registered name Default value: &quot;WAGO Kontakttechnik GmbH &amp; Co. KG&quot;</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.1.2</td>
<td>wagoDescription</td>
<td>R</td>
<td>Description of company Default value: &quot;WAGO Kontakttechnik GmbH &amp; Co. KG, Hansastr. 27, D-32423 Minden&quot;</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.1.3</td>
<td>wagoURL</td>
<td>R</td>
<td>URL for company web site Default value: &quot;www.wago.com&quot;</td>
</tr>
</tbody>
</table>

15.2.2 Product Group

The product group contains information about the product.

Table 204: WAGO MIB – Product Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.1</td>
<td>wioArticleName</td>
<td>R</td>
<td>Name of article Default value: &quot;750-xxx/000-000&quot;</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.2</td>
<td>wioArticleDescription</td>
<td>R</td>
<td>Description of article Default value: &quot;WAGO Ethernet (10/100MBit) FBC&quot;</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.3</td>
<td>wioSerialNumber</td>
<td>R</td>
<td>Serial number of article Default value: &quot;SNxxxxxxxx-Txxxxxx-mac</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.4</td>
<td>wioMacAddress</td>
<td>R</td>
<td>MAC address of article Default value: &quot;0030DExxxxxx&quot;</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.5</td>
<td>wioURLDatasheet</td>
<td>R</td>
<td>URL to datasheet of article Default value: &quot;<a href="http://www.wago.com/">http://www.wago.com/</a> wagoweb/documentation/navigate/nmd_0dc_e.htm#ethernet&quot;</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.6</td>
<td>wioURLManual</td>
<td>R</td>
<td>URL to manual of article Default value: &quot;<a href="http://www.wago.com/">http://www.wago.com/</a> wagoweb/documentation/navigate/nmd_0dc_e.htm#ethernet&quot;</td>
</tr>
</tbody>
</table>
### 15.2.3 Versions Group

The version group contains information about the used hardware/software versions.

Table 205: WAGO MIB – Versions Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.10.1</td>
<td>wioFirmwareIndex</td>
<td>R</td>
<td>Index of firmware version</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.10.2</td>
<td>wioHardwareIndex</td>
<td>R</td>
<td>Index of hardware version</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.10.3</td>
<td>wioFwIndex</td>
<td>R</td>
<td>Index of software version from firmware loader</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.10.4</td>
<td>wioFirmwareVersion</td>
<td>R</td>
<td>Complete firmware string</td>
</tr>
</tbody>
</table>
15.2.4 Real-Time Clock Group

The real-time clock group contains information about the system's real-time clock.

Table 206: WAGO MIB – Real Time Clock Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.11.1</td>
<td>wioRtcDateTime</td>
<td>R/W</td>
<td>Date/time of coupler in UTC as string. For writing date/time use the following string time 11:22:33 date 13-1-2007 Default value: &quot;time xx:xx:xx date xx-xx-xxxx (UTC)&quot;</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.11.2</td>
<td>wioRtcTime</td>
<td>R/W</td>
<td>Date/time of coupler in UTC as integer in seconds from 1970-01-01 Default value: &quot;0&quot;</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.11.3</td>
<td>wioTimezone</td>
<td>R/W</td>
<td>&quot;Actual time zone of article in hours (-12 - +12) Default value: &quot;0&quot;</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.11.4</td>
<td>wioRtcHourMode</td>
<td>R</td>
<td>Hour mode 0 = 12h mode 1 = 24h mode Default value: &quot;0&quot;</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.11.5</td>
<td>wioRtcBatteryStatus</td>
<td>R</td>
<td>RTC battery status: 0 = ok 1 = battery empty Default value: &quot;1&quot;</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.11.6</td>
<td>wioRtcDayLightSaving</td>
<td>R/W</td>
<td>Time offset of 1 hour: 0 = not offset 1 = offset 1 hour (DayLightSaving) Default value: &quot;0&quot;</td>
</tr>
</tbody>
</table>
15.2.5 Ethernet Group

The Ethernet group contains the settings for Ethernet.

Table 207: WAGO MIB – Ethernet Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.12.1</td>
<td>wioEthernetMode</td>
<td>R/W</td>
<td>IP configuration of Ethernet connection:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 = fix Ip address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 = dynamic IP address over Bootp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 = dynamic IP address over DHCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: “1”</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.12.2</td>
<td>wioIp</td>
<td>R/W</td>
<td>Actual IP address of coupler</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.12.3</td>
<td>wioSubnetMask</td>
<td>R/W</td>
<td>Actual subnet mask of coupler</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.12.4</td>
<td>wioGateway</td>
<td>R/W</td>
<td>Actual gateway IP of coupler</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.12.5</td>
<td>wioHostname</td>
<td>R/W</td>
<td>Actual host name of coupler</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.12.6</td>
<td>wioDomainName</td>
<td>R/W</td>
<td>Actual domain name of coupler</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.12.7</td>
<td>wioDnsServer1</td>
<td>R/W</td>
<td>IP address of first DNS server</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.12.8</td>
<td>wioDnsServer2</td>
<td>R/W</td>
<td>IP address of second DNS server</td>
</tr>
</tbody>
</table>

15.2.6 Actual Error Group

The actual error group contains information about the last system status/error status.

Table 208: WAGO MIB – Actual Error Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.20.1</td>
<td>wioErrorGroup</td>
<td>R</td>
<td>Error group of last error</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.20.2</td>
<td>wioErrorCode</td>
<td>R</td>
<td>Error code of last error</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.20.3</td>
<td>wioErrorArgument</td>
<td>R</td>
<td>Error argument of last error</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.20.4</td>
<td>wioErrorDescription</td>
<td>R</td>
<td>Error description string</td>
</tr>
</tbody>
</table>
15.2.7 PLC Project Group

The PLC project group contains information about the controller’s PLC program.

Table 209: WAGO MIB – PLC Project Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.1</td>
<td>wioProjectId</td>
<td>R</td>
<td>ID of CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.2</td>
<td>wioProjectDate</td>
<td>R</td>
<td>Date of CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.3</td>
<td>wioProjectName</td>
<td>R</td>
<td>Name of CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.4</td>
<td>wioProjectTitle</td>
<td>R</td>
<td>Title of CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.5</td>
<td>wioProjectVersion</td>
<td>R</td>
<td>Version of CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.6</td>
<td>wioProjectAuthor</td>
<td>R</td>
<td>Author of CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.7</td>
<td>wioProjectDescription</td>
<td>R</td>
<td>Description of CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.8</td>
<td>wioNumberOfIecTasks</td>
<td>R</td>
<td>Number of IEC tasks in the CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9</td>
<td>wioecTaskTable</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9.1</td>
<td>wioecTaskEntry</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9.1.1</td>
<td>wioecTaskId</td>
<td>R</td>
<td>ID of IEC task in the CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9.1.2</td>
<td>wioecTaskName</td>
<td>R</td>
<td>Name of IEC task in the CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9.1.3</td>
<td>wioecTaskStatus</td>
<td>R</td>
<td>Status of IEC task in the CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9.1.4</td>
<td>wioecTaskMode</td>
<td>R</td>
<td>Mode of IEC task in the CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9.1.5</td>
<td>wioecTaskPriority</td>
<td>R</td>
<td>Priority of IEC task in the CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9.1.6</td>
<td>wioecTaskInterval</td>
<td>R</td>
<td>Interval of cyclic IEC task in the CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9.1.7</td>
<td>wioecTaskEvent</td>
<td>R</td>
<td>Event for IEC task in the CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9.1.8</td>
<td>wioecTaskCycleCount</td>
<td>R</td>
<td>Count of IEC task in the CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9.1.9</td>
<td>wioecTaskCycleTime</td>
<td>R</td>
<td>Last cycle time of IEC task in the CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9.1.10</td>
<td>wioecTaskCycleTime-Min</td>
<td>R</td>
<td>Minimal cycle time of IEC task in the CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9.1.11</td>
<td>wioecTaskCycleTime-Max</td>
<td>R</td>
<td>Maximal cycle time of IEC task in the CODESYS project</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.30.9.1.12</td>
<td>wioecTaskCycleTime-Avg</td>
<td>R</td>
<td>Average cycle time of IEC task in the CODESYS project</td>
</tr>
</tbody>
</table>
15.2.8 **Http Group**

The Http group contains information and settings for the controller's Web server.

Table 210: WAGO MIB – Http Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.1.1</td>
<td>wioHttpEnable</td>
<td>R/W</td>
<td>Enable/disable the port of the webserver:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 = port of webserver disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 = port of webserver enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: {1}</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.1.2</td>
<td>wioHttpAuthenticationEnable</td>
<td>R/W</td>
<td>Enable/disable the authentication on the websites:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 = authentication disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 = authentication enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: {1}</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.1.3</td>
<td>wioHttpPort</td>
<td>R/W</td>
<td>Port of the http web server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: {80}</td>
</tr>
</tbody>
</table>

15.2.9 **Ftp Group**

The Ftp group contains information and settings for the controller's Ftp server.

Table 211: WAGO MIB – Ftp Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.2.1</td>
<td>wioFtpEnable</td>
<td>R/W</td>
<td>Enable/disable the port of the ftp server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 = port of ftp server disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 = port of ftp server enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: {1}</td>
</tr>
</tbody>
</table>
15.2.10 Sntp Group

The Sntp group contains information and settings for the controller's Sntp server.

Table 212: WAGO MIB – Sntp Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.3.1</td>
<td>wioSntpEnable</td>
<td>R/W</td>
<td>Enable/disable the port of the SNTP server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 = port of SNTP server disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 = port of SNTP server enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 1 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.3.2</td>
<td>wioSntpServer-Address</td>
<td>R/W</td>
<td>IP address of SNTP server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 0 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.3.3</td>
<td>wioSntpClient-Interval</td>
<td>R/W</td>
<td>Interval to pool SNTP manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 0 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.3.4</td>
<td>wioSntpClient-Timeout</td>
<td>R/W</td>
<td>Timeout to corrupt SNTP answer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 2000 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.3.5</td>
<td>wioSntpClient-DayLightSaving</td>
<td>R/W</td>
<td>Time offset of 1 hour:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 = not offset</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 = offset 1 hour (DayLightSaving)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 0 }</td>
</tr>
</tbody>
</table>

15.2.11 Snmp Group

The Snmp group contains information and settings for the controller's SNMP agent.

Table 213: WAGO MIB – Snmp Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.1</td>
<td>wioSnmpEnable</td>
<td>R/W</td>
<td>Enable/disable the port of the SNMP server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 = port of SNMP server disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 = port of SNMP server enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 1 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.2.1</td>
<td>wioSnmp1-ProtocolEnable</td>
<td>R/W</td>
<td>Enable/disable first SNMPv1/v2c agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 1 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.2.2</td>
<td>wioSnmp1-ManagerIp</td>
<td>R/W</td>
<td>IP address of first SNMP server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: '{ C0A80101'h }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.2.3</td>
<td>wioSnmp1-Community</td>
<td>R/W</td>
<td>Community identification string for SNMPv1/v2c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { &quot;public&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.2.4</td>
<td>wioSnmp1Trap-V1enable</td>
<td>R/W</td>
<td>Enable/disable SNMPv1 traps to first SNMP server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 1 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.2.5</td>
<td>wioSnmp1Trap-V2enable</td>
<td>R/W</td>
<td>Enable/disable SNMPv2c traps to first SNMP server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 0 }</td>
</tr>
<tr>
<td>Identifier</td>
<td>Entry</td>
<td>Access</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.2.6</td>
<td>wioSnmp2-ProtocolEnable</td>
<td>R/W</td>
<td>Enable/disable first SNMPv1/v2c agent. Default value: { 0 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.2.7</td>
<td>wioSnmp2-ManagerIp</td>
<td>R/W</td>
<td>IP address of second SNMP server. Default value: {'00000000'h}</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.2.8</td>
<td>wioSnmp2-Community</td>
<td>R/W</td>
<td>Community identification string for SNMPv1/v2c. Default value: { &quot;public&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.2.9</td>
<td>wioSnmp2Trap-V1enable</td>
<td>R/W</td>
<td>Enable/disable SNMPv1 traps to first SNMP server. Default value: { 0 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.2.10</td>
<td>wioSnmp2Trap-V2enable</td>
<td>R/W</td>
<td>Enable/disable SNMPv2c traps to first SNMP server. Default value: { 0 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.3.1</td>
<td>wioSnmp1User-Enable</td>
<td>R/W</td>
<td>Enable/disable first SNMPv3 user. Default value: { 1 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.3.2</td>
<td>wioSnmp1-Authentication-Typ</td>
<td>R/W</td>
<td>Authentication type for first SNMPv3 user: 0 = no Authentication, 1 = MD5 Authentication, 2 = SHA1 Authentication. Default value: { 1 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.3.3</td>
<td>wioSnmp1-Authentication-Name</td>
<td>R/W</td>
<td>Authentication name for first SNMPv3 user. Default value: { &quot;SecurityName&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.3.4</td>
<td>wioSnmp1-Authentication-Key</td>
<td>R/W</td>
<td>Authentication key for first SNMPv3 user. Default value: { &quot;AuthenticationKey&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.3.5</td>
<td>wioSnmp1-PrivacyEnable</td>
<td>R/W</td>
<td>Disable/enable data encryption for first SNMPv3 user: 0 = no Encryption, 1 = DES Encryption. Default value: { 1 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.3.6</td>
<td>wioSnmp1-PrivacyKey</td>
<td>R/W</td>
<td>Privacy key for SNMPv3 for first SNMPv3 user. Default value: { &quot;PrivacyKey&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.3.7</td>
<td>wioSnmp1-Notification-Enable</td>
<td>R/W</td>
<td>Enable/disable notification (SNMPv3 traps) with SNMPv3 user. Default value: { 1 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.3.8</td>
<td>wioSnmp1-Notification-ReceiverIP</td>
<td>R/W</td>
<td>Receiver IP address for notification (SNMPv3 traps) with SNMPv3 user. Default value: {'C0A80101'h}</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.3.9</td>
<td>wioSnmp2User-Enable</td>
<td>R/W</td>
<td>Enable/disable second SNMPv3 user. Default value: { 0 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.3.10</td>
<td>wioSnmp2-Authentication-Typ</td>
<td>R/W</td>
<td>Authentication type for second SNMPv3 user: 0 = no authentication, 1 = MD5 authentication, 2 = SHA1 authentication. Default value: { 1 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.3.11</td>
<td>wioSnmp2-Authentication-Name</td>
<td>R/W</td>
<td>Authentication name for second SNMPv3 user. Default value: { &quot;SecurityName&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.3.12</td>
<td>wioSnmp2-Authentication-Key</td>
<td>R/W</td>
<td>Authentication key for second SNMPv3 user. Default value: { &quot;AuthenticationKey&quot; }</td>
</tr>
</tbody>
</table>
### 15.2.12 Snmp Trap String Group

The Snmp trap string group contains strings that are attached to the manufacturer-specific traps.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.4.1</td>
<td>wioTrapKbus-Error</td>
<td>R/W</td>
<td>String for 1st SNMP trap Default value: { &quot;Kbus Error&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.4.2</td>
<td>wioTrapPlcStart</td>
<td>R/W</td>
<td>String for 2nd SNMP trap Default value: { &quot;Plc Start&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.4.3</td>
<td>wioTrapPlcStop</td>
<td>R/W</td>
<td>String for 3rd SNMP trap Default value: { &quot;Plc Stop&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.4.4</td>
<td>wioTrapPlc-Reset</td>
<td>R/W</td>
<td>String for 4th SNMP trap Default value: { &quot;Plc Reset&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.4.5</td>
<td>wioTrapPlcSoftwareWatchdog</td>
<td>R/W</td>
<td>String for 5th SNMP trap Default value: { &quot;Plc Software Watchdog&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.4.6</td>
<td>wioTrapPlc-DivideByZero</td>
<td>R/W</td>
<td>String for 6th SNMP trap Default value: { &quot;Plc Divide By Zero&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.4.7</td>
<td>wioTrapPlc-OnlineChange</td>
<td>R/W</td>
<td>String for 7th SNMP trap Default value: { &quot;Plc Online Change&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.4.8</td>
<td>wioTrapPlc-Download</td>
<td>R/W</td>
<td>String for 8th SNMP trap Default value: { &quot;Plc Download Programm&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.4.9</td>
<td>wioTrapPlc-Login</td>
<td>R/W</td>
<td>String for 9th SNMP trap Default value: { &quot;Plc Login&quot; }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.4.10</td>
<td>wioTrapPlc-Logout</td>
<td>R/W</td>
<td>String for 10th SNMP trap Default value: { &quot;Plc Logout&quot; }</td>
</tr>
</tbody>
</table>
15.2.13 Snmp User Trap String Group

The Snmp user trap string group contains strings that can be attached to user-specific traps. These strings can be changed via SNMP or Wago_SNMP.lib in CODESYS.

Table 215: WAGO MIB – Snmp User Trap String Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.5.1</td>
<td>wioUserTrapMsg1</td>
<td>R/W</td>
<td>String for 1st SNMP trap</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.5.2</td>
<td>wioUserTrapMsg2</td>
<td>R/W</td>
<td>String for 2nd SNMP trap</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.5.3</td>
<td>wioUserTrapMsg3</td>
<td>R/W</td>
<td>String for 3rd SNMP trap</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.5.4</td>
<td>wioUserTrapMsg4</td>
<td>R/W</td>
<td>String for 4th SNMP trap</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.5.5</td>
<td>wioUserTrapMsg5</td>
<td>R/W</td>
<td>String for 5th SNMP trap</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.5.6</td>
<td>wioUserTrapMsg6</td>
<td>R/W</td>
<td>String for 6th SNMP trap</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.5.7</td>
<td>wioUserTrapMsg7</td>
<td>R/W</td>
<td>String for 7th SNMP trap</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.5.8</td>
<td>wioUserTrapMsg8</td>
<td>R/W</td>
<td>String for 8th SNMP trap</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.5.9</td>
<td>wioUserTrapMsg9</td>
<td>R/W</td>
<td>String for 9th SNMP trap</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.4.5.10</td>
<td>wioUserTrapMsg10</td>
<td>R/W</td>
<td>String for 10th SNMP trap</td>
</tr>
</tbody>
</table>

15.2.14 Plc Connection Group

Activate or deactivate the connection to CODESYS with the Plc connection group.

Table 216: WAGO MIB – Plc Connection Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.5.1</td>
<td>wioCODESYSEnable</td>
<td>R/W</td>
<td>Enable/disable the port of the CODESYS server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 = port of CODESYS server disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 = port of CODESYS server enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 1 }</td>
</tr>
</tbody>
</table>
15.2.15 Modbus Group

The Modbus group contains information and settings about the controller's modbus server.

Table 217: WAGO MIB – Modbus Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.6.1</td>
<td>wioModbusTcp-Enable</td>
<td>R/W</td>
<td>Enable/disable the port of the Modbus TCP server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 = port of Modbus TCP server disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 = port of Modbus TCP server enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 1 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.6.2</td>
<td>wioModbusUdb-Enable</td>
<td>R/W</td>
<td>Enable/disable the port of the Modbus UDP server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 = port of Modbus UDP server disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 = port of Modbus UDP server enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 1 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.6.3</td>
<td>wioMax-Connections</td>
<td>R/W</td>
<td>The maximal count of modbus connections</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 15 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.6.4</td>
<td>wioConnection-Timeout</td>
<td>R/W</td>
<td>Timeout of the modbus connection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 600 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.6.5</td>
<td>wioModbus-WatchdogMode</td>
<td>R/W</td>
<td>Mode of the modbus watchdog</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 0 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.6.6</td>
<td>wioModbus-WatchdogTime</td>
<td>R/W</td>
<td>Timeout of the modbus watchdog</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 100 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.6.7</td>
<td>wioFreeModbus-Sockets</td>
<td>R/W</td>
<td>Unused and free modbus connections</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: { 15 }</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.6.8</td>
<td>wioModbus-ConnectionTable</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.6.8.1</td>
<td>wioModbus-ConnectionEntry</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.6.8.1.1</td>
<td>wioModbus-ConnectionIndex</td>
<td>R/W</td>
<td>Index of modbus connection</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.6.8.1.2</td>
<td>wioModbus-Connectionlp</td>
<td>R/W</td>
<td>IP address of modbus connection</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.40.6.8.1.3</td>
<td>wioModbus-ConnectionPort</td>
<td>R/W</td>
<td>Port of modbus connection</td>
</tr>
</tbody>
</table>
15.2.16 Process Image Group

The process image group contains a list of information about the terminals connected to the controller.

Table 218: WAGO MIB – Process Image Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.1</td>
<td>wioModulCount</td>
<td>R</td>
<td>Count of modules</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.2</td>
<td>wioAnalogOutLength</td>
<td>R</td>
<td>Length of analog output process datas</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.3</td>
<td>wioAnalogInLength</td>
<td>R</td>
<td>Length of analog input process datas</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.4</td>
<td>wioDigitalOutLength</td>
<td>R</td>
<td>Length of digital output process datas</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.5</td>
<td>wioDigitalInLength</td>
<td>R</td>
<td>Length of digital input process datas</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.6</td>
<td>wioDigitalOutOffset</td>
<td>R</td>
<td>Offset of digital output process datas</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.7</td>
<td>wioDigitalInOffset</td>
<td>R</td>
<td>Offset of digital input process datas</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.8</td>
<td>wioModuleTable</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.8.1</td>
<td>wioModuleEntry</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.8.1.1</td>
<td>wioModuleName</td>
<td>R</td>
<td>Number of module slot</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.8.1.2</td>
<td>wioModuleName</td>
<td>R</td>
<td>Name of module</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.8.1.3</td>
<td>wioModuleType</td>
<td>R</td>
<td>Type of module</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.8.1.4</td>
<td>wioModuleCount</td>
<td>R</td>
<td>Count of module</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.8.1.5</td>
<td>wioModule-AlternativeFormat</td>
<td>R</td>
<td>Module in alternative format</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.8.1.6</td>
<td>wioModuleAnalog-OutLength</td>
<td>R</td>
<td>Length of analog output data of module (Bit)</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.8.1.7</td>
<td>wioModuleAnalog-InLength</td>
<td>R</td>
<td>Length of analog input data of module (Bit)</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.8.1.8</td>
<td>wioModuleDigital-OutLength</td>
<td>R</td>
<td>Length of digital output data of module (Bit)</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.50.8.1.9</td>
<td>wioModuleDigital-InLength</td>
<td>R</td>
<td>Length of digital input data of module (Bit)</td>
</tr>
</tbody>
</table>

15.2.17 Plc Data Group

The Plc data group contains values that can be used for data exchange with CODESYS.

Table 219: WAGO MIB – Plc Data Group

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Entry</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.13576.10.1.100.1</td>
<td>wioPlcDataTable</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.100.1.1</td>
<td>wioPlcDataEntry</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.100.1.1.1</td>
<td>wioPlcDataIndex</td>
<td>R/W</td>
<td>Number of plc data DWORD</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.100.1.1.2</td>
<td>wioPlcDataReadArea</td>
<td>R/W</td>
<td>Readable plc data (DWORD)</td>
</tr>
<tr>
<td>1.3.6.1.4.1.13576.10.1.100.1.1.3</td>
<td>wioPlcDataWriteArea</td>
<td>R</td>
<td>Write-/readable plc data DWORD</td>
</tr>
</tbody>
</table>
ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers)
ASHRAE is an American professional association for HVAC engineering that was founded in 1894. ASHRAE prepares and publishes manuals, magazines, standards and guidelines for the air-conditioning sector. The BACnet protocol has been the standard for ASHRAE since 1995 and was accepted by ANSI in 2004 (ANSI/ASHRAE 135-2004).

BACnet (Building Automation and Control Networks)
BACnet denotes a fieldbus, a protocol, a standard or a process that can be used to compatibly exchange data between devices of various manufacturers. BACnet was developed in 1987 by ASHRAE for building automation services and has become anchored in different standards since then (ASHRAE/ANSI standard (135-2004), DIN EN ISO standard (16484-5)). BACnet is primarily oriented toward the HVAC sector.

BACnet standard objects and properties, which can be accessed by likewise standardized services, are defined in the standard to achieve the required interoperability. Manufacturers publish in a document (PICS) those BACnet standard objects, properties and services that they support. This information is provided in blocks broken down into the various functions (BIBBs). Devices are classified in five device profiles to permit easier comparison of the BACnet devices with regard to their various functions and the different possible combinations of objects and services. Each device profile specifies defined minimum requirements for the BACnet functionality that is implemented, facilitating the selection of a suitable device by the customer for specific applications. BACnet is suitable for the field level as well as the automation level.

BACnet Configurator
The BACnet Configurator is free software that is used for commissioning and configuration of WAGO BACnet couplers/controllers. This includes, among other things, logical structuring of the project and network, addressing of the coupler/controller, configuration of the client and the service in every BACnet device and a value browser (for BACnet object properties). The BACnet Configurator is separate, dedicated software and should not be confused with the I/O Configurator for the WAGO-I/O-PRO.
**BACnet Data Types**

Services utilize standardized BACnet data types and communication units, so-called application layer protocol data units (APDUs) that are defined in an abstract ASN.8824 syntax in accordance with ISO Standard 1 to ensure uniform data transfer.

Elementary data types such as BOOLEAN and INTEGER, and defined BACnet base types are used which consist of SEQUENCES and CHOICES, for example. The latter are made up of elementary or nested, compiled data types.

**BACnet/IP**

BACnet/IP is a standardized and company-neutral network protocol for building automation services used primarily in the HVAC sector.

This protocol supports building-specific, standard objects and services for integrating devices within networks to ensure interoperability.

This protocol is defined in three (3) layers: BACnet Virtual Link Layer (BVLL) as a backup and bit transfer layer, BACnet Network Layer as the transfer layer and BACnet Application as the application layer. ARCNET, ETHERNET, BACnet/IP, PTP (Point-To-Point) are supported via RS232; MS/TP (Master Slave/Token Passing) via RS485 and LonTalk ANSI/EIA709.1 on the backup and bit transfer layer.

Communication between different devices is executed based on the client/server method, with each device able to act as a client or as a server.

This protocol, which has been an ASHRAE standard since 1995, was accepted as a standard by ANSI (ANSI/ASHRAE 135-2004) and has become anchored in the DIN EN ISO standard 16484-5 (Building Automation Systems, Data Communication Protocols).

**BACstac**

Function libraries that implement the BACnet protocol and interfaces with well-known high-level languages are known as BACstacs. BACstacs are generally available on the market. BACstacs simplify and accelerate the development of new BACnet devices, as protocol communication at the lowest level is already implemented by BACstac, enabling the developer to build directly upon the application level.

**Baseband**

Baseband systems are systems that operate without carrier frequencies, i.e. with non-modulated signals. This means they provide exactly one channel that must be logically adapted to the various, specific requirements. Opposite: Broadband

**BBMD (BACnet Broadcast Management Device)**

BACnet uses broadcast messages ("to everyone") for data communication via networks. Many routers block broadcasts. This is why special routers, BBMDs, are used in networks. A BBMD receives a broadcast that is to be sent to a different network and transmits it directly to the BBMD in the other network. The BBMD receiving the message then transmits the broadcast within its local network. This allows the broadcast to be received by the target device.
**B-BC (BACnet-Building-Controller)**
The BACnet Building Controller forms one of six different device profiles described by the BACnet Standard. The B-BC is comparable to a control system in building automation services (Direct Digital Control (DDC)).

To meet the requirements of the BACnet Standard for a B-BC, or for a defined device profile, certain BACnet objects, services, etc., must be implemented in the device. These are defined by the function blocks (BIBBs). The BIBBs that are supported by the device are entered in a document (PICS) that serves as the basis for communication and comparison for manufacturers and customers.

**BIBB (BACnet Interoperability Building Block)**
A BIBB defines which BACnet features must be implemented in a device for each task. Compared to the BIBBs from different manufacturers, common features represent a basis for interoperability between the devices. BIBBs form the function blocks for the specific interoperability area (IA) and define the functions within this base.

A BIBB is formed from the IA in which it is contained, the Service that can be used and the user (client or server).

Example: DS - RP - A (consisting of IA (DS), Service (RP), User (A))

BIBBs are published in the manufacturers PICS. The Device profile is classified on the basis of the supported BIBBs.

**BIG EU (BACnet Interest Group Europe)**
The BIG EU is made up of famous members of the building, planning and production industries as well as different training facilities. It publishes reference solutions in the BACnet area to support planners who work in this field. Among other things the NISTIR (National Institute of Standards and Technology Interagency Report) Guideline is also published (http://www.big-eu.de).

**Bit**
Smallest information unit. Its value can either be 1 or 0.

**Bit Rate**
Number of bits transmitted within a time unit.

**BootP**
The Bootstrap Protocol sends configuration data to several controllers/computers, etc. (without hard drives). This eliminates the need for manual, individual configuration.

BootP is used at WAGO for assigning IP addresses to couplers/controllers. DHCP reverts back to BootP.

**Bridge**
A bridge runs on Layer 2 of the ISO/OSI model. Although the bridge corresponds to a Switch, it has only one output, however. Bridges separate the network into Segments, allowing the number of nodes to be increased. Corrupt data is filtered out. Telegrams are then sent when the target address is located in the linked Segment. Only the frame of the MAC layer is treated.
If the destination address is known, the bridge then forwards the data (when the destination address is on a different string than the one where the Frame originated), or destroys it (subscriber already has the frame). If you do not know the address, the bridge forwards the data in all its known Segments and notes the source address.

A bridge is used to transfer messages independently of the message destination.

**Broadband**
Transmission technique using a high bandwidth to permit high data transfer rates. This technique allows several devices to transmit simultaneously.

Opposite: Baseband

**Broadcast**
Broadcast. A message that is sent to all stations connected to the network.

**Bus**
Bus is a general designation for a line used for bit-parallel or bit-serial data transfer. The bus consists of address, data, control and supply bus. The width of the bus (8, 16, 32, 64-bit) and its frequency are the determining factors for the data transmission rate. The width of the address bus limits network expansion. The fieldbus is a special type of serial bus.

**Byte (Binary Yoked Transfer Element)**
A data element larger than a bit and smaller than a word. A byte generally contains 8 bits. A byte may contain 9 bits in 36-bit computers.

**Client**
Service-requesting device within the Client Server System. With the aid of the service request, the client can access objects (data) on the Server. The service is provided by the server.

**Coaxial Cable**
This cable contains one, single conductor and radial shielding for transmitting information.

**CSMA/CD (Carrier Sense Multiple Access/Collision Detection)**
Random bus access procedure (Carrier Sense Multiple Access with Collision Detection). When a collision is detected, all subscribers back. After waiting (a random delay time), the subscribers attempt to re-transmit the data.
Deterministic ETHERNET
Deterministic ETHERNET denotes that the runtimes can be defined and calculated in an ETHERNET network. This is possible by setting up a Switched ETHERNET.

Device profiles (BACnet)
Six (6) device profiles are defined, with each one classifying a minimum number of functions/BBBs that are supported.
Classification for the devices is specified in Appendix L of the BACnet standards and can be used to determine interoperability in the specific IAs.
Standardized Device Profile:
B-OWS  BACnet Operator Workstation
B-BC    BACnet Building Controller
B-AAC   BACnet Advanced Application Controller
B-SA    BACnet Smart Actuator
B-SS    BACnet Smart Sensor
B-GW    BACnet Gateway
BACnet Gateway Device profiles are published in the manufacturer PICS and make it easier for the customer to compare different BACnet devices with respect to their functions and interoperability.

DHCP (Dynamic Host Configuration Protocol)
This protocol permits automatic configuration of the network for a computer, and also assigns addresses or sets parameters centrally. The DHCP server uses a fixed IP address pool for automatically assigning random, temporary IP addresses to networked computers (Clients) or couplers/controllers, thus saving considerable configuration work in large networks. The client also obtains other information, such as the gateway address (router) and the IP address of the Domain Name System (DNS).

DNS (Domain Name System)
The Domain Name System is a distributed, decentralized database that manages the name sector in the Internet. Unique domain names (such as http://www.wago.de) are transformed into IP addresses (such as 123.45.67.123) using a “forward lookup.” IP addresses can be converted back to domain names using a “reverse lookup.” Using the naming service several IP address can be used for one domain name for distribution of network load. Besides this, domain names are easier to remember than IP addresses. If an IP address changes in the background, this does not affect the domain name. Paul Mockapetris developed the DNS in 1983. Since then it has been expanded to include other standards and has become anchored in the RFC 1034 and RFC.

Driver
Software code, which communicates with a hardware device. This communication is normally performed by internal device registers.
E

EDE (Electronic Data Exchange)
The EDE file serves as a configuration aid for coordinating the functions between devices from different suppliers or commissioning parties. This file contains the addresses set in the BACnet Configurator and the names of the devices and objects, along with the values for the object properties. Generation of the EDE file for the WAGO BACnet coupler/controller can be started directly from the user interface for the BACnet Configurator.

In the “Server” mode the objects for the BACnet coupler/controller can be exported into an EDE file. In the “Client” mode, external objects can be imported using the EDE file.

EIB (European Installation Bus)
see KNX

ETHERNET
Specifies a Local Area Network (LAN), which was developed by Xerox, Intel and DEC in the 70’s. The bus access process takes place according to the CSMA/CD method.

ETHERNET Standard
ETHERNET was standardized in 1983 with IEEE 802.3 10Base5. ISO accepted this standardization with the ISO Standard 8802/3. ETHERNET can, in the meantime, be used with all common types of cables and with optic fibers. There are, however, some technical and considerable logical differences between the standardized variants and the original “ETHERNET,” which is why the term “ETHERNET” is used when the older design is meant and “802.3” is used for standardized systems. The essential differences between the ETHERNET and the IEEE standard are found in the frame architecture and in the handling of pad characters.

F

Fieldbus
The fieldbus is a dedicated bus for the serial transmission of information. Fieldbus systems connect sensors, actuators and controls from the field level to the management level. Numerous different fieldbus systems have been developed for various purposes. For example, the BACnet, LON and KNX fieldbus systems are used primarily in building automation, whereas CANbus and Interbus are applied chiefly in the automotive industry.

Firewall
Collective name for solutions that protect LANs from unauthorized access from the internet. They are also able to control and regulate the traffic from the LAN
into the Internet. The crucial part of firewalls is static Routers, which have an access control list used to decide which data packets can pass from which Host.

**Frame**
Unit of data transferred at the Data-Link layer. It contains the header and addressing information.

**FTP (File Transfer Protocol)**
A standard application for TCP/IP, which permits files to be transferred without files being accessed.

**Function**
Functions are modules that always return the same results (as a function value) when the input values are identical. They have no local variables that store values beyond an invoke.

**Function Block**
Function blocks are used for IEC 61131 programming and stored in libraries for repeated utilization. A function block is a structured module, which has a name and contains input and output variables, as well as local variables.

**Gateway**
Device for connecting two different networks, performs the translation between differing protocols.

**Hardware**
Electronic, electric and mechanical components of a module.

**Header**
A portion of the data packet, containing information such as the receiver's address information.

**Host**
Originally used to describe a central mainframe computer accessed from other systems. The services provided by the subscriber can be called up by means of local and remote request. Today, host can also refer to computers that provide certain services from a central location (such as UNIX hosts on the Internet).
HTML (Hypertext Markup Language)
HTML is the descriptive language for documents on the World Wide Web. It contains language elements for the design of hypertext documents.

HTTP (Hyper Text Transfer Protocol)
Client/Server TCP/IP protocol, which is used on the Internet or Intranets for exchange of HTML documents. It normally uses Port 80.

Hub
A device, which allows communication between several network users via twisted pair cable. Its topology is star-shaped.

HVAC (Heating, Ventilation and Air Conditioning)
HVAC is a special sector of building automation services.

Hypertext
Document format used by HTTP. Hypertext documents are text files that provide links to other text documents via particular highlighted keywords.

ICMP (Internet Control Message Protocol)
ICMP is a protocol for transmission of status information and error messages of the IP, TCP and UDP protocols between IP network nodes. ICMP offers, among other things, the possibility of an echo (ping) request to determine whether a destination is available and is responding.

IEC 61131-3
International standard for modern systems with PLC functionality created in 1993. Based on a structured software model, it defines a series of powerful programming languages to be utilized for different automation tasks. AWL (statement list - STL), ST (structured text), AS (process structure), FUP (function plan), KOP (contact plan).

IEEE
Institute of Electrical and Electronic Engineers.

IEEE 802.3
IEEE 802.3 is an IEEE standard. ETHERNET only supports the yellow cable as a medium (Thicknet ETHERNET coaxial cable). IEEE 802.3 also supports S UTP and Broadband coaxial cable. The segment lengths range from 500 m for yellow cable, 100 m for TP and 1800 m for Broadband coaxial cable. A star or bus topology is possible. ETHERNET (IEEE 802.3) uses CSMA/CD as a channel access method.

Intel Format
Set configuration for the coupler/controller for setting up the process image. In the coupler/controller memory, the module data is aligned in different ways,
depending on the set configuration (Intel/Motorola-Format, word alignment, etc.). The format determines whether or not high and low bytes are changed over – they are not changed with the Intel format.

**Internet**
A collection of networks interconnected to each other throughout the world. It is most commonly referred to as the World Wide Web, or simply as the Web.

**Interoperability**
Interoperability is the capability of different devices, systems, methods or even organizations to find a common language for mutually achieving a set goal. Systems and software operate with interoperability, for example, when they are linked via interfaces, when they use common network protocols and data formats, or when they contain the same standards. These conditions enable information and data to be exchanged and provided in an efficient manner.

**Interoperability Area (IA)**
To evaluate the overall interoperability of a system the requirements made on the individual devices are broken down into seven areas (Interoperability Areas) according to their functions. These then serve as the basis for evaluating the interoperability.
The following IAs are defined: Data Sharing (DS), Alarm and Event Notification (AE), Scheduling, (SCHED), Trending (T), Device Management (DM), Network Management, Network Management (NM) und Virtual Terminal Management (VT).
Each of these IAs possesses a collection of interoperability or function modules, the BIBBS. These modules define all services that a client or server can perform with the IA.
The abbreviation for the IA (e.g. DS) is placed in front of the BIBB name.

**Intranet**
A private network within an organization that allows users to exchange data within that particular organization.

**I/O Configurator**
The I/O Configurator is a plug-in incorporated into WAGO-I/O-PRO for easier assignment of addresses and protocols for modules at a coupler/controller.

**IP (Internet Protocol)**
Internet protocol is a network protocol that performs packet-oriented, connectionless and non-acknowledged transfer of data within a network. This protocol builds upon the transfer layer for the ISO/OSI model. Stations identify themselves using IP addresses.

**IP Message Tunneling**
In addition to BACnet/IP, IP message tunneling is a method for transferring BACnet messages to a network.
Communication via IP message tunneling takes place via the BACnet tunneling router (BTR), which is also designated as “Annex H Router” on account of its description in the annex of the BACnet Standard.
Implementation between the different communication technologies BACnet and
IP is performed using routing tables, with a combination of BACnet network numbers and IP addresses. The BACnet protocol requires an Annex H router in both local area networks in order to send a message from one device to another one on a different network. The Annex H router for the first network transfers the BACnet message to a UDP (User Datagram Protocol) frame and transmits the message over standard IP links, or over the Internet to the Annex H router in network 2. This router then “unpacks” the incoming data packet and sends the message to the destination device via the BACnet protocol. BACnet devices do not require IP compatibility for IP message tunneling via BTRs. BTRs are frequently used in existing BACnet networks that have a link to IP networks, to an intranet or to the Internet.

**ISO/OSI (Open Systems Interconnection) Model**

The ISO/OSI model is a reference model for networks, with the goal of creating open communication. It defines the interface standards of the respective software and hardware requirements between computer manufacturers. The model treats communication removed from specific implementations, using seven layers. The model treats communication removed from specific implementations, using seven layers: 1 - Bit transfer layer, 2 - Backup layer, 3 - Transfer layer, 4 - Transport layer, 5 - Session layer, 6 - Presentation layer and 7 - Application layer.

**KNX**

KNX has been established as a flexible bus system for building automation and has been standardized by the KNX Association in ISO/IEC 14543. KNX was developed by the European installation bus (EIB), BatiBUS and European Home Systems (EHS). In addition to twisted pair, other transmission media, such as powerline, radio and links to ETHERNET (“KNXnet/IP”) are also supported.

**LAN (Local Area Network)**

A LAN is a spatially limited, local network for permanently linking computers over shorter distances. Data transfer can take place via ETHERNET, Token Ring and FDDI, as well as wireless (WLAN).

**Library**

Collection of Modules available to the programmer in the WAGO-I/O-PRO programming tool for creating control programs in accordance with IEC61131-3.

**LON (Local Operating Network)**

LON is used as a fieldbus for building automation. It was developed 1990 by
Echelon and enables, as does KNX, the communication between different devices, independent of the manufacturer and active application.

M

MIB (Management Information Base)
MIB is a collection of information about all parameters, which can be handed over to the management software with a request via SNMP. This enables remote maintenance, monitoring and control of networks to be performed via SNMP protocol.

MODBUS
MODBUS is an open protocol based on the Master/Slave principle. The MODBUS links the master with several clients, via either serial interface or ETHERNET.
Three data transmission types are available: MODBUS/RTU (binary data transmission), MODBUS/TCP (data transmission using TCP/IP packets) and MODBUS/ASCII (ASCII code transmission).

Module
Modules consist of functions, function blocks and programs.
Every module is made up of a declaration part and a body. The body is written in one of the IEC programming languages AWL (statement list - STL), ST (structured text), AS (process structure), FUP (function plan) or KOP (contact plan).
Natives BACnet

“Native” BACnet objects are those objects that are recognized by BACnet couplers/controllers during run-up, without a configuration being loaded. These objects are created automatically for the plugged binary and analog input and output modules. The configuration for the native objects is loaded from the firmware and an internal database. Besides the BACnet coupler/controller, no additional hardware is necessary for integrating BACnet into a network. All requisite, native BACnet objects, properties and services are directly available. This standard behavior for a BACnet coupler/controller can be deactivated in the BACnet Configurator, or in the I/O Configuration using the option “Disable native BACnet”. A gateway is required for communication with non-native BACnet devices/networks. Complex modules do not have any direct equivalent as BACnet objects. Objects for these modules must be created and configured using the WAGO-I/O-PRO I/O Configurator.

Object

BACnet communication takes place using standardized objects (DIN EN 16484-5). These objects are tailored specifically to the HVAC sector for building automation services. Both simple field devices as well as complex automation control systems can be modeled in the object presentation. Objects may represent both physical inputs and outputs and virtual objects, such as counting values. Objects possess certain properties, whose values can be read and/or written using services. All of the objects supported by a device are also described in the PICS data from the specific manufacturer.

Open MODBUS/TCP Specification

Specification, which establishes the specific structure of a MODBUS/TCP data packet. This is dependent upon the selected function code or upon the selected function (import or export bit or register).

Operating System

An operating system is software used for managing equipment such as memory and connected devices, and for executing programs.

Parameter Setting

Parameterization is defined as the assignment and storage of set-up and configuration data as they are required for the execution of predefined functions.
Ping Command
When a ping command (ping < IP address) is entered, the ping program ICMP generates echo request packets. It is used to test for node availability.

Port Number
The port number, in conjunction with the IP address, is the unique connection point between two processes (applications).

Predictable ETHERNET
The predictable message delay time on an ETHERNET network. The measures that are taken here enable nearly real-time requests to be realized.

Prioritization
BACnet applications can access Objects through Services and change their properties. Access prioritization is required to regulate and organize access of various applications to the properties. The BACnet standard distinguishes between 16 different priority levels. A priority can only be set for the current values (Present_Value) of output objects. For this reason they are also called "command properties". The processing sequences for individual applications can be changed using prioritization. Simultaneous access of several applications to the same Objects is regulated in this manner. The application with the highest priority level (lowest number) is given priority.

Property
Objects are described by specific properties and values. In this manner, object information, such as name, status and behavior of an object can be read. Properties may be editable and readable (R), readable and writable (W) and optionally readable and/or writable (O). Access to object properties is gained using Services.
The properties Object_Identifier, Object_Name, Object_Type and Present_Value are common to all Objects. Other properties are object-specific, depending on the function.

Protocol Implementation Conformance Statement (PICS)
The Protocol Implementation Conformance Statement (PICS) described objects and functions supported by BACnet devices. This is a standard document that must be filled in by the manufacturer. When linking different systems, the PICS and the BIBBs for the devices contained therein are compared with one another.

Proxy Server
Proxy means agent or representative. A proxy server (or proxy gateway) allows indirect access to the network by systems, which do not have direct access to the Internet. This may be systems that are restricted from direct access by a firewall for security reasons. A proxy can filter out individual data packets between the Internet and a local network LAN to enhance security. Proxies are also used to limit access to particular servers.
In addition, proxy servers can also have a cache function. In this case they check whether the respective URL address is already available locally and return it immediately, if necessary. This saves time and costs associated with multiple accesses. If the URL is not in the cache, the proxy forwards the request as normal.
The user should not notice the proxy server apart from the single configuration in the web browser. Most web browsers can be configured so that they use different or no proxy gateways per access method (FTP, HTTP).

R

Repeater
Repeater operate (like hubs, but with only one, instead of several outputs) on Layer 1 of the ISO/OSI model. Repeaters are physical amplifiers without their own processing function. They refresh data without detecting damaged data and forward all signals. Repeaters are used for implementing greater transmission distances, or when the maximum number of nodes (normally) 64 devices for each twisted-pair segment is exceeded. The repeater is then always counted as a node in a segment when the maximum number of nodes is reached. The media can also be changed when routers are used that are configured as repeaters.

Request
A service request from a client, which requests the provision of a service from a server.

Response
Response from a server in reply to a request from a client.

RFC Specifications
Specifications, suggestions, ideas and guidelines regarding the Internet are published in the form of RFCs (Request For Comments).

RJ-45 Connector
The RJ-45 plug is also referred to as a Western connector. This connector creates the connection of two network controllers via a twisted-pair cable.

Router
Routers are used to connect neighboring subnets, with the router operating with addresses and protocols of the third ISO/OSI layer. As this layer is hardware independent, the routers allow transition to another transmission medium. To transmit a message the router evaluates the logical address (source and destination address) and finds the best path if there are several possibilities. Routers can be operated in the Repeater or Bridge modes.

Routing
Method of selecting the best path for sending data to a distant network.

RS-232
The RS-232 (official designation ANSI/EIA/TIA-232-F-1997) is a serial interface for point-to-point connections. “RS” stands for “Radio Sector”, but is frequently translated as “Recommended Standard”.

Data is transmitted via this interface bit-serial over a data line and received on a different data line. As only one data line is used at a time, the data is transmitted time-delayed consecutively and asynchronously. The time intervals between transmissions of the data may be randomly long.

As the RS-232 interface is a so-called powered interface, data is transferred electrically encoded.

The cable connections used for this interface are 9-pin Sub-D connectors and 9-pin jacks. A distinction is made here between data lines (RxD, TxD and GND) and control lines (DCD, DTR, DSR, RTS, CTS and RI).

**SCADA (Supervisory Control and Data Acquisition)**

SCADA software is a program for the control and visualization of processes (supervisory control and data acquisition).

**Segment**

Typically, a network is divided up into different physical network segments by way of routers or repeaters.

**Server**

Service-supplying device within a Client Server System. The service is requested by the Client.

**Service**

A service is an operation (Read, Write) oriented toward an object.

BACnet specified standardized services that are transmitted via a special BACnet network layer. Communication is based on the client/server method: The client makes requests to the server. The server processes the requests from the client and then transmits a response. A distinction is made between 38 services that are broken down into 5 categories: Alarm and events, object access, file access, remote device access, and virtual terminal services.

**Service port**

The service port is located next to the mode switch, behind the cover flap on the controller. This port acts as the configuration and programming interface and is used for communication with WAGO-I/O-CHECK, WAGO-I/O-PRO and for downloading firmware. A special programming cable (750-920) is necessary.

**SMTP (Simple Mail Transfer Protocol)**

Standard protocol, with which E-mails are sent via Internet.

**SNMP (Simple Network Management Protocol)**

SNMP is used for remote maintenance of servers. This allows routers, for example, to be configured directly from the network provider's office, without having to physically visit the customer.
**SNTP (Simple Network Time Protocol)**
This connectionless network protocol performs time synchronization in networks with a time server via Internet. SNTP is a simplified version of the NTP protocol. On account of this simplification (also with regard to the software), SNTP operates somewhat less exact than NTP. SNTP is defined in RFC 4330.

**Socket**
A software interface implemented with BSD-UNIX for inter-process communication. Sockets are also possible in the network via TCP/IP. Per Windows 3.11, they are also available in Microsoft operating systems.

**STP (Shielded Twisted Pair)**
An STP cable is a symmetrical cable with shielded cores twisted in pairs. The classic STP cable is a multi-core cable, whose stranded conductors are isolated. The conductors of the STP cable are individually protected; it has no total shielding.

**S-STEP (Screened/Shielded Twisted Pair)**
In addition to STP cables, S-STEP cables are provided with total shielding consisting of foil or network shielding in addition to the single shielding for the individual conductors.

**Structured Cabling**
With structured cabling, maximum permissible cable lengths are defined (EIA/TIA 568, IS 11801) for site, building and floor cabling, with recommendations for topologies also indicated.

**Subnet**
A portion of a network that shares the same network address as the other portions. These subnets are distinguished through the subnet mask.

**Subnet Mask**
Subnet masks can be used to manipulate the address ranges in the IP address area in reference to the number of subnets and hosts. A standard subnet mask, for example, is 255.255.255.0.

**S/UTP (Screened Unshielded Twisted-Pair)**
Screened twisted pair cable, which only has one external shield. However, the twisted pair cables are not shielded from each other.

**Switch**
Switches are comparable to bridges, but with several outputs. Each output uses the full ETHERNET bandwidth. Each output uses the full ETHERNET bandwidth. Switches learn which nodes are connected and filter the information transmitted over the network accordingly. Switches learn which nodes are connected and filter the information transmitted over the network accordingly.

**Switched ETHERNET**
ETHERNET network set up using switches. There are a multitude of applications
for switching technologies. ETHERNET switching is becoming increasingly popular in local networks as it allows deterministic ETHERNET.

**TCP (Transport Control Protocol)**
TCP is a connection-oriented network protocol for the transport layer (Layer 4) of the ISO/OSI model provided with relatively secure transmission mechanisms.

**TCP/IP Protocol Stack**
The TCP/IP protocol stack denotes network protocols that enable communication between different networks and topologies.

**Telnet**
The Telnet protocol fulfills the function of a virtual terminal. It allows remote access from the user’s computer to other computer systems on the network.

**Traps**
Traps are unsolicited messages, which are sent by an “agent” to a management system, as soon as something unexpected and interesting for the management system happens. Traps are comparable to interrupts from hardware. A well-known example of a trap message is the “Blue screen” with Win95/98.

**Twisted Pair**
Twisted pair cables (abbreviated to TP).

**UDP (Users Datagram Protocol)**
The user datagram protocol is a communication protocol between two computers and an alternative to TCP (Transmission Control Protocol). As with TCP, UDP communicates via Internet Protocol, although it is somewhat less reliable due to its uncontrolled communication method.

**URL (Uniform Resource Locator)**
Address form for Internet files which are mostly applied within the World Wide Web (WWW). The URL format makes a unique designation of all documents on the internet possible. It describes the address of a document or objects that can be read by a web browser. URL includes the transmission type (HTTP, FTP), the computer that contains the information and the path on the computer. A URL has the following format:

Document type://Computer name/List of contents/File name.
UTP (Unshielded Twisted Pair)
The UTP cable is a symmetrical, non-protected cable with twisted colored wires in pairs. This cable type, either of a two-pair or four-pair design, is the cable type most used for floor wiring and terminal wiring.

V

Vendor ID (BACnet)
The BACnet standard defines numerical identifiers for suppliers. These IDs can be obtained free of charge from ASHRAE and are a prerequisite for development, marketing and operation of BACnet components in a standard BACnet network.
The vendor ID for WAGO Kontakttechnik GmbH & Co. KG is “222”. A list of all assigned vendor IDs is available at the following Internet page: http://www.bacnet.org/VendorID/index.html

W

WAGO-I/O-PRO (CODESYS Automation Alliance)
Uniform programming environment, programming tool by WAGO Kontakttechnik GmbH & Co. KG for the generation of a control program as per IEC61131-3 for all programmable fieldbus controllers (PFC). The software enables a program to be created, tested, debugged and started up.
The predecessor to the WAGO-I/O-PRO software is the WAGO-I/O-PRO 32, Versions 2.1 and 2.2.
The new WAGO-I/O-PRO consists of the basic tool “CODESYS 2.3 CAA” and the target files with the WAGO-specific Drivers.

Web Browser
A Web browser is a program used for reading Hypertext. The browser allows the various documents to be viewed in Hypertext and navigation between documents.

Word Alignment
Set configuration for the fieldbus coupler/controller for setting up the process image. Word-alignment is used to establish the process image word-by-word (2 bytes).

WWW (World Wide Web)
The World Wide Web (network) is a Hypertext system that can be called up via Internet. It is based on the HTTP network protocol, the descriptive language HTML and URLs for unique page (site) addressing.
Switching Technology in the Local Network
Mathias Hein
Thomson Executive Press
ISBN 9781850321668

TCP/IP 2: Running a Successful Network
(Data Communications and Networks Series)
Kevin Washburn, Jim Evans
Addison-Wesley Publishing Company, 1996
ISBN 9780201877113

Local Area Networks - An Introduction to the Technology
John E. McNamara
Digital Press, 1995
ISBN 9780135330500

Information on the Internet:

Fit in one day for TCP/IP sockets
Wiesemann & Theis GmbH
http://www.wut.de

BIG EU (BACnet Interest Group Europe)
The BIG-EU publishes reference solutions in the BACnet area to support planners who work in this field. Among other things the NISTIR (National Institute of Standards and Technology Interagency Report) Guideline is also published.
http://www.big-eu.de/eng

ASHRAE (American Society of Heating, Refrigeration and Air-Conditioning Engineers)
Professional association for all employed in the heating, cooling, ventilation and air-conditioning fields in the USA
http://www.ashrae.org

ASHRAE SSPC 135 Committee
The "Standing Standard Project Committee 135" steers the ongoing development of the protocol
http://www.bacnet.org
List of Figures

Figure 1: Fieldbus Node (Example) ................................................................. 21
Figure 2: Marking Area for Serial Numbers ................................................... 23
Figure 3: Update Matrix from 2016 ................................................................. 25
Figure 4: Isolation for Fieldbus Couplers/Controllers (Example) .................... 28
Figure 5: System Supply via Fieldbus Coupler/Controller (left) and via Internal System Supply Module (right) ............................................................... 29
Figure 6: System Voltage for Standard Couplers/Controllers and Extended ECO Couplers .............................................................. 30
Figure 7: Field Supply for Standard Couplers/Controllers and Extended ECO Couplers ............................................................... 34
Figure 8: Supply Module with Fuse Carrier (Example 750-610) ....................... 36
Figure 9: Removing the Fuse Carrier .............................................................. 37
Figure 10: Opening the Fuse Carrier .............................................................. 37
Figure 11: Changing the Fuse ................................................................... 37
Figure 12: Fuse Modules for Automotive Fuses, Series 282 ......................... 38
Figure 13: Fuse Modules for Automotive Fuses, Series 2006 ......................... 38
Figure 14: Fuse Modules with Pivotable Fuse Carrier, Series 281 ................... 38
Figure 15: Fuse Modules with Pivotable Fuse Carrier, Series 2002 .................. 39
Figure 16: Power Supply Concept ................................................................. 40
Figure 17: Supply Example for Standard Couplers/Controllers ...................... 41
Figure 18: Carrier Rail Contact (Example) .................................................... 45
Figure 19: Cable Shield at Ground Potential ................................................. 46
Figure 20: Examples of the WAGO Shield Connecting System ....................... 47
Figure 21: Application of the WAGO Shield Connecting System .................... 47
Abbildung 22: Ansicht BACnet/IP-Koppler ..................................................... 51
Figure 23: Device Supply ............................................................................. 53
Figure 24: RJ-45 Connector .......................................................................... 54
Figure 25: Display Elements ....................................................................... 55
Figure 26: Service Interface (Closed and Opened Flap) ................................... 56
Figure 27: Mode Selector Switch (Closed and Open Damper of the Service Port) ............................................................................................................. 57
Figure 28: Address Selection Switch (for example setting “0”) ......................... 58
Figure 29: Opening the Memory Card Slot, Inserting an SD/SDHC Memory Card .......................................................... 59
Figure 30: Spacing ..................................................................................... 85
Figure 31: Release Tab of Extended ECO Fieldbus Coupler (Example) ........... 88
Figure 32: Insert I/O Module (Example) ........................................................ 89
Figure 33: Snap the I/O Module into Place (Example) ..................................... 89
Figure 34: Removing the I/O Module (Example) ........................................... 90
Figure 35: Data Contacts ........................................................................... 91
Figure 36: Example for the Arrangement of Power Contacts ......................... 92
Figure 37: Connecting a Conductor to a CAGE CLAMP® ............................ 93
Figure 38: Operating System ..................................................................... 94
Figure 39: Memory Areas and Data Exchange for a Fieldbus Coupler ........... 99
Figure 40: Data Exchange Between MODBUS Master and I/O Modules ...... 101
Figure 41: Restore Function ..................................................................... 105
Figure 42: WBM Page “Backup & Restore” ................................................. 107
Figure 43: WBM Page “Backup & Restore” ....................................................... 109
Figure 44: WBM Page “Backup & Restore” ....................................................... 109
Figure 45: WBM Page “BACnet” ........................................................................ 111
Figure 46: Example of Directory Structure on the SD Card ............................... 115
Figure 47: Address Selection Switch, for Example the Value Setting “50” (2^4 + 2^5) .......................................................................................................... 121
Figure 48: WBM page “Information” (example) ................................................. 139
Figure 49: Display Elements .............................................................................. 168
Figure 50: Node Status – I/O LED Signaling ..................................................... 171
Figure 51: Error Message Coding ..................................................................... 171
Figure 52: Use of the MODBUS Functions ....................................................... 202
Figure 53: Example SCADA Software with Modbus Driver ........................... 244
Figure 54: Marking Example According to ATEX and IECEx ............................ 246
Figure 55: Text Detail – Marking Example According to ATEX and IECEx ........ 246
Figure 56: Marking Example for Approved Ex i I/O Module According to ATEX  
and IECEx ................................................................................................. 248
Figure 57: Text Detail – Marking Example for Approved Ex i I/O Module  
According to ATEX and IECEx ..................................................................... 248
Figure 58: Marking Example According to NEC ............................................... 250
Figure 59: Text Detail – Marking Example According to NEC 500 ................. 250
Figure 60: Text Detail – Marking Example for Approved Ex i I/O Module  
According to NEC 505 ............................................................................. 251
Figure 61: Text Detail – Marking Example for Approved Ex i I/O Module  
According to NEC 506 ............................................................................... 251
Figure 62: Text Detail – Marking Example for Approved Ex i I/O Modules  
According to CEC 18 attachment J .......................................................... 252
List of Tables

Table 1: Number Notation ................................................................. 13
Table 2: Font Conventions ............................................................... 13
Table 3: Labeling Symbols ............................................................... 22
Table 4: Legend for Figure "Update Matrix from 2016" .................... 25
Table 5: Legend for Figure "System Supply via Fieldbus Coupler/Controller (left) and via Internal System Supply Module (right)" ............................................................... 29
Table 6: Alignment .......................................................................... 31
Table 7: Legend for Figure "Field Supply for Standard Couplers/Controllers and Extended ECO Couplers" ............................................................... 34
Table 8: Power Supply Modules .......................................................... 36
Table 9: Filter Modules for 24 V Supply .............................................. 40
Table 10: Legend for Figure “Supply Example for Fieldbus Coupler/Controller” ................................................................. 42
Table 11: WAGO Ground Wire Terminals ........................................... 44
Table 12: Legend for Figure “View FC BACnet/IP; G4 750-332” .......... 52
Table 13: RJ-45 Connector and RJ-45 Connector Configuration ............ 54
Table 14: Display Elements Fieldbus Status ....................................... 55
Table 15: Display Elements Node Status ............................................. 55
Table 16: Display Elements Supply Voltage ........................................ 55
Table 17: Legend for Figure “Service Interface (Closed and Opened Flap)” ................................................................. 56
Table 18: Legend for Figure „Mode Selector Switch“ .......................... 57
Table 19: Meaning of DIP Switch Positions ......................................... 58
Table 20: Technical Data - Device ...................................................... 61
Table 21: Technical Data - System ...................................................... 61
Table 22: Technical Data – Accessories .............................................. 63
Table 23: Technical Data – Field Wiring ............................................. 63
Table 24: Technical Data – Data Contacts ........................................... 63
Table 25: Technical Data – Climatic Environmental Conditions .......... 64
Table 26: Technical Data – Mechanical Strength .................................. 65
Table 27: Technical Data – Software Compatibility ............................ 65
Table 28: BACnet Approvals ............................................................. 66
Table 29: BIBBs of the B-BC ............................................................. 70
Table 30: WAGO DIN Rails ............................................................... 85
Table 31: Data Width for I/O Modules ................................................ 100
Table 32: Allocation of Digital Inputs and Outputs to Process Data Words in Accordance with the ................................................................. 101
Table 33: Possible Errors on System Start .......................................... 106
Table 34: Possible Errors During the Backup Function ....................... 108
Table 35: Possible Errors During the Restore Function ........................ 110
Table 36: Possible Errors when Inserting the Memory Card During Ongoing Operation ................................................................. 112
Table 37: Possible Errors when Removing the Memory Card During Ongoing Operation ................................................................. 113
Table 38: Possible Errors During the FTP Network Access on the File System of the Memory Card ................................................................. 114
Table 39: Data Saved in the Directory Structure .................................. 115
Table 40: Address selection switch values (host ID) ............................. 120
Table 41: WBM User Groups ............................................................ 137
Table 42: WBM Page “Information” ................................................................... 140
Table 43: WBM Page “Administration” ............................................................. 141
Table 44: WBM Page „Backup & Restore” ........................................................ 144
Table 45: WBM Page „Clock“ ........................................................................... 148
Table 46: WBM Page “Miscellaneous” .............................................................. 149
Table 47: WBM Page “SD Card” ...................................................................... 150
Table 48: WBM page "Storage Media" ............................................................. 151
Table 49: WBM Page “Clock” ........................................................................... 151
Table 50: WBM Page „Ethernet“ ................................................................. 152
Table 51: WBM page „Protocols“ ................................................................. 156
Table 52: WBM Page “SNMP v1/v2” ................................................................. 158
Table 53: WBM Page “SNMP V3” .................................................................. 159
Table 54: WBM Page “SNTP” .......................................................................... 160
Table 55: WBM-Seite „TCP/IP“ ....................................................................... 161
Table 56: WBM Page “BACnet” ....................................................................... 162
Table 57: WBM page „BACnet Information“ .................................................... 163
Table 58: WBM page “MODBUS” ................................................................... 165
Table 59: WBM page „I/O Data“ .................................................................... 167
Table 60: LED Assignment for Diagnostics ................................................... 168
Table 61: Fieldbus Assignment for Diagnostics – Solution in Event of Error .... 169
Table 62: Node Status Assignment for Diagnostics – Solution in Event of Error 170
Table 63: Blink code- table for the I/O LED signaling, error code 1 .................. 173
Table 64: Blink Code Table for the I/O LED Signaling, Error Code 2 .............. 174
Table 65: Blink Code Table for the I/O LED Signaling, Error Code 3 .............. 175
Table 66: Blink Code Table for the I/O LED Signaling, Error Code 4 .............. 176
Table 67: Blink Code Table for the I/O LED Signaling, Error Code 5 .............. 176
Table 68: Blink Code Table for the I/O LED Signaling, Error Code 6 .............. 177
Table 69: Blink Code Table for the I/O LED Signaling, Error Code 7 .............. 177
Table 70: Blink Code Table for the I/O LED Signaling, Error Code 8 … 10 … 177
Table 71: Blink Code Table for the I/O LED Signaling, Error Code 11 .......... 178
Table 72: Blink code table for I/O LED signaling, error code 12 ………………….. 178
Table 73: Blink code table for I/O LED signaling, error code 13 ………………….. 178
Table 74: Blink Code Table for the I/O LED Signaling, Error Code 14 .......... 179
Table 75: Power supply status diagnostics – Solution in Event of Error ........... 180
Table 76: IP Packet ......................................................................................... 183
Table 77: Network Class A ............................................................................... 184
Table 78: Network Class B ............................................................................... 184
Table 79: Network Class C ............................................................................... 184
Table 80: Key Data Class A, B and C ............................................................... 185
Table 81: Example: Class B Address with Field for Subnet IDs ...................... 186
Table 82: Subnet Mask for Class A Network .................................................. 186
Table 83: Subnet Mask for Class B Network .................................................. 186
Table 84: Subnet Mask for Class C Network .................................................. 186
Table 85: Example for an IP Address from a Class B Network ....................... 186
Table 86: BootP Options .................................................................................. 190
Table 87: Meaning of DHCP Options ............................................................. 192
Table 88: MIB II groups .................................................................................. 195
Table 89: Standard Traps ............................................................................... 196
Table 90: Modbus TCP Header ...................................................................... 199
Table 91: Basic Data Types of MODBUS Protocol ......................................... 200
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>92</td>
<td>List of the MODBUS Functions in the Fieldbus Coupler</td>
<td>200</td>
</tr>
<tr>
<td>93</td>
<td>Exception Codes</td>
<td>203</td>
</tr>
<tr>
<td>94</td>
<td>Request of Function Code FC1</td>
<td>204</td>
</tr>
<tr>
<td>95</td>
<td>Response of Function Code FC1</td>
<td>204</td>
</tr>
<tr>
<td>96</td>
<td>Assignment of Inputs</td>
<td>205</td>
</tr>
<tr>
<td>97</td>
<td>Exception of Function Code FC1</td>
<td>205</td>
</tr>
<tr>
<td>98</td>
<td>Request of Function Code FC2</td>
<td>206</td>
</tr>
<tr>
<td>99</td>
<td>Response of Function Code FC2</td>
<td>206</td>
</tr>
<tr>
<td>100</td>
<td>Assignment of Inputs</td>
<td>206</td>
</tr>
<tr>
<td>101</td>
<td>Exception of Function Code FC2</td>
<td>207</td>
</tr>
<tr>
<td>102</td>
<td>Request of Function Code FC3</td>
<td>208</td>
</tr>
<tr>
<td>103</td>
<td>Response of Function Code FC3</td>
<td>208</td>
</tr>
<tr>
<td>104</td>
<td>Exception of Function Code FC3</td>
<td>208</td>
</tr>
<tr>
<td>105</td>
<td>Request of Function Code FC4</td>
<td>209</td>
</tr>
<tr>
<td>106</td>
<td>Response of Function Code FC4</td>
<td>209</td>
</tr>
<tr>
<td>107</td>
<td>Exception of Function Code FC4</td>
<td>209</td>
</tr>
<tr>
<td>108</td>
<td>Request of Function Code FC5</td>
<td>210</td>
</tr>
<tr>
<td>109</td>
<td>Response of Function Code FC5</td>
<td>210</td>
</tr>
<tr>
<td>110</td>
<td>Exception of Function Code FC5</td>
<td>210</td>
</tr>
<tr>
<td>111</td>
<td>Request of Function Code FC6</td>
<td>211</td>
</tr>
<tr>
<td>112</td>
<td>Response of Function Code FC6</td>
<td>211</td>
</tr>
<tr>
<td>113</td>
<td>Exception of Function Code FC6</td>
<td>211</td>
</tr>
<tr>
<td>114</td>
<td>Request of function code FC11</td>
<td>212</td>
</tr>
<tr>
<td>115</td>
<td>Response of Function Code FC11</td>
<td>212</td>
</tr>
<tr>
<td>116</td>
<td>Exception of Function Code FC 11</td>
<td>212</td>
</tr>
<tr>
<td>117</td>
<td>Request of Function Code FC15</td>
<td>213</td>
</tr>
<tr>
<td>118</td>
<td>Response of Function Code FC15</td>
<td>213</td>
</tr>
<tr>
<td>119</td>
<td>Exception of Function Code FC15</td>
<td>214</td>
</tr>
<tr>
<td>120</td>
<td>Request of Function Code FC16</td>
<td>215</td>
</tr>
<tr>
<td>121</td>
<td>Response of Function Code FC16</td>
<td>215</td>
</tr>
<tr>
<td>122</td>
<td>Exception of Function Code FC16</td>
<td>215</td>
</tr>
<tr>
<td>123</td>
<td>Request of Function Code FC22</td>
<td>216</td>
</tr>
<tr>
<td>124</td>
<td>Response of Function Code FC22</td>
<td>216</td>
</tr>
<tr>
<td>125</td>
<td>Exception of Function Code FC22</td>
<td>216</td>
</tr>
<tr>
<td>126</td>
<td>Request of Function Code FC23</td>
<td>217</td>
</tr>
<tr>
<td>127</td>
<td>Response of Function Code FC23</td>
<td>217</td>
</tr>
<tr>
<td>128</td>
<td>Exception of Function Code FC23</td>
<td>217</td>
</tr>
<tr>
<td>129</td>
<td>Register Access Reading (with FC3 and FC4)</td>
<td>217</td>
</tr>
<tr>
<td>130</td>
<td>Register Access Writing (with FC6 and FC16)</td>
<td>219</td>
</tr>
<tr>
<td>131</td>
<td>Bit Access Reading (with FC1 and FC2)</td>
<td>221</td>
</tr>
<tr>
<td>132</td>
<td>Bit Access Writing (with FC5 and FC15)</td>
<td>221</td>
</tr>
<tr>
<td>133</td>
<td>Modbus Registers</td>
<td>222</td>
</tr>
<tr>
<td>134</td>
<td>MODBUS registers (Continuation)</td>
<td>223</td>
</tr>
<tr>
<td>135</td>
<td>Register Address 0x1000</td>
<td>225</td>
</tr>
<tr>
<td>136</td>
<td>Register Address 0x1001</td>
<td>226</td>
</tr>
<tr>
<td>137</td>
<td>Register Address 0x1002</td>
<td>226</td>
</tr>
<tr>
<td>138</td>
<td>Register Address 0x1003</td>
<td>226</td>
</tr>
<tr>
<td>139</td>
<td>Register Address 0x1004</td>
<td>227</td>
</tr>
<tr>
<td>140</td>
<td>Register Address 0x1005</td>
<td>227</td>
</tr>
<tr>
<td>141</td>
<td>Register Address 0x1006</td>
<td>227</td>
</tr>
<tr>
<td>Table</td>
<td>Register Address</td>
<td>Page</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------</td>
<td>------</td>
</tr>
<tr>
<td>142</td>
<td>0x1007</td>
<td>227</td>
</tr>
<tr>
<td>143</td>
<td>0x1008</td>
<td>227</td>
</tr>
<tr>
<td>144</td>
<td>0x1009</td>
<td>228</td>
</tr>
<tr>
<td>145</td>
<td>0x100A</td>
<td>228</td>
</tr>
<tr>
<td>146</td>
<td>Starting Watchdog</td>
<td>228</td>
</tr>
<tr>
<td>147</td>
<td>0x100B</td>
<td>229</td>
</tr>
<tr>
<td>148</td>
<td>0x1020</td>
<td>230</td>
</tr>
<tr>
<td>149</td>
<td>0x1021</td>
<td>230</td>
</tr>
<tr>
<td>150</td>
<td>0x1022</td>
<td>231</td>
</tr>
<tr>
<td>151</td>
<td>0x1023</td>
<td>231</td>
</tr>
<tr>
<td>152</td>
<td>0x1024</td>
<td>231</td>
</tr>
<tr>
<td>153</td>
<td>0x1025</td>
<td>231</td>
</tr>
<tr>
<td>154</td>
<td>0x1029</td>
<td>231</td>
</tr>
<tr>
<td>155</td>
<td>0x102A</td>
<td>232</td>
</tr>
<tr>
<td>156</td>
<td>0x102B</td>
<td>232</td>
</tr>
<tr>
<td>157</td>
<td>0x1030</td>
<td>232</td>
</tr>
<tr>
<td>158</td>
<td>0x1031</td>
<td>232</td>
</tr>
<tr>
<td>159</td>
<td>0x1037</td>
<td>232</td>
</tr>
<tr>
<td>160</td>
<td>0x1038</td>
<td>232</td>
</tr>
<tr>
<td>161</td>
<td>0x1050</td>
<td>233</td>
</tr>
<tr>
<td>162</td>
<td>0x2000</td>
<td>233</td>
</tr>
<tr>
<td>163</td>
<td>0x2001</td>
<td>233</td>
</tr>
<tr>
<td>164</td>
<td>0x2002</td>
<td>233</td>
</tr>
<tr>
<td>165</td>
<td>0x2003</td>
<td>233</td>
</tr>
<tr>
<td>166</td>
<td>0x2004</td>
<td>234</td>
</tr>
<tr>
<td>167</td>
<td>0x2005</td>
<td>234</td>
</tr>
<tr>
<td>168</td>
<td>0x2006</td>
<td>234</td>
</tr>
<tr>
<td>169</td>
<td>0x2007</td>
<td>234</td>
</tr>
<tr>
<td>170</td>
<td>0x2008</td>
<td>234</td>
</tr>
<tr>
<td>171</td>
<td>0x2010</td>
<td>235</td>
</tr>
<tr>
<td>172</td>
<td>0x2011</td>
<td>235</td>
</tr>
<tr>
<td>173</td>
<td>0x2012</td>
<td>235</td>
</tr>
<tr>
<td>174</td>
<td>0x2013</td>
<td>235</td>
</tr>
<tr>
<td>175</td>
<td>0x2014</td>
<td>235</td>
</tr>
<tr>
<td>176</td>
<td>0x2020</td>
<td>235</td>
</tr>
<tr>
<td>177</td>
<td>0x2021</td>
<td>236</td>
</tr>
<tr>
<td>178</td>
<td>0x2022</td>
<td>236</td>
</tr>
<tr>
<td>179</td>
<td>0x2023</td>
<td>236</td>
</tr>
<tr>
<td>180</td>
<td>0x2030</td>
<td>237</td>
</tr>
<tr>
<td>181</td>
<td>0x2031</td>
<td>237</td>
</tr>
<tr>
<td>182</td>
<td>0x2032</td>
<td>237</td>
</tr>
<tr>
<td>183</td>
<td>0x2033</td>
<td>237</td>
</tr>
<tr>
<td>184</td>
<td>0x2035</td>
<td>238</td>
</tr>
<tr>
<td>185</td>
<td>0x2036</td>
<td>238</td>
</tr>
<tr>
<td>186</td>
<td>0x2040</td>
<td>238</td>
</tr>
<tr>
<td>187</td>
<td>0x2043</td>
<td>238</td>
</tr>
<tr>
<td>188</td>
<td>Modbus Table and Function Codes</td>
<td>244</td>
</tr>
<tr>
<td>189</td>
<td>Description of Marking Example According to ATEX and IECEx</td>
<td>247</td>
</tr>
<tr>
<td>190</td>
<td>Description of Marking Example for Approved Ex i I/O Module According to ATEX and IECEx</td>
<td>249</td>
</tr>
</tbody>
</table>
Table 191: Description of Marking Example According to NEC 500 ................. 250
Table 192: Description of Marking Example for Approved Ex i I/O Module
According to NEC 505 ....................................................................................... 251
Table 193: Description of Marking Example for Approved Ex i I/O Modules
According to NEC 506 ....................................................................................... 251
Table 194: Description of Marking Example for Approved Ex i I/O Modules
According to CEC 18 attachment J ................................................................. 252
Table 195: MIB II – System Group ................................................................. 256
Table 196: MIB II – Interface Group ............................................................... 257
Table 197: MIB II – IP Group ........................................................................... 259
Table 198: MIB II – IpRoute Table Group ....................................................... 260
Table 199: MIB II – ICMP Group ..................................................................... 261
Table 200: MIB II – TCP Group ....................................................................... 262
Table 201: MIB II – UDP Group ....................................................................... 263
Table 202: MIB II – SNMP Group .................................................................... 264
Table 203: WAGO MIB – Company Group .................................................... 265
Table 204: WAGO MIB – Product Group ....................................................... 265
Table 205: WAGO MIB – Versions Group ...................................................... 266
Table 206: WAGO MIB – Real Time Clock Group .......................................... 267
Table 207: WAGO MIB – Ethernet Group ....................................................... 268
Table 208: WAGO MIB – Actual Error Group ............................................... 268
Table 209: WAGO MIB – PLC Project Group ................................................. 269
Table 210: WAGO MIB – Http Group ............................................................. 270
Table 211: WAGO MIB – Ftp Group ............................................................... 270
Table 212: WAGO MIB – Snmp Group ............................................................ 271
Table 213: WAGO MIB – Snmp Trap String Group ......................................... 273
Table 214: WAGO MIB – Snmp User Trap String Group .................................. 274
Table 215: WAGO MIB – Plc Connection Group ............................................. 274
Table 216: WAGO MIB – Plc Connection Group ............................................. 274
Table 217: WAGO MIB – Modbus Group ......................................................... 275
Table 218: WAGO MIB – Process Image Group ............................................. 276
Table 219: WAGO MIB – Plc Data Group ....................................................... 276